Policy Compliance Auditing

Report generated by Nessus™ Mon, 06 May 2024 09:37:52 CEST

TABLE OF CONTENTS

Vulnerabilities by Plugin

- 14272 (9) - Netstat Portscanner (SSH)..... 18
- 19506 (1) - Nessus Scan Information..... 20
- 141118 (1) - Target Credential Status by Authentication Protocol - Valid Credentials Provided..... 22

Compliance 'FAILED'

- 1.1.1.1 Ensure mounting of cramfs filesystems is disabled..... 25
- 1.1.2.1 Ensure /tmp is a separate partition..... 27
- 1.1.2.2 Ensure nodev option set on /tmp partition..... 31
- 1.1.2.3 Ensure noexec option set on /tmp partition..... 34
- 1.1.2.4 Ensure nosuid option set on /tmp partition..... 37
- 1.1.3 Ensure auditing is configured for the Docker daemon..... 40
- 1.1.4 Ensure auditing is configured for Docker files and directories - /run/containerd..... 43
- 1.1.5 Ensure auditing is configured for Docker files and directories - /var/lib/docker..... 46
- 1.1.6 Ensure auditing is configured for Docker files and directories - /etc/docker..... 49
- 1.1.7 Ensure auditing is configured for Docker files and directories - docker.service..... 52
- 1.1.8 Ensure auditing is configured for Docker files and directories - containerd.sock..... 55
- 1.1.8.2 Ensure noexec option set on /dev/shm partition..... 58
- 1.1.9 Ensure auditing is configured for Docker files and directories - docker.sock..... 61
- 1.1.10 Disable USB Storage - blacklist..... 64
- 1.1.10 Disable USB Storage - modprobe..... 66
- 1.1.10 Ensure auditing is configured for Docker files and directories - /etc/default/docker..... 68
- 1.1.11 Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json..... 71
- 1.1.12 Ensure auditing is configured for Docker files and directories - /etc/containerd/config.toml..... 74
- 1.1.13 Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker..... 77
- 1.1.14 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd..... 80
- 1.1.15 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim..... 83
- 1.1.16 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-run..... 86

- 1.1.17 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-run..... 89
- 1.1.18 Ensure auditing is configured for Docker files and directories - /usr/bin/runc..... 92
- 1.2.2 Ensure that the version of Docker is up to date..... 95
- 1.3.1 Ensure AIDE is installed - aide..... 97
- 1.3.1 Ensure AIDE is installed - aide-common..... 100
- 1.3.2 Ensure filesystem integrity is regularly checked..... 103
- 1.4.1 Ensure bootloader password is set - 'passwd_pbkdf2'..... 106
- 1.4.1 Ensure bootloader password is set - 'set superusers'..... 108
- 1.4.2 Ensure permissions on bootloader config are configured..... 110
- 1.5.4 Ensure core dumps are restricted - limits config..... 113
- 1.5.4 Ensure core dumps are restricted - sysctl config..... 116
- 1.7.2 Ensure local login warning banner is configured properly - banner..... 119
- 1.7.3 Ensure remote login warning banner is configured properly - banner..... 121
- 2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver - NTP..... 123
- 2.2.16 Ensure rsync service is either not installed or masked..... 126
- 2.3.4 Ensure telnet client is not installed..... 128
- 2.8 Enable user namespace support --userns-remap=default..... 130
- 2.9 Enable user namespace support - SecurityOptions..... 132
- 2.11 Ensure that authorization for Docker client commands is enabled..... 134
- 2.12 Ensure centralized and remote logging is configured..... 136
- 2.12 Ensure that authorization for Docker client commands is enabled..... 138
- 2.13 Ensure centralized and remote logging is configured..... 140
- 2.17 Ensure that a daemon-wide custom seccomp profile is applied if appropriate..... 143
- 3.2.1 Ensure packet redirect sending is disabled - net.ipv4.conf.all.send_redirects (sysctl.conf/sys..... 145
- 3.2.1 Ensure packet redirect sending is disabled - net.ipv4.conf.default.send_redirects (sysctl.conf..... 148
- 3.2.1 Ensure packet redirect sending is disabled - sysctl net.ipv4.conf.default.send_redirects..... 151
- 3.2.2 Ensure IP forwarding is disabled - sysctl ipv4..... 154
- 3.3.1 Ensure source routed packets are not accepted - net.ipv4.conf.all.accept_source_route (sysctl..... 157
- 3.3.1 Ensure source routed packets are not accepted - net.ipv4.conf.default.accept_source_route (sys..... 161

- 3.3.1 Ensure source routed packets are not accepted - net.ipv6.conf.all.accept_source_route (sysctl..... 165
- 3.3.1 Ensure source routed packets are not accepted - net.ipv6.conf.default.accept_source_route (sys..... 169
- 3.3.2 Ensure ICMP redirects are not accepted - net.ipv4.conf.all.accept_redirects (sysctl.conf/sysct..... 173
- 3.3.2 Ensure ICMP redirects are not accepted - net.ipv4.conf.default.accept_redirects (sysctl.conf/s..... 177
- 3.3.2 Ensure ICMP redirects are not accepted - net.ipv6.conf.all.accept_redirects (sysctl.conf/sysct..... 181
- 3.3.2 Ensure ICMP redirects are not accepted - net.ipv6.conf.default.accept_redirects (sysctl.conf/s..... 185
- 3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv4.conf.default.accept_redirects..... 189
- 3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv6.conf.all.accept_redirects..... 192
- 3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv6.conf.default.accept_redirects..... 195
- 3.3.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.all.secure_redirects' (sysctl.c..... 198
- 3.3.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.default.secure_redirects' (sysc..... 201
- 3.3.3 Ensure secure ICMP redirects are not accepted - 'sysctl net.ipv4.conf.all.secure_redirects'..... 204
- 3.3.3 Ensure secure ICMP redirects are not accepted - 'sysctl net.ipv4.conf.default.secure_redirects..... 207
- 3.3.4 Ensure suspicious packets are logged - 'net.ipv4.conf.all.log_martians' (sysctl.conf/sysctl.d)..... 210
- 3.3.4 Ensure suspicious packets are logged - 'net.ipv4.conf.default.log_martians' (sysctl.conf/sysct..... 214
- 3.3.4 Ensure suspicious packets are logged - 'sysctl net.ipv4.conf.all.log_martians'..... 218
- 3.3.4 Ensure suspicious packets are logged - 'sysctl net.ipv4.conf.default.log_martians'..... 222
- 3.3.5 Ensure broadcast ICMP requests are ignored - sysctl.conf/sysctl.d..... 226
- 3.3.6 Ensure bogus ICMP responses are ignored - (sysctl.conf/sysctl.d)..... 229
- 3.3.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.all.rp_filter' (sysctl.conf/sysctl.d..... 232
- 3.3.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.default.rp_filter' (sysctl.conf/sysc..... 235
- 3.3.7 Ensure Reverse Path Filtering is enabled - 'sysctl net.ipv4.conf.all.rp_filter'..... 238
- 3.3.7 Ensure Reverse Path Filtering is enabled - 'sysctl net.ipv4.conf.default.rp_filter'..... 241
- 3.3.8 Ensure TCP SYN Cookies is enabled - sysctl.conf/sysctl.d..... 244
- 3.3.9 Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.all.accept_ra' (sysctl.con..... 247
- 3.3.9 Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.default.accept_ra' (sysctl..... 250
- 3.3.9 Ensure IPv6 router advertisements are not accepted - 'sysctl net.ipv6.conf.all.accept_ra'..... 253
- 3.3.9 Ensure IPv6 router advertisements are not accepted - 'sysctl net.ipv6.conf.default.accept_ra'..... 256
- 3.7 Ensure that registry certificate file ownership is set to root:root..... 259

- 3.8 Ensure that registry certificate file permissions are set to 444 or more restrictively..... 261
- 3.9 Ensure that TLS CA certificate file ownership is set to root:root..... 264
- 3.10 Ensure that TLS CA certificate file permissions are set to 444 or more restrictively..... 266
- 3.11 Ensure that Docker server certificate file ownership is set to root:root..... 269
- 3.12 Ensure that the Docker server certificate file permissions are set to 444 or more restrictively.....271
- 4.1.4.1 Ensure audit log files are mode 0640 or less permissive.....274
- 4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - auditctl.....277
- 4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - auditd..... 280
- 4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - augenrul.....283
- 4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - aureport... 286
- 4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - ausearch.....289
- 4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - autrace.....292
- 4.2.1.1.2 Ensure systemd-journal-remote is configured.....295
- 4.2.1.1.3 Ensure systemd-journal-remote is enabled..... 298
- 4.2.1.3 Ensure journald is configured to compress large log files..... 300
- 4.2.1.4 Ensure journald is configured to write logfiles to persistent disk..... 303
- 4.2.2.3 Ensure journald is configured to send logs to rsyslog.....305
- 4.2.2.5 Ensure logging is configured..... 308
- 4.2.2.6 Ensure rsyslog is configured to send logs to a remote log host.....311
- 4.2.3 Ensure all logfiles have appropriate permissions and ownership.....314
- 4.5 Ensure Content trust for Docker is Enabled.....320
- 5.1.2 Ensure permissions on /etc/crontab are configured.....322
- 5.1.3 Ensure permissions on /etc/cron.hourly are configured.....325
- 5.1.4 Ensure permissions on /etc/cron.daily are configured.....328
- 5.1.5 Ensure permissions on /etc/cron.weekly are configured.....331
- 5.1.6 Ensure permissions on /etc/cron.monthly are configured..... 334
- 5.1.7 Ensure permissions on /etc/cron.d are configured..... 337
- 5.1.8 Ensure cron is restricted to authorized users - '/etc/cron.allow'..... 340

- 5.1.9 Ensure at is restricted to authorized users - '/etc/at.allow'..... 343
- 5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured..... 346
- 5.2.4 Ensure SSH access is limited..... 349
- 5.2.6 Ensure SSH PAM is enabled..... 353
- 5.2.7 Ensure SSH root login is disabled..... 356
- 5.2.17 Ensure SSH warning banner is configured..... 359
- 5.2.18 Ensure SSH MaxAuthTries is set to 4 or less..... 362
- 5.2.19 Ensure SSH MaxStartups is configured..... 365
- 5.2.21 Ensure SSH LoginGraceTime is set to one minute or less..... 368
- 5.2.22 Ensure SSH Idle Timeout Interval is configured..... 371
- 5.3.2 Ensure sudo commands use pty..... 374
- 5.3.3 Ensure sudo log file exists..... 376
- 5.3.7 Ensure access to the su command is restricted..... 379
- 5.4.1 Ensure password creation requirements are configured - 'dcredit'..... 382
- 5.4.1 Ensure password creation requirements are configured - 'lcredit'..... 385
- 5.4.1 Ensure password creation requirements are configured - 'minlen'..... 388
- 5.4.1 Ensure password creation requirements are configured - 'ocredit'..... 391
- 5.4.1 Ensure password creation requirements are configured - 'ucredit'..... 394
- 5.4.2 Ensure lockout for failed password attempts is configured..... 397
- 5.4.3 Ensure password reuse is limited..... 400
- 5.4.4 Ensure password hashing algorithm is up to date with the latest standards..... 402
- 5.5.1.1 Ensure minimum days between password changes is configured - login.defs..... 405
- 5.5.1.1 Ensure minimum days between password changes is configured - users..... 407
- 5.5.1.2 Ensure password expiration is 365 days or less - login.defs..... 409
- 5.5.1.2 Ensure password expiration is 365 days or less - users..... 411
- 5.5.1.4 Ensure inactive password lock is 30 days or less - useradd..... 413
- 5.5.1.4 Ensure inactive password lock is 30 days or less - users..... 415
- 5.5.4 Ensure default user umask is 027 or more restrictive - Default user umask..... 417
- 5.5.4 Ensure default user umask is 027 or more restrictive - Restrictive system umask..... 422

- 5.5.5 Ensure default user shell timeout is 900 seconds or less..... 427
- 6.1.9 Ensure no world writable files exist..... 430
- 6.1.10 Ensure no unowned files or directories exist.....434
- 6.1.11 Ensure no ungrouped files or directories exist.....437
- 6.2.9 Ensure root PATH Integrity.....440
- 6.2.13 Ensure local interactive user home directories are mode 750 or more restrictive.....442
- 6.2.17 Ensure local interactive user dot files are not group or world writable.....445

Compliance 'SKIPPED'

Compliance 'PASSED'

- 1.1.3.2 Ensure nodev option set on /var partition..... 450
- 1.1.3.3 Ensure nosuid option set on /var partition..... 453
- 1.1.4.2 Ensure noexec option set on /var/tmp partition..... 456
- 1.1.4.3 Ensure nosuid option set on /var/tmp partition.....459
- 1.1.4.4 Ensure nodev option set on /var/tmp partition..... 462
- 1.1.5.2 Ensure nodev option set on /var/log partition.....465
- 1.1.5.3 Ensure noexec option set on /var/log partition..... 468
- 1.1.5.4 Ensure nosuid option set on /var/log partition.....471
- 1.1.6.2 Ensure noexec option set on /var/log/audit partition.....474
- 1.1.6.3 Ensure nodev option set on /var/log/audit partition.....477
- 1.1.6.4 Ensure nosuid option set on /var/log/audit partition.....480
- 1.1.7.2 Ensure nodev option set on /home partition.....483
- 1.1.7.3 Ensure nosuid option set on /home partition.....486
- 1.1.8.1 Ensure nodev option set on /dev/shm partition.....489
- 1.1.8.3 Ensure nosuid option set on /dev/shm partition.....492
- 1.1.9 Disable Automounting..... 495
- 1.1.10 Disable USB Storage - lsmod.....497
- 1.4.3 Ensure authentication required for single user mode..... 499
- 1.5.1 Ensure address space layout randomization (ASLR) is enabled - config.....501

- 1.5.1 Ensure address space layout randomization (ASLR) is enabled - sysctl 503
- 1.5.2 Ensure prelink is not installed 505
- 1.5.3 Ensure Automatic Error Reporting is not enabled 508
- 1.5.4 Ensure core dumps are restricted - processsizemax 510
- 1.5.4 Ensure core dumps are restricted - storage 512
- 1.5.4 Ensure core dumps are restricted - sysctl 514
- 1.6.1.1 Ensure AppArmor is installed 517
- 1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration - apparmor 520
- 1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration - security 523
- 1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode - loaded 526
- 1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode - unconfined 529
- 1.7.1 Ensure message of the day is configured properly - banner 532
- 1.7.1 Ensure message of the day is configured properly - platform flags 534
- 1.7.2 Ensure local login warning banner is configured properly - platform flags 536
- 1.7.3 Ensure remote login warning banner is configured properly - platform flags 538
- 1.7.4 Ensure permissions on /etc/motd are configured 540
- 1.7.5 Ensure permissions on /etc/issue are configured 543
- 1.7.6 Ensure permissions on /etc/issue.net are configured 546
- 1.8.2 Ensure GDM login banner is configured - banner-message-enable 549
- 1.8.2 Ensure GDM login banner is configured - banner-message-text 552
- 1.8.3 Ensure GDM disable-user-list option is enabled 554
- 1.8.4 Ensure GDM screen locks when the user is idle - idle-delay 556
- 1.8.4 Ensure GDM screen locks when the user is idle - lock-delay 560
- 1.8.5 Ensure GDM screen locks cannot be overridden - idle-delay 564
- 1.8.5 Ensure GDM screen locks cannot be overridden - lock-delay 567
- 1.8.6 Ensure GDM automatic mounting of removable media is disabled 570
- 1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden 573
- 1.8.8 Ensure GDM autorun-never is enabled 576
- 1.8.9 Ensure GDM autorun-never is not overridden 579

- 1.8.10 Ensure XDCMP is not enabled..... 581
- 1.9 Ensure updates, patches, and additional security software are installed.....583
- 2.1.1.1 Ensure a single time synchronization daemon is in use.....586
- 2.1.2.1 Ensure chrony is configured with authorized timeserver.....589
- 2.1.2.2 Ensure chrony is running as user _chrony..... 591
- 2.1.2.3 Ensure chrony is enabled and running - enabled..... 593
- 2.1.2.3 Ensure chrony is enabled and running - running.....595
- 2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver - FallbackNTP.....597
- 2.1.3.2 Ensure systemd-timesyncd is enabled and running - enabled..... 600
- 2.1.3.2 Ensure systemd-timesyncd is enabled and running - running..... 602
- 2.1.4.1 Ensure ntp access control is configured - restrict -4..... 604
- 2.1.4.1 Ensure ntp access control is configured - restrict -6..... 607
- 2.1.4.2 Ensure ntp is configured with authorized timeserver.....610
- 2.1.4.3 Ensure ntp is running as user ntp..... 613
- 2.1.4.4 Ensure ntp is enabled and running - active..... 615
- 2.1.4.4 Ensure ntp is enabled and running - enabled..... 617
- 2.2.1 Ensure X Window System is not installed.....619
- 2.2.2 Ensure Avahi Server is not installed..... 621
- 2.2.3 Ensure CUPS is not installed..... 623
- 2.2.4 Ensure DHCP Server is not installed - isc-dhcp-server.....625
- 2.2.5 Ensure LDAP server is not installed.....627
- 2.2.6 Ensure NFS is not installed..... 629
- 2.2.7 Ensure DNS Server is not installed..... 631
- 2.2.8 Ensure FTP Server is not installed..... 633
- 2.2.9 Ensure HTTP server is not installed.....635
- 2.2.10 Ensure IMAP and POP3 server are not installed - dovecot-imapd..... 637
- 2.2.10 Ensure IMAP and POP3 server are not installed - dovecot-pop3d..... 639
- 2.2.11 Ensure Samba is not installed.....641
- 2.2.12 Ensure HTTP Proxy Server is not installed..... 643

- 2.2.13 Ensure SNMP Server is not installed..... 645
- 2.2.14 Ensure NIS Server is not installed..... 647
- 2.2.15 Ensure mail transfer agent is configured for local-only mode..... 649
- 2.3.1 Ensure NIS Client is not installed..... 651
- 2.3.2 Ensure rsh client is not installed..... 653
- 2.3.3 Ensure talk client is not installed..... 655
- 2.3.5 Ensure LDAP client is not installed..... 657
- 2.3.6 Ensure RPC is not installed..... 659
- 2.8 Enable user namespace support - /etc/subgid..... 661
- 2.8 Enable user namespace support - /etc/subuid..... 663
- 2.9 Enable user namespace support - /etc/subgid..... 665
- 2.9 Enable user namespace support - /etc/subuid..... 667
- 2.9 Ensure the default cgroup usage has been confirmed..... 669
- 2.10 Ensure the default cgroup usage has been confirmed - daemon.json..... 671
- 2.10 Ensure the default cgroup usage has been confirmed - dockerd..... 673
- 2.11 Ensure base device size is not changed until needed - daemon.json..... 675
- 2.11 Ensure base device size is not changed until needed - dockerd..... 677
- 3.1 Ensure that the docker.service file ownership is set to root:root..... 679
- 3.1.2 Ensure wireless interfaces are disabled..... 682
- 3.2 Ensure that docker.service file permissions are appropriately set..... 684
- 3.2.1 Ensure packet redirect sending is disabled - sysctl net.ipv4.conf.all.send_redirects..... 687
- 3.2.2 Ensure IP forwarding is disabled - ipv4 (sysctl.conf/sysctl.d)..... 690
- 3.2.2 Ensure IP forwarding is disabled - ipv6 (sysctl.conf/sysctl.d)..... 693
- 3.2.2 Ensure IP forwarding is disabled - sysctl ipv6..... 696
- 3.3 Ensure that docker.socket file ownership is set to root:root..... 699
- 3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv4.conf.all.accept_source_route..... 702
- 3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv4.conf.default.accept_source_rou..... 706
- 3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv6.conf.all.accept_source_route..... 710

- 3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv6.conf.default.accept_source_rou..... 714
- 3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv4.conf.all.accept_redirects..... 718
- 3.3.5 Ensure broadcast ICMP requests are ignored - sysctl exec..... 721
- 3.3.6 Ensure bogus ICMP responses are ignored - (sysctl exec)..... 724
- 3.3.8 Ensure TCP SYN Cookies is enabled - sysctl exec..... 727
- 3.4 Ensure that docker.socket file permissions are set to 644 or more restrictive..... 730
- 3.5 Ensure that the /etc/docker directory ownership is set to root:root..... 733
- 3.5.1.1 Ensure ufw is installed..... 735
- 3.5.1.2 Ensure iptables-persistent is not installed with ufw..... 737
- 3.5.1.3 Ensure ufw service is enabled - systemctl..... 739
- 3.5.1.3 Ensure ufw service is enabled - ufw..... 742
- 3.5.1.4 Ensure ufw loopback traffic is configured - v4..... 745
- 3.5.1.4 Ensure ufw loopback traffic is configured - v6..... 747
- 3.5.1.5 Ensure ufw outbound connections are configured..... 749
- 3.5.1.6 Ensure ufw firewall rules exist for all open ports..... 751
- 3.5.1.7 Ensure ufw default deny firewall policy..... 753
- 3.5.2.1 Ensure nftables is installed..... 756
- 3.5.2.2 Ensure ufw is uninstalled or disabled with nftables..... 758
- 3.5.2.3 Ensure iptables are flushed with nftables - ip6tables..... 760
- 3.5.2.3 Ensure iptables are flushed with nftables - iptables..... 762
- 3.5.2.4 Ensure a nftables table exists..... 764
- 3.5.2.5 Ensure nftables base chains exist - forward..... 766
- 3.5.2.5 Ensure nftables base chains exist - input..... 769
- 3.5.2.5 Ensure nftables base chains exist - output..... 772
- 3.5.2.6 Ensure nftables loopback traffic is configured - lo..... 775
- 3.5.2.6 Ensure nftables loopback traffic is configured - v4..... 777
- 3.5.2.6 Ensure nftables loopback traffic is configured - v6..... 779
- 3.5.2.7 Ensure nftables outbound and established connections are configured - input..... 781
- 3.5.2.7 Ensure nftables outbound and established connections are configured - output..... 783

- 3.5.2.8 Ensure nftables default deny firewall policy - forward..... 785
- 3.5.2.8 Ensure nftables default deny firewall policy - input..... 788
- 3.5.2.8 Ensure nftables default deny firewall policy - output..... 791
- 3.5.2.9 Ensure nftables service is enabled..... 794
- 3.5.2.10 Ensure nftables rules are permanent - forward..... 796
- 3.5.2.10 Ensure nftables rules are permanent - input..... 798
- 3.5.2.10 Ensure nftables rules are permanent - output..... 800
- 3.5.3.1.1 Ensure iptables packages are installed - iptables..... 802
- 3.5.3.1.1 Ensure iptables packages are installed - iptables-persistent..... 804
- 3.5.3.1.2 Ensure nftables is not installed with iptables..... 806
- 3.5.3.1.3 Ensure ufw is uninstalled or disabled with iptables..... 808
- 3.5.3.2.1 Ensure iptables default deny firewall policy - 'Chain FORWARD'..... 810
- 3.5.3.2.1 Ensure iptables default deny firewall policy - 'Chain INPUT'..... 812
- 3.5.3.2.1 Ensure iptables default deny firewall policy - 'Chain OUTPUT'..... 814
- 3.5.3.2.2 Ensure iptables loopback traffic is configured..... 816
- 3.5.3.2.3 Ensure iptables outbound and established connections are configured..... 818
- 3.5.3.2.4 Ensure iptables firewall rules exist for all open ports..... 820
- 3.5.3.3.1 Ensure ip6tables default deny firewall policy - 'Chain FORWARD'..... 823
- 3.5.3.3.1 Ensure ip6tables default deny firewall policy - 'Chain INPUT'..... 825
- 3.5.3.3.1 Ensure ip6tables default deny firewall policy - 'Chain OUTPUT'..... 827
- 3.5.3.3.2 Ensure ip6tables loopback traffic is configured..... 829
- 3.5.3.3.3 Ensure ip6tables outbound and established connections are configured..... 831
- 3.5.3.3.4 Ensure ip6tables firewall rules exist for all open ports..... 833
- 3.6 Ensure that /etc/docker directory permissions are set to 755 or more restrictively..... 835
- 3.15 Ensure that the Docker socket file ownership is set to root:docker..... 838
- 3.16 Ensure that the Docker socket file permissions are set to 660 or more restrictively..... 841
- 3.17 Ensure that the daemon.json file ownership is set to root:root..... 844
- 3.18 Ensure that daemon.json file permissions are set to 644 or more restrictive..... 846
- 3.19 Ensure that the /etc/default/docker file ownership is set to root:root..... 849

- 3.20 Ensure that the /etc/default/docker file permissions are set to 644 or more restrictively..... 851
- 3.21 Ensure that the /etc/sysconfig/docker file permissions are set to 644 or more restrictively.....854
- 3.22 Ensure that the /etc/sysconfig/docker file ownership is set to root:root.....857
- 3.23 Ensure that the Containerd socket file ownership is set to root:root..... 859
- 3.24 Ensure that the Containerd socket file permissions are set to 660 or more restrictively..... 862
- 4.1.4.2 Ensure only authorized users own audit log files.....865
- 4.1.4.3 Ensure only authorized groups are assigned ownership of audit log files.....868
- 4.1.4.4 Ensure the audit log directory is 0750 or more restrictive.....871
- 4.1.4.5 Ensure audit configuration files are 640 or more restrictive.....874
- 4.1.4.6 Ensure audit configuration files are owned by root.....877
- 4.1.4.7 Ensure audit configuration files belong to group root.....880
- 4.1.4.8 Ensure audit tools are 755 or more restrictive.....883
- 4.1.4.9 Ensure audit tools are owned by root..... 886
- 4.1.4.10 Ensure audit tools belong to group root.....889
- 4.2.1.1.1 Ensure systemd-journal-remote is installed.....892
- 4.2.1.1.4 Ensure journald is not configured to receive logs from a remote client.....894
- 4.2.1.2 Ensure journald service is enabled.....897
- 4.2.1.5 Ensure journald is not configured to send logs to rsyslog.....899
- 4.2.2.1 Ensure rsyslog is installed.....902
- 4.2.2.2 Ensure rsyslog service is enabled.....904
- 4.2.2.4 Ensure rsyslog default file permissions are configured.....906
- 4.2.2.7 Ensure rsyslog is not configured to receive logs from a remote client.....910
- 5.1 Ensure swarm mode is not Enabled, if not needed.....913
- 5.1.1 Ensure cron daemon is enabled and running - enabled.....915
- 5.1.1 Ensure cron daemon is enabled and running - running.....917
- 5.1.8 Ensure cron is restricted to authorized users - '/etc/cron.deny'.....919
- 5.1.9 Ensure at is restricted to authorized users - '/etc/at.deny'..... 922
- 5.2.2 Ensure permissions on SSH private host key files are configured.....925
- 5.2.3 Ensure permissions on SSH public host key files are configured.....928

- 5.2.5 Ensure SSH LogLevel is appropriate....931
- 5.2.8 Ensure SSH HostbasedAuthentication is disabled....934
- 5.2.9 Ensure SSH PermitEmptyPasswords is disabled....937
- 5.2.10 Ensure SSH PermitUserEnvironment is disabled....940
- 5.2.11 Ensure SSH IgnoreRhosts is enabled....943
- 5.2.13 Ensure only strong Ciphers are used....946
- 5.2.14 Ensure only strong MAC algorithms are used....950
- 5.2.15 Ensure only strong Key Exchange algorithms are used....954
- 5.2.20 Ensure SSH MaxSessions is set to 10 or less....958
- 5.3 Ensure that, if applicable, SELinux security options are set....960
- 5.3.1 Ensure sudo is installed....962
- 5.3.5 Ensure re-authentication for privilege escalation is not disabled globally....965
- 5.3.6 Ensure sudo authentication timeout is configured correctly....967
- 5.5.1.3 Ensure password expiration warning days is 7 or more - login.defs....969
- 5.5.1.3 Ensure password expiration warning days is 7 or more - users....971
- 5.5.1.5 Ensure all users last password change date is in the past....973
- 5.5.2 Ensure system accounts are secured....976
- 5.5.3 Ensure default group for the root account is GID 0....979
- 5.23 Ensure that docker exec commands are not used with the privileged option....982
- 5.24 Ensure that docker exec commands are not used with the user=root option....984
- 6.1.1 Ensure permissions on /etc/passwd are configured....986
- 6.1.2 Ensure permissions on /etc/passwd- are configured....989
- 6.1.3 Ensure permissions on /etc/group are configured....992
- 6.1.4 Ensure permissions on /etc/group- are configured....995
- 6.1.5 Ensure permissions on /etc/shadow are configured....998
- 6.1.6 Ensure permissions on /etc/shadow- are configured....1001
- 6.1.7 Ensure permissions on /etc/gshadow are configured....1004
- 6.1.8 Ensure permissions on /etc/gshadow- are configured....1007
- 6.2.1 Ensure accounts in /etc/passwd use shadowed passwords....1010

- 6.2.2 Ensure /etc/shadow password fields are not empty..... 1012
- 6.2.3 Ensure all groups in /etc/passwd exist in /etc/group..... 1014
- 6.2.4 Ensure shadow group is empty..... 1016
- 6.2.5 Ensure no duplicate UIDs exist..... 1019
- 6.2.6 Ensure no duplicate GIDs exist..... 1021
- 6.2.7 Ensure no duplicate user names exist..... 1023
- 6.2.8 Ensure no duplicate group names exist..... 1025
- 6.2.10 Ensure root is the only UID 0 account..... 1027
- 6.2.11 Ensure local interactive user home directories exist..... 1029
- 6.2.12 Ensure local interactive users own their home directories..... 1032
- 6.2.14 Ensure no local interactive user has .netrc files..... 1035
- 6.2.15 Ensure no local interactive user has .forward files..... 1038
- 6.2.16 Ensure no local interactive user has .rhosts files..... 1041
- 7.5 Ensure Docker's secret management commands are used for managing secrets in a Swarm cluster..... 1044
- 7.8 Ensure node certificates are rotated as appropriate..... 1046
- 7.9 Ensure CA certificates are rotated as appropriate..... 1048
- 7.10 Ensure management plane traffic has been separated from data plane traffic..... 1050
- CIS Docker Community Edition v1.1.0 L2 Docker..... 1052
- CIS_Docker_v1.6.0_L2_Docker_Linux.audit from CIS Docker Benchmark v1.6.0..... 1053
- CIS_Ubuntu_22.04_LTS_Server_v1.0.0_L1.audit from CIS Ubuntu Linux 22.04 LTS Benchmark..... 1054

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

- 1.2.1 Ensure package manager repositories are configured..... 1056
- 1.2.1 Ensure the container host has been Hardened..... 1059
- 1.2.2 Ensure GPG keys are configured..... 1061
- 2.4 Ensure nonessential services are removed or masked..... 1064
- 2.10 Ensure base device size is not changed until needed..... 1066
- 2.16 Ensure daemon-wide custom seccomp profile is applied, if needed..... 1067
- 3.1.1 Ensure system is checked to determine if IPv6 is enabled..... 1069

- 4.2.1.6 Ensure journald log rotation is configured per site policy..... 1072
- 4.2.1.7 Ensure journald default file permissions configured..... 1074
- 4.8 Ensure setuid and setgid permissions are removed..... 1078
- 4.8 Ensure setuid and setgid permissions are removed in the images..... 1080
- 4.11 Ensure only verified packages are installed..... 1081
- 4.11 Ensure verified packages are only Installed..... 1083
- 5.2 Ensure SELinux security options are set, if applicable..... 1085
- 5.4.5 Ensure all current passwords uses the configured hashing algorithm..... 1087
- 5.22 Ensure docker exec commands are not used with privileged option..... 1089
- 5.23 Ensure docker exec commands are not used with user option..... 1090
- 5.29 Ensure Docker's default bridge docker0 is not used..... 1091
- 5.30 Ensure that Docker's default bridge 'docker0' is not used..... 1094
- 6.1.12 Audit SUID executables..... 1096
- 6.1.13 Audit SGID executables..... 1100
- CIS Docker Community Edition v1.1.0 L2 Docker..... 1104
- CIS_Docker_v1.6.0_L2_Docker_Linux.audit from CIS Docker Benchmark v1.6.0..... 1106
- CIS_Ubuntu_22.04_LTS_Server_v1.0.0_L1.audit from CIS Ubuntu Linux 22.04 LTS Benchmark..... 1107
- CIS_Ubuntu_22.04_LTS_Workstation_v1.0.0_L1.audit from CIS Ubuntu Linux 22.04 LTS Benchmark..... 1108
- CIS_Ubuntu_22.04_LTS_v.1.0.0_Server_L2.audit from CIS Ubuntu Linux 22.04 LTS Benchmark..... 1109
- CIS_Ubuntu_22.04_LTS_v.1.0.0_Workstation_L2.audit from CIS Ubuntu Linux 22.04 LTS Benchmark..... 1110
- DISA_STIG_Docker_Enterprise_2.x_Linux_Unix_v2r1.audit from DISA Docker Enterprise 2.x Linux/UNIX v2r..... 1111

Remediations

- Suggested Remediations..... 1113

Vulnerabilities by Plugin

14272 (9) - 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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

Plugin Output

192.168.111.1 (tcp/22/ssh)

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

192.168.111.1 (tcp/80/www)

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

192.168.111.1 (tcp/443/www)

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

192.168.111.1 (udp/443)

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

192.168.111.1 (udp/30041)

```
Port 30041/udp was found to be open
```

192.168.111.1 (udp/30042)

```
Port 30042/udp was found to be open
```

192.168.111.1 (tcp/30252)

```
Port 30252/tcp was found to be open
```

192.168.111.1 (tcp/42001/www)

```
Port 42001/tcp was found to be open
```

192.168.111.1 (udp/51021)

```
Port 51021/udp was found to be open
```

19506 (1) - 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: 2024/03/13

Plugin Output

192.168.111.1 (tcp/0)

```
Information about this scan :

Nessus version : 10.7.2
Nessus build : 20029
Plugin feed version : 202405060214
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
```

```
Scan name : Policy Compliance Auditing
Scan policy used : Policy Compliance Auditing
Scanner IP : 192.168.111.25
Port scanner(s) : netstat
Port range : default
Ping RTT : 161.535 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'anapaya' 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 : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/6 9:33 CEST
Scan duration : 247 sec
Scan for malware : no
```

141118 (1) - 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

192.168.111.1 (tcp/22/ssh)

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

User:       'anapaya'
Port:       22
Proto:      SSH
Method:     publickey
```

```
Escalation: sudo
```

Compliance 'FAILED'

1.1.1.1 Ensure mounting of cramfs filesystems is disabled

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.

Rationale:

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

Solution

Run the following script to disable cramfs:

#!/usr/bin/env bash

{ l_mname='cramfs' # set module name if ! modprobe -n -v '$l_mname' | grep -P -- '^h*install /bin/(true|false)'; then echo -e ' - setting module: '$l_mname' to be not 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*blacklisth+$l_mnameb' /etc/modprobe.d/*; then echo -e ' - deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mname'.conf fi }

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ** PASS ** system: Linux

Hosts

192.168.111.1

```
The command script with multiple lines returned :

-- INFO --
 - module: "cramfs" exists in:
  - "/lib/modules/5.15.0-100-generic/kernel/fs"
  - "/lib/modules/5.15.0-86-generic/kernel/fs"

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - module: "cramfs" is not deny listed
 - module: "cramfs" is loadable: "insmod /lib/modules/5.15.0-86-generic/kernel/fs/cramfs/cramfs.ko "


- Correctly set:

 - module: "cramfs" is not loaded
```

1.1.2.1 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.

Rationale:

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.

Impact:

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

Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a 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.

/tmp utilizing tmpfs can be resized using the size={size} parameter in the relevant entry in /etc/fstab.

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 or tmp.mount.

Example of /etc/fstab configured tmpfs file system with specific mount options:

tmpfs/tmptmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0

Example of tmp.mount configured tmpfs file system with specific mount options:

[Unit] Description=Temporary Directory /tmp ConditionPathIsSymbolicLink=!/tmp DefaultDependencies=no Conflicts=umount.target Before=local-fs.target umount.target After=swap.target

[Mount] What=tmpfs Where=/tmp Type=tmpfs

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/findmnt /tmp expect: ^[\s]*/tmp[\s].* system: Linux

Hosts

192.168.111.1

```
The command '/bin/findmnt /tmp' did not return any result
```

1.1.2.2 Ensure nodev option set on /tmp partition

Info

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

Rationale:

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

Solution

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /tmp partition.

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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/findmnt /tmp -n expect: nodev system: Linux

Hosts

192.168.111.1

```
The command '/bin/findmnt /tmp -n' did not return any result
```

1.1.2.3 Ensure noexec option set on /tmp partition

Info

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

Rationale:

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

Solution

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /tmp partition.

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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/findmnt /tmp -n expect: noexec system: Linux

Hosts

192.168.111.1

```
The command '/bin/findmnt /tmp -n' did not return any result
```

1.1.2.4 Ensure nosuid option set on /tmp partition

Info

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

Rationale:

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

Solution

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /tmp partition.

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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/findmnt /tmp -n expect: nosuid system: Linux

Hosts

192.168.111.1

```
The command '/bin/findmnt /tmp -n' did not return any result
```

1.1.3 Ensure auditing is configured for the Docker daemon

Info

Audit all Docker daemon activities.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit the Docker daemon. Because this daemon runs with root privileges. It is very important to audit its activities and usage.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add rules for the Docker daemon.

For example:

Add the line below to the /etc/audit/rules.d/audit.rules file:

-w /usr/bin/dockerd -k docker

Then, restart the audit daemon using the following command

systemctl restart auditd

Default Value:

By default, the Docker daemon is not audited.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/bin/dockerd expect: -w /usr/bin/dockerd[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/bin/dockerd' returned :

sh: 1: auditctl: not found
```

1.1.4 Ensure auditing is configured for Docker files and directories - /run/containerd

Info

Audit /run/containerd.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit all Docker related files and directories. The Docker daemon runs with root privileges and its behaviour depends on some key files and directories. /run/containerd is one such directory. As it holds all the information about containers it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /run/containerd directory.

For example, Add the line as below to the /etc/audit/rules.d/audit.rules file:

-a exit,always -F path=/run/containerd -F perm=war -k docker

Then, restart the audit daemon using the following command

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /run/containerd expect: -w /run/containerd[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /run/containerd' returned :

sh: 1: auditctl: not found
```

1.1.5 Ensure auditing is configured for Docker files and directories - /var/lib/docker

Info

Audit /var/lib/docker.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit all Docker related files and directories. The Docker daemon runs with root privileges and its behaviour depends on some key files and directories. /var/lib/docker is one such directory. As it holds all the information about containers it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /var/lib/docker directory.

For example, Add the line as below to the /etc/audit/rules.d/audit.rules file:

-a exit,always -F path=/var/lib/docker -F perm=war -k docker

Then, restart the audit daemon using the following command

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /var/lib/docker expect: -w /var/lib/docker[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /var/lib/docker' returned :

sh: 1: auditctl: not found
```

1.1.6 Ensure auditing is configured for Docker files and directories - /etc/docker

Info

Audit /etc/docker.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit all Docker related files and directories. The Docker daemon runs with root privilege and its behavior depends on some key files and directories, one of these being /etc/docker. This holds various certificates and keys used for TLS communication between Docker daemon and Docker client and as such it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /etc/docker directory.

For example:

Add the line below to the /etc/audit/rules.d/audit.rules file:

-w /etc/docker -k docker

Then restart the audit daemon. For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /etc/docker expect: -w /etc/docker[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /etc/docker' returned :

sh: 1: auditctl: not found
```

1.1.7 Ensure auditing is configured for Docker files and directories - docker.service

Info

Audit the docker.service if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories with docker.service being one such file. The docker.service file might be present if the daemon parameters have been changed by an administrator. If so, it holds various parameters for the Docker daemon and should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

If the file exists, a rule for it should be added.

For example:

Add the line as below in /etc/audit/rules.d/audit.rules file:

-w /usr/lib/systemd/system/docker.service -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file docker.service may not be present on the system.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/lib/systemd/system/docker.service expect: -w /usr/lib/systemd/system/docker.service[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/lib/systemd/system/docker.service' returned :

sh: 1: auditctl: not found
```

1.1.8 Ensure auditing is configured for Docker files and directories - containerd.sock

Info

Audit containerd.sock, if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit the Docker daemon. Because this daemon runs with root privileges, it is very important to audit its activities and usage. Its behavior depends on some key files and directories with containerd.sock being one such file, and as this holds various parameters for the Docker daemon, it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

If the file exists, you should add a rule for it.

For example:

Add the line below to the /etc/audit/rules.d/audit.rules file:

-w /run/containerd/containerd.sock -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file containerd.sock may not be present, but if it is, it should be audited.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /run/containerd/containerd.sock expect: -w /run/containerd/containerd.sock[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /run/containerd/containerd.sock' returned :

sh: 1: auditctl: not found
```

1.1.8.2 Ensure noexec option set on /dev/shm partition

Info

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

Rationale:

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

Solution

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition.

Example:

<device> /dev/shm <fstype> 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /dev/shm | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'
expect: noexec system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /dev/shm | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

TARGET   SOURCE FSTYPE OPTIONS
/dev/shm tmpfs  tmpfs  rw,nosuid,nodev,inode64
```

1.1.9 Ensure auditing is configured for Docker files and directories - docker.sock

Info

Audit docker.sock, if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit the Docker daemon. Because this daemon runs with root privileges, it is very important to audit its activities and usage. Its behavior depends on some key files and directories with docker.socket being one such file, and as this holds various parameters for the Docker daemon, it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

If the file exists, you should add a rule for it.

For example:

Add the line below to the /etc/audit/rules.d/audit.rules file:

-w /var/run/docker.sock -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file docker.sock may not be present, but if it is, it should be audited.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /var/run/docker.sock expect: -w /var/run/docker.sock[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /var/run/docker.sock' returned :

sh: 1: auditctl: not found
```

1.1.10 Disable USB Storage - blacklist

Info

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

Rationale:

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

Solution

Run the following script to disable usb-storage:

#!/usr/bin/env bash

{ l_mname='usb-storage' # set module name if ! modprobe -n -v '$l_mname' | grep -P -- '^h*install /bin/(true|false)'; then echo -e ' - setting module: '$l_mname' to be not 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*blacklisth+$l_mnameb' /etc/modprobe.d/*; then echo -e ' - deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mname'.conf fi }

Additional Information:

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

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/grep '^[[:space:]]*blacklist usb-storage' /etc/modprobe.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/grep '^[[:space:]]*blacklist usb-storage' /etc/modprobe.d/* | /usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

1.1.10 Disable USB Storage - modprobe

Info

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

Rationale:

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

Solution

Run the following script to disable usb-storage:

#!/usr/bin/env bash

{ l_mname='usb-storage' # set module name if ! modprobe -n -v '$l_mname' | grep -P -- '^h*install /bin/(true|false)'; then echo -e ' - setting module: '$l_mname' to be not 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*blacklisth+$l_mnameb' /etc/modprobe.d/*; then echo -e ' - deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mname'.conf fi }

Additional Information:

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

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /sbin/modprobe -n -v usb-storage expect: install /bin/(true|false) system: Linux

Hosts

192.168.111.1

```
The command '/sbin/modprobe -n -v usb-storage' returned :

insmod /lib/modules/5.15.0-86-generic/kernel/drivers/usb/storage/usb-storage.ko
```

1.1.10 Ensure auditing is configured for Docker files and directories - /etc/default/docker

Info

Audit /etc/default/docker, if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /etc/default/docker is one such file. It holds various parameters related to the Docker daemon and should therefore be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /etc/default/docker file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /etc/default/docker -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited so these defaults should be changed in line with organizational security policy. The file /etc/default/docker may not be present, and if so, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /etc/default/docker expect: -w /etc/default/docker[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /etc/default/docker' returned :

sh: 1: auditctl: not found
```

1.1.11 Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json

Info

Audit /etc/docker/daemon.json, if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /etc/docker/daemon.json is one such file. This holds various parameters for the Docker daemon, and as such it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /etc/docker/daemon.json file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /etc/docker/daemon.json -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /etc/docker/daemon.json may not exist on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /etc/docker/daemon.json expect: -w /etc/docker/daemon.json[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /etc/docker/daemon.json' returned :

sh: 1: auditctl: not found
```

1.1.12 Ensure auditing is configured for Docker files and directories - /etc/containerd/config.toml

Info

Audit /etc/containerd/config.toml if applicable

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit the Docker daemon. Because this daemon runs with root privileges it is very important to audit its activities and usage. Its behavior depends on some key files and directories and /etc/containerd/config.toml is one such file as it contains various parameters. If present, it is important that it is audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for /etc/containerd/config.toml file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /etc/containerd/config.toml -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /etc/containerd/config.toml may not be present on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /etc/containerd/config.toml expect: -w /etc/containerd/config.toml[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /etc/containerd/config.toml' returned :

sh: 1: auditctl: not found
```

1.1.13 Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker

Info

Audit /etc/sysconfig/docker if applicable

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit the Docker daemon. Because this daemon runs with root privileges it is very important to audit its activities and usage. Its behavior depends on some key files and directories and /etc/sysconfig/docker is one such file as it contains various parameters related to the Docker daemon when run on CentOS and RHEL based distributions. If present, it is important that it is audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for /etc/sysconfig/docker file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /etc/sysconfig/docker -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /etc/sysconfig/docker may not be presemt on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /etc/sysconfig/docker expect: -w /etc/sysconfig/docker[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /etc/sysconfig/docker' returned :

sh: 1: auditctl: not found
```

1.1.14 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd

Info

Audit /usr/bin/containerd if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /usr/bin/containerd is one such file and as such should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /usr/bin/containerd file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /usr/bin/containerd -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /usr/bin/containerd may not be present on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/bin/containerd expect: -w /usr/bin/containerd[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/bin/containerd' returned :

sh: 1: auditctl: not found
```

1.1.15 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim

Info

Audit /usr/bin/containerd-shim if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /usr/bin/containerd-shim is one such file and as such should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /usr/bin/containerd-shim file.

For example:

Add the line below to the /etc/audit/rules.d/audit.rules file:

-w /usr/bin/containerd-shim -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /usr/bin/containerd-shim may not be present on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/bin/containerd-shim expect: -w /usr/bin/containerd-shim[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/bin/containerd-shim' returned :

sh: 1: auditctl: not found
```

1.1.16 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v1

Info

Audit /usr/bin/containerd-shim-runc-v1 if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /usr/bin/containerd-shim-runc-v1 is one such file and as such should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /usr/bin/containerd-shim-runc-v1 file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /usr/bin/containerd-shim-runc-v1 -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /usr/bin/containerd-shim-runc-v1 may not be present on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/bin/containerd-shim-runc-v1 expect: -w /usr/bin/containerd-shim-runc-v1[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/bin/containerd-shim-runc-v1' returned :

sh: 1: auditctl: not found
```

1.1.17 Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v2

Info

Audit /usr/bin/containerd-shim-runc-v2 if applicable.

Rationale:

As well as auditing the normal Linux file system and system calls, you should audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /usr/bin/containerd-shim-runc-v2 is one such file and as such should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for the /usr/bin/containerd-shim-runc-v2 file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /usr/bin/containerd-shim-runc-v2 -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /usr/bin/containerd-shim-runc-v2 may not be present on the system and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/bin/containerd-shim-runc-v2 expect: -w /usr/bin/containerd-shim-runc-v2[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/bin/containerd-shim-runc-v2' returned :

sh: 1: auditctl: not found
```

1.1.18 Ensure auditing is configured for Docker files and directories - /usr/bin/runc

Info

Audit /usr/bin/runc if applicable

Rationale:

As well as auditing the normal Linux file system and system calls, you should also audit all Docker related files and directories. The Docker daemon runs with root privileges and its behavior depends on some key files and directories. /usr/bin/runc is one such file, and as such it should be audited.

Impact:

Auditing can generate large log files. You should ensure that these are rotated and archived periodically. A separate partition should also be created for audit logs to avoid filling up any other critical partition.

Solution

You should add a rule for /usr/bin/runc file.

For example:

Add the line below to the /etc/audit/audit.rules file:

-w /usr/bin/runc -k docker

Then restart the audit daemon.

For example:

systemctl restart auditd

Default Value:

By default, Docker related files and directories are not audited. The file /usr/bin/runc may not be present on the system and in that case this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: auditctl -l | grep /usr/bin/runc expect: -w /usr/bin/runc[\s]+

Hosts

192.168.111.1

```
The command 'auditctl -l | grep /usr/bin/runc' returned :

sh: 1: auditctl: not found
```

1.2.2 Ensure that the version of Docker is up to date

Info

Frequent releases for Docker are issued which address security vulnerabilities, resolve product bugs and bring in new functionality. You should keep a tab on these product updates and upgrade as frequently as possible in line with the general IT security policy of your organization.

Rationale:

By staying up to date on Docker updates, vulnerabilities in the software can be mitigated. An experienced attacker may be able to exploit known vulnerabilities resulting in them being able to attain inappropriate access or to elevate their privileges. If you do not ensure that Docker is running at the most current release consistent with the requirements of of your application, you may introduce unwanted behaviour and it is therefore important to ensure that you monitor software versions and upgrade in a timely fashion.

Impact:

You should perform a risk assessment regarding Docker version updates and review how they may impact your operations. You should be aware that third-party products that use Docker may require older major versions of Docker to be supported, and this should be reviewed in line with the general IT security policy of your organization, particularly where security vulnerabilities in older versions have been publicly disclosed.

Solution

You should monitor versions of Docker releases and make sure your software is updated as required.

Default Value:

Not Applicable

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.14.1
800-53	SI-2c.
800-53R5	SI-2c.
CN-L3	8.1.4.4(e)
CN-L3	8.1.10.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.5.4.1(b)
CN-L3	8.5.4.1(d)
CN-L3	8.5.4.1(e)
CSCV7	3
CSCV8	16.5
CSF	ID.RA-1

CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1M
LEVEL	2M
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39
NIAV2	SS14b
PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.3
QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: docker version --format '{{ .Server.Version }}'

expect: 19.[0-9]+.[0-9]+

Hosts

192.168.111.1

```
The command 'docker version --format '{{ .Server.Version }}'' returned :

25.0.3
```

1.3.1 Ensure AIDE is installed - aide

Info

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

Rationale:

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

Solution

Install AIDE using the appropriate package manager or manual installation:

apt install aide aide-common

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

Run the following commands to initialize AIDE:

aideinit # mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db

Additional Information:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

1.3.1 Ensure AIDE is installed - aide-common

Info

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

Rationale:

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

Solution

Install AIDE using the appropriate package manager or manual installation:

apt install aide aide-common

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

Run the following commands to initialize AIDE:

aideinit # mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db

Additional Information:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

1.3.2 Ensure filesystem integrity is regularly checked

Info

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

Rationale:

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

Solution

If cron will be used to schedule and run aide check:

Run the following command:

crontab -u root -e

Add the following line to the crontab:

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

OR If aidecheck.service and aidecheck.timer will be used to schedule and run aide check:

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

[Unit] Description=Aide Check

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

[Install] WantedBy=multi-user.target

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

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

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

[Install] WantedBy=multi-user.target

Run the following commands:

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

systemctl daemon-reload

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1

800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^([^# \r]+\h+)?(\/usr\/s?bin\/|^\h*)aide(\.wrapper)?\h+(--check|([^# \r]+\h+)?\$AIDEARGS)\b file: /etc/cron.daily/* /etc/cron.hourly/* /etc/cron.monthly/* /etc/cron.weekly/* /var/spool/cron/* /etc/crontab min_occurrences: 1 regex: ^([^# \r]+\h+)?(\/usr\/s?bin\/|^\h*)aide(\.wrapper)?\h+(--check|([^# \r]+\h+)?\$AIDEARGS)\b string_required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

1.4.1 Ensure bootloader password is set - 'passwd_pbkdf2'

Info

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

Rationale:

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

Impact:

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

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

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

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

Solution

Create an encrypted password with grub-mkpasswd-pbkdf2:

grub-mkpasswd-pbkdf2

Enter password: <password>

Reenter password: <password>

PBKDF2 hash of your password is <encrypted-password>

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

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

password_pbkdf2 <username> <encrypted-password>

EOF

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

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

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

Run the following command to update the grub2 configuration:

update-grub

Default Value:

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

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

1.4.1 Ensure bootloader password is set - 'set superusers'

Info

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

Rationale:

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

Impact:

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

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

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

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

Solution

Create an encrypted password with grub-mkpasswd-pbkdf2:

grub-mkpasswd-pbkdf2

Enter password: <password>

Reenter password: <password>

PBKDF2 hash of your password is <encrypted-password>

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

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

password_pbkdf2 <username> <encrypted-password>

EOF

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

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

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

Run the following command to update the grub2 configuration:

update-grub

Default Value:

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

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

1.4.2 Ensure permissions on bootloader config are configured

Info

The grub configuration file contains information on boot settings and passwords for unlocking boot options.

Rationale:

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

Solution

Run the following commands to set permissions on your grub configuration:

chown root:root /boot/grub/grub.cfg # chmod u-wx,go-rwx /boot/grub/grub.cfg

Additional Information:

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

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

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /boot/grub/grub.cfg group: root mask: 377 owner: root system: Linux

Hosts

192.168.111.1

```
The file /boot/grub/grub.cfg with fmode owner: root group: root mode: 0444 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 377 uneven
 permissions : FALSE

/boot/grub/grub.cfg
```

1.5.4 Ensure core dumps are restricted - limits config

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

IF systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1005, T1005.000

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

1.5.4 Ensure core dumps are restricted - sysctl config

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

IF systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1005, T1005.000

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
800-171	3.4.6
800-171	3.4.7
800-53	AC-6(10)
800-53	CM-7
800-53R5	AC-6(10)
800-53R5	CM-7
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
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ITSG-33	AC-6
ITSG-33	CM-7
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	SS15a
NIAV2	SS15c
PCI-DSSV3.2.1	2.2.2
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	2.3
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

1.7.2 Ensure local login warning banner is configured properly - banner

Info

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

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

Rationale:

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

Solution

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

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1082, T1082.000, T1592, T1592.004

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.9
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8

LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
First ERROR: Ubuntu 22.04.3 != Authorized uses
Ubuntu 22.04.3 LTS \n \l
```

1.7.3 Ensure remote login warning banner is configured properly - banner

Info

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

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

Rationale:

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

Solution

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

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1018, T1018.000, T1082, T1082.000, T1592, T1592.004

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.9
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8

LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
First ERROR: Ubuntu 22.04.3 != Authorized uses
Ubuntu 22.04.3 LTS
```

2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver - NTP

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.

Rationale:

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 or create a file in /etc/systemd/timesyncd.conf.d ending in .conf and add the NTP= and/or FallbackNTP= lines to the [Time] section:

Example:

[Time] NTP=time.nist.gov # Uses the generic name for NIST's time servers

-AND/OR- FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov # Space separated list of NIST time servers

Note: Servers added to these line(s) should follow local site policy. NIST servers are for example. The timesyncd.conf.d directory may need to be created Example script: The following example script will create the systemd-timesyncd drop-in configuration snippet:

#!/usr/bin/env bash

ntp_ts='time.nist.gov'

ntp_fb='time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov'

disfile='/etc/systemd/timesyncd.conf.d/50-timesyncd.conf'

if ! find /etc/systemd -type f -name '*.conf' -exec grep -Ph '^h*NTP=H+' {} +; then [! -d /etc/systemd/timesyncd.conf.d] && mkdir /etc/systemd/timesyncd.conf.d ! grep -Pqs '^h*[Time]' '$disfile' && echo '[Time]' >> '$disfile'

echo 'NTP=$ntp_ts' >> '$disfile'

fi if ! find /etc/systemd -type f -name '*.conf' -exec grep -Ph '^h*FallbackNTP=H+' {} +; then [! -d /etc/systemd/timesyncd.conf.d] && mkdir /etc/systemd/timesyncd.conf.d ! grep -Pqs '^h*[Time]' '$disfile' && echo '[Time]' >> '$disfile'

echo 'FallbackNTP=$ntp_fb' >> '$disfile'

fi

Run the following command to reload the systemd-timesyncd configuration:

systemctl try-reload-or-restart systemd-timesyncd

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

Default Value:

#NTP=

#FallbackNPT=

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^NTP[\s]*=0.pool.ntp.org file: /etc/systemd/timesyncd.conf regex: ^NTP[\s]*= system: Linux

Hosts

192.168.111.1

```
Non-compliant file(s):
      /etc/systemd/timesyncd.conf - regex '^NTP[\s]*=' found - expect '^NTP[\s]*=0.pool.ntp.org' not
 found in the following lines:
         15: NTP=time1.keen.fsnets.com time2.keen.fsnets.com
```

2.2.16 Ensure rsync service is either not installed or masked

Info

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

Rationale:

The rsync service presents a security risk as it uses unencrypted protocols for communication. The rsync package should be removed to reduce the attack area of the system.

Solution

Run the following command to remove rsync:

apt purge rsync

OR Run the following commands to stop and mask rsync:

systemctl stop rsync

systemctl mask rsync

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - rsync service install check
The command '/usr/bin/dpkg -s rsync | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed

-------------------------
FAILED - rsync service masking check
The command '/usr/bin/systemctl is-enabled rsync | /usr/bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

enabled
```

2.3.4 Ensure telnet client is not installed

Info

The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

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.

Solution

Uninstall telnet:

apt purge telnet

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s telnet 2>&1 expect: (?:(^[\s]*dpkg-query: package 'telnet' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$)) system: Linux

Hosts

192.168.111.1

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

Package: telnet
Status: install ok installed
Priority: standard
Section: net
Installed-Size: 154
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Source: netkit-telnet
Version: 0.17-44build1
Replaces: netstd
Provides: telnet-client
Depends: libc6 (>= 2.34), libstdc++6 (>= 5), netbase
Description: basic telnet client
 The telnet command is used for interactive communication with another host
 using the TELNET protocol.
 .
 For the purpose of remote login, the present client executable should be
 depreciated in favour of an ssh-client, or in some cases with variants like
 telnet-ssl or Kerberized TELNET clients.  The most important reason is that
 this implementation exchanges user name and password in clear text.
 .
 On the other hand, the present program does satisfy common use cases of
 network diagnostics, like protocol testing of SMTP services, so it can
 become handy enough.
Homepage: http://www.hcs.harvard.edu/~dholland/computers/netkit.html
Original-Maintainer: Debian QA Group <packages@qa.debian.org>
```

2.8 Enable user namespace support --userns-remap=default

Info

Enable user namespace support in Docker daemon to utilize container user to host user re-mapping. This recommendation is beneficial where containers you are using do not have an explicit container user defined in the container image. If container images that you are using have a pre-defined non-root user, this recommendation may be skipped since this feature is still in its infancy and might give you unpredictable issues and complexities.

Rationale:

The Linux kernel user namespace support in Docker daemon provides additional security for the Docker host system. It allows a container to have a unique range of user and group IDs which are outside the traditional user and group range utilized by the host system.

For example, the root user will have expected administrative privilege inside the container but can effectively be mapped to an unprivileged UID on the host system.

Solution

Please consult Docker documentation for various ways in which this can be configured depending upon your requirements. Your steps might also vary based on platform - For example, on Red Hat, sub-UIDs and sub-GIDs mapping creation does not work automatically. You might have to create your own mapping.

However, the high-level steps are as below:

Step 1: Ensure that the files /etc/subuid and /etc/subgid exist.

touch /etc/subuid /etc/subgid Step 2: Start the docker daemon with --userns-remap flag dockerd --userns-remap=default Impact:

User namespace remapping makes quite a few Docker features incompatible and also currently breaks a few functionalities. Check out the Docker documentation and referenced links for details.

Default Value:

By default, user namespace is not remapped.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.13.1
800-171	3.13.5
800-53	SC-7a.
800-53R5	SC-7a.
CN-L3	8.1.10.6(j)
CSCV6	18
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5

CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7a.
LEVEL	2A
NESA	T3.4.1
NESA	T3.6.3
NESA	T4.2.1
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
PCI-DSSV3.2.1	1.1
PCI-DSSV3.2.1	1.2
PCI-DSSV3.2.1	1.2.1
PCI-DSSV3.2.1	1.3
PCI-DSSV4.0	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: ps -ef | grep docker | grep [-][-]userns-remap=default expect: --userns-remap=default

Hosts

192.168.111.1

```
The command 'ps -ef | grep docker | grep [-][-]userns-remap=default' did not return any result
```

2.9 Enable user namespace support - SecurityOptions

Info

You should enable user namespace support in Docker daemon to utilize container user to host user re-mapping. This recommendation is beneficial where the containers you are using do not have an explicit container user defined in the container image. If the container images that you are using have a pre-defined non-root user, this recommendation may be skipped as this feature is still in its infancy, and might result in unpredictable issues or difficulty in configuration.

Rationale:

The Linux kernel 'user namespace' support within the Docker daemon provides additional security for the Docker host system. It allows a container to have a unique range of user and group IDs which are outside the traditional user and group range utilized by the host system.

For example, the root user can have the expected administrative privileges inside the container but can effectively be mapped to an unprivileged UID on the host system.

Impact:

User namespace remapping is incompatible with a number of Docker features and also currently breaks some of its functionalities. Reference the Docker documentation and included links for details.

Solution

Please consult the Docker documentation for various ways in which this can be configured depending upon your requirements. Your steps might also vary based on platform - For example, on Red Hat, sub-UIDs and sub-GIDs mapping creation do not work automatically. You might have to create your own mapping.

The high-level steps are as below:

Step 1: Ensure that the files /etc/subuid and /etc/subgid exist.

touch /etc/subuid /etc/subgid

Step 2: Start the docker daemon with --userns-remap flag

dockerd --userns-remap=default

Default Value:

By default, user namespace is not remapped. Consideration should be given to implementing this in line with the requirements of the applications being used and the organization's security policy.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-171	3.13.2
800-53	SA-8

800-53R5	SA-8
CSCV7	18
CSCV8	6
CSF	PR.IP-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SA-8
ITSG-33	SA-8a.
LEVEL	2M
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.6.5
NIAV2	SS3
NIAV2	VL2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: docker info --format '{{ .SecurityOptions }}'

expect: name=userns

Hosts

192.168.111.1

```
The command 'docker info --format '{{ .SecurityOptions }}'' returned :

[name=apparmor name=seccomp,profile=builtin name=cgroupns]
```

2.11 Ensure that authorization for Docker client commands is enabled

Info

Use native Docker authorization plugins or a third party authorization mechanism with Docker daemon to manage access to Docker client commands.

Rationale:

Dockers out-of-the-box authorization model is all or nothing. Any user with permission to access the Docker daemon can run any Docker client command. The same is true for callers using Dockers remote API to contact the daemon. If you require greater access control, you can create authorization plugins and add them to your Docker daemon configuration. Using an authorization plugin, a Docker administrator can configure granular access policies for managing access to Docker daemon.

Third party integrations of Docker may implement their own authorization models to require authorization with the Docker daemon outside of docker's native authorization plugin (i.e. Kubernetes, Cloud Foundry, Openshift).

Solution

Step 1: Install/Create an authorization plugin.

Step 2: Configure the authorization policy as desired.

Step 3: Start the docker daemon as below:

dockerd --authorization-plugin=<PLUGIN_ID>

Impact:

Each docker command specifically passes through authorization plugin mechanism. This might introduce a slight performance drop.

Third party use of alternative container engines that utilize the docker daemon may provide alternative mechanisms to provide this security control.

Default Value:

By default, authorization plugins are not set up.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.5.1
800-53	IA-2
800-53R5	IA-2
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSCV6	16

CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2
ITSG-33	IA-2a.
LEVEL	2A
NESA	T2.3.8
NESA	T5.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
NESA	T5.5.3
NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: ps -ef | grep docker | grep [-][-]authorization-plugin expect: authorization-plugin=1234

Hosts

192.168.111.1

```
The command 'ps -ef | grep docker | grep [-][-]authorization-plugin' did not return any result
```

2.12 Ensure centralized and remote logging is configured

Info

Docker now supports various log drivers. A preferable way to store logs is the one that supports centralized and remote logging.

Rationale:

Centralized and remote logging ensures that all important log records are safe despite catastrophic events. Docker now supports various such logging drivers. Use the one that suits your environment the best.

Solution

Step 1: Setup the desired log driver by following its documentation.

Step 2: Start the docker daemon with that logging driver.

For example, dockerd --log-driver=syslog --log-opt syslog-address=tcp://192.xxx.xxx.xxx Impact:

None.

Default Value:

By default, container logs are maintained as json files

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.3.8
800-53	AU-9(2)
800-53R5	AU-9(2)
CN-L3	8.1.3.5(d)
CN-L3	8.1.4.3(c)
CSCV6	6.6
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9(2)
LEVEL	2A
NESA	M5.2.3
NESA	M5.5.2
NIAV2	SS13e
PCI-DSSV3.2.1	10.5.3
PCI-DSSV3.2.1	10.5.4
PCI-DSSV4.0	10.3.3

QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: ps -ef | grep docker | grep [-][-]log-driver expect: log-driver=syslog

Hosts

192.168.111.1

```
The command 'ps -ef | grep docker | grep [-][-]log-driver' did not return any result
```

2.12 Ensure that authorization for Docker client commands is enabled

Info

You should use native Docker authorization plugins or a third party authorization mechanism with the Docker daemon to manage access to Docker client commands.

Rationale:

Docker's out-of-the-box authorization model is currently 'all or nothing'. This means that any user with permission to access the Docker daemon can run any Docker client command. The same is true for remote users accessing Docker's API to contact the daemon. If you require greater access control, you can create authorization plugins and add them to your Docker daemon configuration. Using an authorization plugin, a Docker administrator can configure granular access policies for managing access to the Docker daemon.

Third party integrations of Docker may implement their own authorization models to require authorization with the Docker daemon outside of docker's native authorization plugin (i.e. Kubernetes, Cloud Foundry, Openshift).

Impact:

Each Docker command needs to pass through the authorization plugin mechanism. This may have a performance impact.

It may be possible to use alternative mechanisms that do not have this performance hit.

Solution

Step 1: Install/Create an authorization plugin.

Step 2: Configure the authorization policy as desired.

Step 3: Start the docker daemon as below:

dockerd --authorization-plugin=<PLUGIN_ID>

Default Value:

By default, authorization plugins are not set up.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV8	6
CSF	DE.CM-1

CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	2M
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

FAILED

Hosts

192.168.111.1

2.13 Ensure centralized and remote logging is configured

Info

Docker supports various logging mechanisms. A preferable method for storing logs is one that supports centralized and remote management.

Rationale:

Centralized and remote logging ensures that all important log records are safe even in the event of a major data availability issue . Docker supports various logging methods and you should use the one that best corresponds to your IT security policy.

Impact:

None.

Solution

Step 1: Set up the desired log driver following its documentation.

Step 2: Start the docker daemon using that logging driver.

For example:

dockerd --log-driver=syslog --log-opt syslog-address=tcp://192.xxx.xxx.xxx

Default Value:

By default, container logs are maintained as json files

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.5
800-53	AU-1
800-53	AU-2
800-53	AU-6(3)
800-53R5	AU-1
800-53R5	AU-2
800-53R5	AU-6(3)
CN-L3	7.1.3.3(d)
CN-L3	8.1.4.3(a)
CSCV7	6.6
CSCV7	6.8

CSCV8	8.1
CSCV8	8.9
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-1
ITSG-33	AU-2
ITSG-33	AU-6(3)
LEVEL	2M
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	10.8
QCSC-V1	5.2.3
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: docker info --format '{{ .LoggingDriver }}'

expect: syslog

Hosts

192.168.111.1

```
The command 'docker info --format '{{ .LoggingDriver }}'' returned :

json-file
```

2.17 Ensure that a daemon-wide custom seccomp profile is applied if appropriate

Info

You can choose to apply a custom seccomp profile at a daemon-wide level if needed with this overriding Docker's default seccomp profile.

Rationale:

A large number of system calls are exposed to every userland process with many of them not utilized during the entire lifetime of the process. Many applications do not need all these system calls and therefore benefit by having each system call currently in use reviewed in line with organizational security policy. A reduced set of system calls reduces the total kernel surface exposed to the application and therefore improves application security.

A custom seccomp profile can be applied instead of Docker's default seccomp profile. Alternatively, if Docker's default profile is adequate for your environment, you can choose to ignore this recommendation.

Impact:

A misconfigured seccomp profile could possibly interrupt your container environment. Docker-default blocked calls have been carefully scrutinized and address some critical vulnerabilities/issues within container environments (for example, kernel key ring calls). You should therefore exercise extreme care if you choose to override the default settings.

Solution

By default, Docker's default seccomp profile is applied. If this is adequate for your environment, no action is necessary. Alternatively, if you choose to apply your own seccomp profile, use the --seccomp-profile flag at daemon start or put it in the daemon runtime parameters file.

dockerd --seccomp-profile </path/to/seccomp/profile>

Default Value:

By default, Docker applies a default seccomp profile.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-171	3.13.2
800-53	SA-8
800-53R5	SA-8
CSCV7	18
CSCV8	16
CSF	PR.IP-2

GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SA-8
ITSG-33	SA-8a.
LEVEL	2M
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.6.5
NIAV2	SS3
NIAV2	VL2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: docker info --format '{{ .SecurityOptions }}'

expect: name=seccomp,profile=none

Hosts

192.168.111.1

```
The command 'docker info --format '{{ .SecurityOptions }}'' returned :

[name=apparmor name=seccomp,profile=builtin name=cgroupns]
```

3.2.1 Ensure packet redirect sending is disabled - net.ipv4.conf.all.send_redirects (sysctl.conf/sysctl.d)

Info

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

Rationale:

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

Solution

Run the following script to set:

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.send_redirects = 1

net.ipv4.conf.default.send_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*net\.ipv4\.conf\.all\.send_redirects[\s]*=[\s]*0[\s]*$ file: /etc/sysctl.conf /etc/sysctl.d/* min_occurrences: 1 regex: ^[\s]*net\.ipv4\.conf\.all\.send_redirects[\s]* string_required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

3.2.1 Ensure packet redirect sending is disabled - net.ipv4.conf.default.send_redirects (sysctl.conf/sysctl.d)

Info

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

Rationale:

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

Solution

Run the following script to set:

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.send_redirects = 1

net.ipv4.conf.default.send_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*net\.ipv4\.conf\.default\.send_redirects[\s]*=[\s]*0[\s]*$ file: /etc/sysctl.conf /etc/sysctl.d/* min_occurrences: 1 regex: ^[\s]*net\.ipv4\.conf\.default\.send_redirects[\s]* string_required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

3.2.1 Ensure packet redirect sending is disabled - sysctl net.ipv4.conf.default.send_redirects

Info

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

Rationale:

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

Solution

Run the following script to set:

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.send_redirects = 1

net.ipv4.conf.default.send_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.2.2 Ensure IP forwarding is disabled - sysctl ipv4

Info

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

Rationale:

Setting:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

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

Solution

Run the following script to set:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.ip_forward=0 net.ipv6.conf.all.forwarding=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv4.ip_forward' returned :

net.ipv4.ip_forward = 1
```

3.3.1 Ensure source routed packets are not accepted - net.ipv4.conf.all.accept_source_route (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.1 Ensure source routed packets are not accepted - net.ipv4.conf.default.accept_source_route (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.1 Ensure source routed packets are not accepted - net.ipv6.conf.all.accept_source_route (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.1 Ensure source routed packets are not accepted - net.ipv6.conf.default.accept_source_route (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.2 Ensure ICMP redirects are not accepted - net.ipv4.conf.all.accept_redirects (sysctl.conf/sysctl.d)

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.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

```
fail
```

3.3.2 Ensure ICMP redirects are not accepted - net.ipv4.conf.default.accept_redirects (sysctl.conf/sysctl.d)

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.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

```
fail
```

3.3.2 Ensure ICMP redirects are not accepted - net.ipv6.conf.all.accept_redirects (sysctl.conf/sysctl.d)

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.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

```
fail
```

3.3.2 Ensure ICMP redirects are not accepted - net.ipv6.conf.default.accept_redirects (sysctl.conf/sysctl.d)

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.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

```
fail
```

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

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.2 Ensure ICMP redirects are not accepted - sysctl net.ipv6.conf.all.accept_redirects

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

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

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.all.secure_redirects' (sysctl.conf/sysctl.d)

Info

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

Rationale:

It is still possible for even known gateways to be compromised.

Setting:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

protects the system from routing table updates by possibly compromised known gateways.

Solution

Run the following script to set:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

#!/usr/bin/env bash

kernel_parameter_fix() { l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'
sysctl -w '$l_kpname=$l_kpvalue'
sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.default.secure_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.default.secure_redirects' (sysctl.conf/sysctl.d)

Info

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

Rationale:

It is still possible for even known gateways to be compromised.

Setting:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

protects the system from routing table updates by possibly compromised known gateways.

Solution

Run the following script to set:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

#!/usr/bin/env bash

kernel_parameter_fix() { l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'
sysctl -w '$l_kpname=$l_kpvalue'
sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.default.secure_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.3 Ensure secure ICMP redirects are not accepted - 'sysctl net.ipv4.conf.all.secure_redirects'

Info

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

Rationale:

It is still possible for even known gateways to be compromised.

Setting:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

protects the system from routing table updates by possibly compromised known gateways.

Solution

Run the following script to set:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

#!/usr/bin/env bash

kernel_parameter_fix() { l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'
sysctl -w '$l_kpname=$l_kpvalue'
sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.default.secure_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.3 Ensure secure ICMP redirects are not accepted - 'sysctl net.ipv4.conf.default.secure_redirects'

Info

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

Rationale:

It is still possible for even known gateways to be compromised.

Setting:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

protects the system from routing table updates by possibly compromised known gateways.

Solution

Run the following script to set:

net.ipv4.conf.default.secure_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

#!/usr/bin/env bash

kernel_parameter_fix() { l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'
sysctl -w '$l_kpname=$l_kpvalue'
sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.default.secure_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.4 Ensure suspicious packets are logged - 'net.ipv4.conf.all.log_martians' (sysctl.conf/sysctl.d)

Info

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

Rationale:

Enabling this feature and logging these packets by setting:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Solution

Run the following script to set:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.log_martians = 0

net.ipv4.conf.default.log_martians = 0

Additional Information:

NIST SP 800-53 Rev. 5:

AU-3

AU-3(1)

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.4 Ensure suspicious packets are logged - 'net.ipv4.conf.default.log_martians' (sysctl.conf/sysctl.d)

Info

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

Rationale:

Enabling this feature and logging these packets by setting:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Solution

Run the following script to set:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.log_martians = 0

net.ipv4.conf.default.log_martians = 0

Additional Information:

NIST SP 800-53 Rev. 5:

AU-3

AU-3(1)

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.4 Ensure suspicious packets are logged - 'sysctl net.ipv4.conf.all.log_martians'

Info

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

Rationale:

Enabling this feature and logging these packets by setting:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Solution

Run the following script to set:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.log_martians = 0

net.ipv4.conf.default.log_martians = 0

Additional Information:

NIST SP 800-53 Rev. 5:

AU-3

AU-3(1)

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.4 Ensure suspicious packets are logged - 'sysctl net.ipv4.conf.default.log_martians'

Info

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

Rationale:

Enabling this feature and logging these packets by setting:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Solution

Run the following script to set:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'
fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.conf.all.log_martians = 0

net.ipv4.conf.default.log_martians = 0

Additional Information:

NIST SP 800-53 Rev. 5:

AU-3

AU-3(1)

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.5 Ensure broadcast ICMP requests are ignored - sysctl.conf/sysctl.d

Info

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

Rationale:

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

Solution

Run the following script to set net.ipv4.icmp_echo_ignore_broadcasts = 1:

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.icmp_echo_ignore_broadcasts=1'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.default.log_martians = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(net\.ipv4\.|net/ipv4/)icmp_echo_ignore_broadcasts[\s]*=[\s]*1[\s]* file: /run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf /etc/ufw/sysctl.conf min_occurrences: 1 regex: icmp_echo_ignore_broadcasts string_required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

3.3.6 Ensure bogus ICMP responses are ignored - (sysctl.conf/sysctl.d)

Info

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

Rationale:

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

Solution

Run the following script to set icmp_ignore_bogus_error_responses = 1:

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='icmp_ignore_bogus_error_responses=1'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.icmp_ignore_bogus_error_responses = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(net\.ipv4\.|net/ipv4/)icmp_ignore_bogus_error_responses[\s]*=[\s]*1[\s]* file: /run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf /etc/ufw/sysctl.conf min_occurrences: 1 regex: icmp_ignore_bogus_error_responses string_required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

3.3.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.all.rp_filter' (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 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.

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Run the following script to set:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.rp_filter = 2

net.ipv4.conf.default.rp_filter = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.default.rp_filter' (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 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.

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Run the following script to set:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.rp_filter = 2

net.ipv4.conf.default.rp_filter = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.7 Ensure Reverse Path Filtering is enabled - 'sysctl net.ipv4.conf.all.rp_filter'

Info

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

Rationale:

Setting:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 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.

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Run the following script to set:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.rp_filter = 2

net.ipv4.conf.default.rp_filter = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.7 Ensure Reverse Path Filtering is enabled - 'sysctl net.ipv4.conf.default.rp_filter'

Info

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

Rationale:

Setting:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 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.

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Run the following script to set:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.rp_filter = 2

net.ipv4.conf.default.rp_filter = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

net.ipv4.conf.default.rp_filter = 2
```

3.3.8 Ensure TCP SYN Cookies is enabled - sysctl.conf/sysctl.d

Info

When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. Setting net.ipv4.tcp_syncookies = 1 enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

Solution

Run the following script to set net.ipv4.tcp_syncookies = 1:

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.tcp_syncookies=1'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.tcp_syncookies = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.9 Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.all.accept_ra' (sysctl.conf/sysctl.d)

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Setting:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

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

Solution

Run the following script to set:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv6.conf.all.accept_ra = 1

net.ipv6.conf.default.accept_ra = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6

800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.9 Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.default.accept_ra' (sysctl.conf/sysctl.d)

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Setting:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

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

Solution

Run the following script to set:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv6.conf.all.accept_ra = 1

net.ipv6.conf.default.accept_ra = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6

800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

3.3.9 Ensure IPv6 router advertisements are not accepted - 'sysctl net.ipv6.conf.all.accept_ra'

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Setting:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

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

Solution

Run the following script to set:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv6.conf.all.accept_ra = 1

net.ipv6.conf.default.accept_ra = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6

800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_ra' returned :

net.ipv6.conf.all.accept_ra = 1
```

3.3.9 Ensure IPv6 router advertisements are not accepted - 'sysctl net.ipv6.conf.default.accept_ra'

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Setting:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

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

Solution

Run the following script to set:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv6.conf.all.accept_ra = 1

net.ipv6.conf.default.accept_ra = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6

800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.7 Ensure that registry certificate file ownership is set to root:root

Info

You should verify that all the registry certificate files (usually found under /etc/docker/certs.d/<registry-name> directory) are individually owned and group owned by root.

Rationale:

The /etc/docker/certs.d/<registry-name> directory contains Docker registry certificates. These certificate files must be individually owned and group owned by root to ensure that less privileged users are unable to modify the contents of the directory.

Impact:

None.

Solution

The following command could be executed:

chown root:root /etc/docker/certs.d/<registry-name>/*

This would set the individual ownership and group ownership for the registry certificate files to root.

Default Value:

By default, the individual ownership and group ownership for registry certificate files is correctly set to root.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1M
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/certs.d/* group: root owner: root

Hosts

192.168.111.1

```
No files found: /etc/docker/certs.d/*
```

3.8 Ensure that registry certificate file permissions are set to 444 or more restrictively

Info

You should verify that all the registry certificate files (usually found under /etc/docker/certs.d/<registry-name> directory) have permissions of 444 or are set more restrictively.

Note that, by default, this directory might not exist if no registry certificate files are in place.

Rationale:

The /etc/docker/certs.d/<registry-name> directory contains Docker registry certificates. These certificate files must have permissions of 444or more restrictive permissions in order to ensure that unprivileged users do not have full access to them..

Impact:

None.

Solution

You should execute the following command:

find /etc/docker/certs.d/ -type f -exec chmod 0444 {} ;

This would set the permissions for the registry certificate files to 444.

Default Value:

By default, the permissions for registry certificate files might not be 444. The default file permissions are governed by the system or user specific umask values which are defined within the operating system itself.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/certs.d/* mask: 333

Hosts

192.168.111.1

```
No files found: /etc/docker/certs.d/*
```

3.9 Ensure that TLS CA certificate file ownership is set to root:root

Info

You should verify that the TLS CA certificate file (the file that is passed along with the --tlscacert parameter) is individually owned and group owned by root.

Rationale:

The TLS CA certificate file should be protected from any tampering. It is used to authenticate the Docker server based on a given CA certificate. It must be therefore be individually owned and group owned by root to ensure that it cannot be modified by less privileged users.

Impact:

None.

Solution

You should execute the following command:

chown root:root <path to TLS CA certificate file>

This sets the individual ownership and group ownership for the TLS CA certificate file to root.

Default Value:

By default, the ownership and group-ownership for TLS CA certificate file is correctly set to root.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1M
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/certs.d/CA_CERT group: root owner: root

Hosts

192.168.111.1

```
No files found: /etc/docker/certs.d/CA_CERT
```

3.10 Ensure that TLS CA certificate file permissions are set to 444 or more restrictively

Info

You should verify that the TLS CA certificate file (the file that is passed along with the --tlscacert parameter) has permissions of 444 or is set more restrictively.

Rationale:

The TLS CA certificate file should be protected from any tampering. It is used to authenticate the Docker server based on a given CA certificate. It must therefore have permissions of 444, or more restrictive permissions to ensure that the file cannot be modified by a less privileged user.

Impact:

None.

Solution

You should execute the following command:

chmod 444 <path to TLS CA certificate file>

This sets the file permissions on the TLS CA file to 444.

Default Value:

By default, the permissions for the TLS CA certificate file might not be 444. The default file permissions are governed by the operating system or user specific umask values.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/certs.d/CA_CERT mask: 333

Hosts

192.168.111.1

```
No files found: /etc/docker/certs.d/CA_CERT
```

3.11 Ensure that Docker server certificate file ownership is set to root:root

Info

You should verify that the Docker server certificate file (the file that is passed along with the --tlscert parameter) is individual owned and group owned by root.

Rationale:

The Docker server certificate file should be protected from any tampering. It is used to authenticate the Docker server based on the given server certificate. It must therefore be individually owned and group owned by root to prevent modification by less privileged users.

Impact:

None.

Solution

You should run the following command:

chown root:root <path to Docker server certificate file>

This sets the individual ownership and the group ownership for the Docker server certificate file to root.

Default Value:

By default, the ownership and group-ownership for Docker server certificate file is correctly set to root.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1M
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/certs.d/DOCKER_SERVER_CERT group: root owner: root

Hosts

192.168.111.1

```
No files found: /etc/docker/certs.d/DOCKER_SERVER_CERT
```

3.12 Ensure that the Docker server certificate file permissions are set to 444 or more restrictively

Info

You should verify that the Docker server certificate file (the file that is passed along with the --tlscert parameter) has permissions of 444 or more restrictive permissions.

Rationale:

The Docker server certificate file should be protected from any tampering. It is used to authenticate the Docker server based on the given server certificate. It should therefore have permissions of 444 to prevent its modification.

Impact:

None.

Solution

You should execute the command below:

chmod 444 <path to Docker server certificate file>

This sets the file permissions of the Docker server certificate file to 444.

Default Value:

By default, the permissions for the Docker server certificate file might not be 444. The default file permissions are governed by the operating system or user specific umask values.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/certs.d/DOCKER_SERVER_CERT mask: 333

Hosts

192.168.111.1

```
No files found: /etc/docker/certs.d/DOCKER_SERVER_CERT
```

4.1.4.1 Ensure audit log files are mode 0640 or less permissive

Info

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Solution

Run the following command to remove more permissive mode than 0640 from audit log files:

find '$(dirname $(awk -F'=' '/^s*log_files*=s*/ {print $2}' /etc/audit/auditd.conf | xargs))' -type f (! -perm 600 -a ! -perm 0400 -a ! -perm 0200 -a ! -perm 0000 -a ! -perm 0640 -a ! -perm 0440 -a ! -perm 0040) -exec chmod u-x,g-wx,o-rwx {} +

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/stat -Lc "%n %a" "$(dirname $(awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /etc/audit/auditd.conf | xargs))"/* | /bin/grep -v '[0,2,4,6][0,4]0' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/stat -Lc "%n %a" "$(dirname $( awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /
etc/audit/auditd.conf | xargs))"/* | /bin/grep -v '[0,2,4,6][0,4]0' | /usr/bin/awk '{print} END
 { if(NR==0) print "pass" ; else print "fail"}'' returned :

awk: fatal: cannot open file `/etc/audit/auditd.conf' for reading: No such file or directory
dirname: missing operand
Try 'dirname --help' for more information.
/benchmark 755
/bin 755
/boot 755
/cores 755
/dev 755
/etc 755
/home 755
/initrd.img 644
/initrd.img.old 644
/lib 755
/lib32 755
/lib64 755
/libx32 755
/lost+found 700
/media 755
/mnt 755
/opt 755
/proc 555
/root 700
/run 755
/sbin 755
/srv 755
/sys 555
/tmp 1777
/usr 755
/var 755
fail
```

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - auditctl

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for '/etc/aide/aide.conf' to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(/usr)?/sbin/auditctl[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 file: /etc/aide/aide.conf
regex: ^[\s]*(/usr)?/sbin/auditctl[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 system: Linux

Hosts

192.168.111.1

```
No files found: /etc/aide/aide.conf
```

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - auditd

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for '/etc/aide/aide.conf' to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(/usr)?/sbin/auditd[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 file: /etc/aide/aide.conf regex: ^[\s]*(/usr)?/sbin/auditd[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 system: Linux

Hosts

192.168.111.1

```
No files found: /etc/aide/aide.conf
```

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - augenrules

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for '/etc/aide/aide.conf' to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(/usr)?/sbin/augenrules[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 file: /etc/aide/aide.conf regex: ^[\s]*(/usr)?/sbin/augenrules[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 system: Linux

Hosts

192.168.111.1

```
No files found: /etc/aide/aide.conf
```

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - aureport

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for '/etc/aide/aide.conf' to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(/usr)?/sbin/aureport[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 file: /etc/aide/aide.conf regex: ^[\s]*(/usr)?/sbin/aureport[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 system: Linux

Hosts

192.168.111.1

```
No files found: /etc/aide/aide.conf
```

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - ausearch

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for '/etc/aide/aide.conf' to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(/usr)?/sbin/ausearch[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 file: /etc/aide/aide.conf regex: ^[\s]*(/usr)?/sbin/ausearch[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 system: Linux

Hosts

192.168.111.1

```
No files found: /etc/aide/aide.conf
```

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools - autrace

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for '/etc/aide/aide.conf' to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*(/usr)?/sbin/autrace[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 file: /etc/aide/aide.conf
regex: ^[\s]*(/usr)?/sbin/autrace[\s]+p\+i\+n\+u\+g\+s\+b\+acl\+xattrs\+sha512 system: Linux

Hosts

192.168.111.1

```
No files found: /etc/aide/aide.conf
```

4.2.1.1.2 Ensure systemd-journal-remote is configured

Info

Journald (via 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.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Solution

Edit the /etc/systemd/journal-upload.conf file and ensure the following lines are set per your environment:

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

Restart the service:

systemctl restart systemd-journal-upload

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - URL
The file "/etc/systemd/journal-upload.conf" does not contain "^[\s]*URL[\s]*=[\s]*.*"

-------------------------
FAILED - Key
The file "/etc/systemd/journal-upload.conf" does not contain "^[\s]*ServerKeyFile[\s]*=[\s]*.*"
```

```
-------------------------
FAILED - Cert
The file "/etc/systemd/journal-upload.conf" does not contain
 "^[\s]*ServerCertificateFile[\s]*=[\s]*.*"

-------------------------
FAILED - Trusted Cert
The file "/etc/systemd/journal-upload.conf" does not contain
 "^[\s]*TrustedCertificateFile[\s]*=[\s]*.*"
```

4.2.1.1.3 Ensure systemd-journal-remote is enabled

Info

Journald (via 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 centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Solution

Run the following command to enable systemd-journal-remote:

systemctl --now enable systemd-journal-upload.service

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl is-enabled systemd-journal-upload.service expect: enabled system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl is-enabled systemd-journal-upload.service' returned :

disabled
```

4.2.1.3 Ensure journald is configured to compress large log files

Info

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Solution

Edit the /etc/systemd/journald.conf file or a file ending in .conf in /etc/systemd/journald.conf.d/ and add the following line:

Compress=yes

Restart the service:

systemctl restart systemd-journald

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*Compress[\s]*=[\s]*['"]?yes['"]?[\s]*$ file: /etc/systemd/journald.conf /etc/systemd/journald.conf.d/* min_occurrences: 1 regex: ^[\s]*Compress[\s]*= required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

4.2.1.4 Ensure journald is configured to write logfiles to persistent disk

Info

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss due to a reboot.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Solution

Edit the /etc/systemd/journald.conf file or a file ending in .conf in /etc/systemd/journald.conf.d/ and add the following line:

Storage=persistent

Restart the service:

systemctl restart systemd-journald

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*Storage[\s]*=[\s]*['"]?persistent['"]?[\s]*$ file: /etc/systemd/journald.conf /etc/systemd/journald.conf.d/* min_occurrences: 1 regex: ^[\s]*Storage[\s]*= required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

4.2.2.3 Ensure journald is configured to send logs to rsyslog

Info

Data from journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of journald logs, however, use of the RSyslog service provides a consistent means of log collection and export.

Rationale:

IF RSyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

Solution

Edit the /etc/systemd/journald.conf file and add the following line:

ForwardToSyslog=yes

Restart the service:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.5
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-6(3)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*ForwardToSyslog[\s]*=[\s]*['"]?yes['"]?[\s]*$ file: /etc/systemd/journald.conf regex: ^[\s]*ForwardToSyslog[\s]*= system: Linux

Hosts

192.168.111.1

```
The file "/etc/systemd/journald.conf" does not contain "^[\s]*ForwardToSyslog[\s]*="
```

4.2.2.5 Ensure logging is configured

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment.

NOTE: The below configuration is shown for example purposes only. Due care should be given to how the organization wish 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 restart rsyslog

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
PASSED - '*.emerg :omusrmsg:*'
Compliant file(s):
      /etc/rsyslog.conf - regex not found
      /etc/rsyslog.d/21-cloudinit.conf - regex not found
      /etc/rsyslog.d/50-default.conf - regex '^[\s]*\*\.emerg' found - expect '\*\.emerg\s
+:omusrmsg:\*$' found in the following lines:
          39: *.emerg:omusrmsg:*

-------------------------
FAILED - 'auth,authpriv.* /var/log/secure'
Non-compliant file(s):
      /etc/rsyslog.d/50-default.conf - regex '^[\s]*auth,authpriv\.\*' found - expect 'auth,authpriv
\.\*[\s]+/var/log/secure[\s]*$' not found in the following lines:
          8: auth,authpriv.*/var/log/auth.log

-------------------------
FAILED - 'mail.* -/var/log/mail'
Non-compliant file(s):
      /etc/rsyslog.d/50-default.conf - regex '^[\s]*mail\.\*' found - expect 'mail\.\*[\s]+-/var/
log/mail[\s]*$' not found in the following lines:
          14: mail.*-/var/log/mail.log

-------------------------
FAILED - 'mail.info -/var/log/mail.info'
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - 'mail.warning -/var/log/mail.warn'
No matching files were found
Less than 1 matches of regex found

-------------------------
PASSED - 'mail.err /var/log/mail.err'
Compliant file(s):
      /etc/rsyslog.conf - regex not found
      /etc/rsyslog.d/21-cloudinit.conf - regex not found
      /etc/rsyslog.d/50-default.conf - regex '^[\s]*mail\.err' found - expect 'mail\.err[\s]+/var/
log/mail.err[\s]*$' found in the following lines:
          23: mail.err/var/log/mail.err

-------------------------
FAILED - 'cron.* /var/log/cron'
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - '*.=warning;*.=err -/var/log/warn'
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - '*.crit /var/log/warn'
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - ' [...]
```

4.2.2.6 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.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Solution

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add 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.

. action(type='omfwd' target='192.168.2.100' port='514' protocol='tcp'

action.resumeRetryCount='100'

queue.type='LinkedList' queue.size='1000')

Run the following command to reload the rsyslogd configuration:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - rsyslog old format
```

```
No matching files were found
Less than 1 matches of regex found

------------------------
FAILED - rsyslog new format
No matching files were found
Less than 1 matches of regex found
```

4.2.3 Ensure all logfiles have appropriate permissions and ownership

Info

Log files stored in /var/log/ contain logged information from many services on the system and potentially from other logged hosts as well.

Rationale:

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 is captured in the event that the remediation causes issues.

#!/usr/bin/env bash

{ l_op2='' l_output2=''

l_uidmin='$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)'

file_test_fix() { l_op2=''

l_fuser='root'

l_fgroup='root'

if [$(($l_mode & $perm_mask)) -gt 0]; then l_op2='$l_op2

- Mode: '$l_mode' should be '$maxperm' or more restrictive

- Removing excess permissions'

chmod '$l_rperms' '$l_fname'

fi if [[! '$l_user' =~ $l_auser]]; then l_op2='$l_op2

- Owned by: '$l_user' and should be owned by '${l_auser//|/ or }'

- Changing ownership to: '$l_fuser''

chown '$l_fuser' '$l_fname'

fi if [[! '$l_group' =~ $l_agroup]]; then l_op2='$l_op2

- Group owned by: '$l_group' and should be group owned by '${l_agroup//|/ or }'

- Changing group ownership to: '$l_fgroup''

chgrp '$l_fgroup' '$l_fname'

fi [-n '$l_op2'] && l_output2='$l_output2

- File: '$l_fname' is:$l_op2 '

} unset a_file && a_file=() # clear and initialize array # Loop to create array with stat of files that could possibly fail one of the audits while IFS= read -r -d $'0' l_file; do [-e '$l_file'] && a_file+=('$(stat -Lc '%n^ %#a^%U^%u^%G^%g' '$l_file')') done < <(find -L /var/log -type f (-perm /0137 -o ! -user root -o ! -group root) -print0) while IFS='^' read -r l_fname l_mode l_user l_uid l_group l_gid; do l_bname='$(basename '$l_fname')'

```
case '$l_bname' in lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-* | README)
perm_mask='0113'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='ug-x,o-wx'
l_auser='root'
l_agroup='(root|utmp)'
file_test_fix ;;
secure | auth.log | syslog | messages) perm_mask='0137'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='u-x,g-wx,o-rwx'
l_auser='(root|syslog)'
l_agroup='(root|adm)'
file_test_fix ;;
SSSD | sssd) perm_mask='0117'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='ug-x,o-rwx'
l_auser='(root|SSSD)'
l_agroup='(root|SSSD)'
file_test_fix ;;
gdm | gdm3) perm_mask='0117'
l_rperms='ug-x,o-rwx'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_auser='root'
l_agroup='(root|gdm|gdm3)'
file_test_fix ;;
*.journal | *.journal~) perm_mask='0137'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='u-x,g-wx,o-rwx'
l_auser='root'
l_agroup='(root|systemd-journal)'
file_test_fix ;;
*) perm_mask='0137'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='u-x,g-wx,o-rwx'
l_auser='(root|syslog)'
l_agroup='(root|adm)'
if [ '$l_uid' -lt '$l_uidmin' ] && [ -z '$(awk -v grp='$l_group' -F: '$1==grp {print $4}' /etc/group)' ]; then if [[ !
'$l_user' =~ $l_auser ]]; then l_auser='(root|syslog|$l_user)'
fi if [[ ! '$l_group' =~ $l_agroup ]]; then l_tst=''
while l_out3='' read -r l_duid; do [ '$l_duid' -ge '$l_uidmin' ] && l_tst=failed done <<< '$(awk -F:
'$4=='$l_gid'' {print $3}' /etc/passwd)'
```

['$l_tst' != 'failed'] && l_agroup='(root|adm|$l_group)'

fi fi file_test_fix ;;

esac done <<< '$(printf '%s ' '${a_file[@]}')'

unset a_file # Clear array # If all files passed, then we report no changes if [-z '$l_output2']; then echo -e '- All files in '/var/log/' have appropriate permissions and ownership

- No changes required '

else # print report of changes echo -e '

$l_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 access configured.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command script with multiple lines returned :

- Audit Results:
 ** Fail **

 - File: "/var/log/alternatives.log.1" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/alternatives.log.4.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/dpkg.log.7.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/faillog" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/dpkg.log.2.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/ubuntu-advantage-timer.log.3.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/dpkg.log.5.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/ubuntu-advantage-timer.log.4.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/ubuntu-advantage-timer.log.6.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/ubuntu-advantage-timer.log.1" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/dpkg.log" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/dpkg.log.9.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/dpkg.log.3.gz" is:
  - Mode: "0644" should be "640" or more restrictive

 - File: "/var/log/ubuntu-advantage-timer.log" is:
```

```
  - Mode: "0644" should be "640" or more restrictive

- File: "/var/log/dpkg.log.4.gz" is:
  - Mode: "0644" should be "640" or more restrictive

- File: "/var/log/dpkg.log.1" is:
  - Mode: "0644" should be "640" or more restrictive

- File: "/var/log/dpkg.log.8.gz" is:
  - Mode: "0644" should be "640" or more restrictive

- File: "/var/log/ubuntu-advantage-timer.log.5.gz" is:
  - Mode: "0644" should be "640" or more restrictive

- File: "/var/log/alternatives.log.3.gz" is:
  - Mode: "0644" should be "640" or more restrictive

- File: "/var/log/unattended-upgrades/unattended-upgrades-shutdown.log" is:
  - Mode: "0644" should be "640" or [...]
```

4.5 Ensure Content trust for Docker is Enabled

Info

Content trust is disabled by default and should be enabled in line with organizational security policy.

Rationale:

Content trust provides the ability to use digital signatures for data sent to and received from remote Docker registries. These signatures allow client-side verification of the identity and the publisher of specific image tags and ensures the provenance of container images.

Impact:

In an environment where DOCKER_CONTENT_TRUST is set, you are required to follow trust procedures whilst working with the image related commands - build, create, pull, push and run. You can use the --disable-content-trust flag to run individual operations on tagged images without content trust on an as needed basis, but this defeats the purpose of enabling content trust and therefore should be avoided wherever possible.

Note: Content trust is currently only available for users of the public Docker Hub. It is currently not available for the Docker Trusted Registry or for private registries.

Solution

To enable content trust in a bash shell, you should enter the following command:

export DOCKER_CONTENT_TRUST=1

Alternatively, you could set this environment variable in your profile file so that content trust in enabled on every login.

Default Value:

By default, content trust is disabled.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-53	SC-7(10)
800-53R5	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSCV8	3
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5

CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	2M
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
PCI-DSSV3.2.1	1.1
PCI-DSSV3.2.1	1.2
PCI-DSSV3.2.1	1.2.1
PCI-DSSV3.2.1	1.3
PCI-DSSV4.0	1.3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: echo $DOCKER_CONTENT_TRUST expect: 1

Hosts

192.168.111.1

```
The command 'echo $DOCKER_CONTENT_TRUST' did not return any result
```

```
The command 'echo $DOCKER_CONTENT_TRUST' did not return any result
```

5.1.2 Ensure permissions on /etc/crontab are configured

Info

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

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

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

Solution

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

chown root:root /etc/crontab

chmod og-rwx /etc/crontab

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/crontab group: root mask: 177 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/crontab with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 177 uneven
 permissions : FALSE

/etc/crontab
```

5.1.3 Ensure permissions on /etc/cron.hourly are configured

Info

This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on the /etc/cron.hourly directory:

chown root:root /etc/cron.hourly/

chmod og-rwx /etc/cron.hourly/

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.hourly group: root mask: 077 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/cron.hourly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.hourly
```

5.1.4 Ensure permissions on /etc/cron.daily are configured

Info

The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on the /etc/cron.daily directory:

chown root:root /etc/cron.daily/

chmod og-rwx /etc/cron.daily/

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.daily group: root mask: 077 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/cron.daily with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.daily
```

5.1.5 Ensure permissions on /etc/cron.weekly are configured

Info

The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on the /etc/cron.weekly directory:

chown root:root /etc/cron.weekly/

chmod og-rwx /etc/cron.weekly/

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.weekly group: root mask: 077 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/cron.weekly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.weekly
```

5.1.6 Ensure permissions on /etc/cron.monthly are configured

Info

The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on the /etc/cron.monthly directory:

chown root:root /etc/cron.monthly/

chmod og-rwx /etc/cron.monthly/

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.monthly group: root mask: 077 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/cron.monthly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.monthly
```

5.1.7 Ensure permissions on /etc/cron.d are configured

Info

The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab, but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on the /etc/cron.d directory:

chown root:root /etc/cron.d/

chmod og-rwx /etc/cron.d/

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.d group: root mask: 077 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/cron.d with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.d
```

5.1.8 Ensure cron is restricted to authorized users - '/etc/cron.allow'

Info

Configure /etc/cron.allow to allow specific users to use this service. If /etc/cron.allow does not exist, then /etc/cron.deny is checked. Any user not specifically defined in this file is allowed to use cron. By removing the file, only users in /etc/cron.allow are allowed to use cron.

Note:

Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Even though a given user is not listed in cron.allow, cron jobs can still be run as that user

The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

Run the following commands to remove /etc/cron.deny:

rm /etc/cron.deny

Run the following command to create /etc/cron.allow

touch /etc/cron.allow

Run the following commands to set permissions and ownership for /etc/cron.allow:

chmod g-wx,o-rwx /etc/cron.allow

chown root:root /etc/cron.allow

See Also

https://workbench.cisecurity.org/files/4068

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

800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.allow group: root mask: 137 owner: root system: Linux

Hosts

192.168.111.1

```
No files found: /etc/cron.allow
```

5.1.9 Ensure at is restricted to authorized users - '/etc/at.allow'

Info

Configure /etc/at.allow to allow specific users to use this service. If /etc/at.allow does not exist, then /etc/at.deny is checked. Any user not specifically defined in this file is allowed to use at. By removing the file, only users in /etc/at.allow are allowed to use at.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, at should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

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

Run the following commands to remove /etc/at.deny:

rm /etc/at.deny

Run the following command to create /etc/at.allow

touch /etc/at.allow

Run the following commands to set permissions and ownership for /etc/at.allow:

chmod g-wx,o-rwx /etc/at.allow

chown root:root /etc/at.allow

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/at.allow group: root mask: 137 owner: root system: Linux

Hosts

192.168.111.1

```
No files found: /etc/at.allow
```

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

Info

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

Rationale:

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

Solution

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

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

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/ssh/sshd_config group: root mask: 177 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/ssh/sshd_config with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 177 uneven
 permissions : FALSE

/etc/ssh/sshd_config
```

5.2.4 Ensure SSH access is limited

Info

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

AllowUsers:

The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

AllowGroups:

The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

DenyUsers:

The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

DenyGroups:

The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Solution

Edit the /etc/ssh/sshd_config file or a included configuration file to set one or more of the parameter as follows:

AllowUsers <userlist>

OR

AllowGroups <grouplist>

OR

DenyUsers <userlist>

OR

DenyGroups <grouplist>

Default Value:

None

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - sshd output
The command script with multiple lines returned :

port 22:
Fail

-------------------------
FAILED - sshd_config
No matching files were found
Less than 1 matches of regex found
```

5.2.6 Ensure SSH PAM 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.

Rationale:

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Solution

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

UsePAM yes

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b

NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - sshd output
The command script with multiple lines returned :

port 22: usepam no
Fail

-------------------------
FAILED - sshd_config
Non-compliant file(s):
      /etc/ssh/sshd_config - regex '^[\s]*(?i)UsePAM(?-i)[\s]' found - expect '^[\s]*(?i)UsePAM(?-i)
[\s]+no[\s]*$' found in the following lines:
          86: UsePAM no
      /etc/ssh/sshd_config.d/90-anapaya.conf - regex '^[\s]*(?i)UsePAM(?-i)[\s]' found - expect
 '^[\s]*(?i)UsePAM(?-i)[\s]+no[\s]*$' found in the following lines:
          11: UsePAM no
```

5.2.7 Ensure SSH root login is disabled

Info

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

Rationale:

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 parameter as follows:

PermitRootLogin no

Default Value:

PermitRootLogin without-password

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: permitrootlogin without-password
Pass

-------------------------
FAILED - sshd_config
Non-compliant file(s):
      /etc/ssh/sshd_config - regex '^[\s]*(?i)PermitRootLogin(?-i)[\s]' found - expect '^[\s]*(?
i)PermitRootLogin(?-i)[\s]+no[\s]*$' not found in the following lines:
          34: PermitRootLogin without-password
      /etc/ssh/sshd_config.d/90-anapaya.conf - regex '^[\s]*(?i)PermitRootLogin(?-i)[\s]' found -
 expect '^[\s]*(?i)PermitRootLogin(?-i)[\s]+no[\s]*$' not found in the following lines:
```

```
            4: PermitRootLogin prohibit-password
```

5.2.17 Ensure SSH warning banner is configured

Info

The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Solution

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

Banner /etc/issue.net

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3

NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass system: Linux

Hosts

192.168.111.1

```
The command script with multiple lines returned :

port 22: banner none
Fail
```

5.2.18 Ensure SSH MaxAuthTries is set to 4 or less

Info

The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.

Rationale:

Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Solution

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

MaxAuthTries 4

Default Value:

MaxAuthTries 6

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - sshd output
The command script with multiple lines returned :

port 22: maxauthtries 6
Fail

-------------------------
PASSED - sshd_config
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)MaxAuthTries(?-i)[\s]"
```

5.2.19 Ensure SSH MaxStartups is configured

Info

The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

Solution

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

MaxStartups 10:30:60

Default Value:

MaxStartups 10:30:100

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - sshd output
The command script with multiple lines returned :

port 22: maxstartups 10:30:100
Fail

-------------------------
PASSED - sshd_config
No matching files were found
```

5.2.21 Ensure SSH LoginGraceTime is set to one minute or less

Info

The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

Rationale:

Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections. While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Solution

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

LoginGraceTime 60

Default Value:

LoginGraceTime 120

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - sshd output
The command script with multiple lines returned :

port 22: logingracetime 120
Fail

-------------------------
PASSED - sshd_config
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)LoginGraceTime(?-i)[\s]"
```

5.2.22 Ensure SSH Idle Timeout Interval is configured

Info

NOTE: To clarify, the two settings described below is only meant for idle connections from a protocol perspective and 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 where abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused 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 en-abled 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.

Rationale:

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 indefinately, 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 parameters according to site policy.

Example:

ClientAliveInterval 15 ClientAliveCountMax 3

Default Value:

ClientAliveInterval 0

ClientAliveCountMax 3

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.6
800-171	3.4.7
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
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - ClientAliveInterval sshd output
The command script with multiple lines returned :

port 22: clientaliveinterval 0
Fail

-------------------------
```

```
PASSED - ClientAliveCountMax sshd output
The command script with multiple lines returned :

port 22: clientalivecountmax 3
Pass
```

5.3.2 Ensure sudo commands use pty

Info

sudo can be configured to run only from a pseudo terminal (pseudo-pty).

Rationale:

Attackers can run a malicious program using sudo which would fork a background process that remains even when the main program has finished executing.

Impact:

WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

5.3.3 Ensure sudo log file exists

Info

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

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'

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

expect: ^pass$ system: Linux

Hosts

192.168.111.1

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

fail
```

5.3.7 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.

Rationale:

Restricting the use of su , and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo , whereas su can only record that a user executed the su program.

Solution

Create an empty group that will be specified for use of the su command. The group should be named according to site policy.

Example:

groupadd sugroup

Add the following line to the /etc/pam.d/su file, specifying the empty group:

auth required pam_wheel.so use_uid group=sugroup

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: sugroup=$(/usr/bin/grep -Pi '^\h*auth\h+(?:required|requisite)\h+pam_wheel\.so\h+(?:[^# \r]+\h+)?((?!\2)(use_uid\b|group=\H+\b))\h+(?:[^# \r]+\h+)?((?!\1)(use_uid\b|group=\H+\b))(\h+.*)?$' /etc/pam.d/su | /usr/bin/awk 'BEGIN { FS = "=" } ; { print $2 }'); if [! -z $sugroup]; then /usr/bin/grep $sugroup /etc/group | /usr/bin/awk 'BEGIN { FS = ":" }; { if ($4) print $4 }' | /usr/bin/awk '{print} END {if (NR == 0) print "pass"'}; else echo "sugroup has members"; fi expect: pass system: Linux

Hosts

192.168.111.1

```
The command 'sugroup=$(/usr/bin/grep -Pi '^\h*auth\h+(?:required|requisite)\h+pam_wheel\.so\h+(?:
[^#\n\r]+\h+)?((?!\2)(use_uid\b|group=\H+\b))\h+(?:[^#\n\r]+\h+)?((?!\1)(use_uid\b|group=\H+\b))
(\h+.*)?$' /etc/pam.d/su | /usr/bin/awk 'BEGIN { FS = "=" } ; { print $2 }'); if [ ! -z $sugroup ];
 then /usr/bin/grep $sugroup /etc/group | /usr/bin/awk 'BEGIN { FS = ":" }; { if ($4) print $4 }'
 | /usr/bin/awk '{print} END {if (NR == 0) print "pass"'}; else echo "sugroup has members"; fi'
 returned :

sugroup has members
```

5.4.1 Ensure password creation requirements are configured - 'dcredit'

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

Rationale:

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

Solution

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy:

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy:

Option 1

minclass = 4

Option 2

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

Additional Information:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command pam-auth-update is used to manage certain PAM configurations via profiles, such as /etc/pam.d/common-password. Making a manual change to this file will cause pam-auth-update to overwrite it on the next run and is thus against recommendations. Alternatively, pam_pwquality (via /etc/security/pwquality.conf) fully supports the configuration of the maximum number of retries for a password change with the configuration entry retry = XXX. The issue is that the template /usr/share/pam-configs/pwquality contains retry=3 which will override any retry setting in /etc/security/pwquality.conf as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*dcredit[\s]*=[\s]*-[1-9][\s]*$ file: /etc/security/pwquality.conf regex: ^[\s]*dcredit[\s]*= system: Linux

Hosts

192.168.111.1

```
No files found: /etc/security/pwquality.conf
```

5.4.1 Ensure password creation requirements are configured - 'lcredit'

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

Rationale:

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

Solution

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy:

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy:

Option 1

minclass = 4

Option 2

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

Additional Information:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command pam-auth-update is used to manage certain PAM configurations via profiles, such as /etc/pam.d/common-password. Making a manual change to this file will cause pam-auth-update to overwrite it on the next run and is thus against recommendations. Alternatively, pam_pwquality (via /etc/security/pwquality.conf) fully supports the configuration of the maximum number of retries for a password change with the configuration entry retry = XXX. The issue is that the template /usr/share/pam-configs/pwquality contains retry=3 which will override any retry setting in /etc/security/pwquality.conf as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*lcredit[\s]*=[\s]*-[1-9][\s]*$ file: /etc/security/pwquality.conf regex: ^[\s]*lcredit[\s]*= system: Linux

Hosts

192.168.111.1

```
No files found: /etc/security/pwquality.conf
```

5.4.1 Ensure password creation requirements are configured - 'minlen'

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

Rationale:

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

Solution

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy:

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy:

Option 1

minclass = 4

Option 2

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

Additional Information:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command pam-auth-update is used to manage certain PAM configurations via profiles, such as /etc/pam.d/common-password. Making a manual change to this file will cause pam-auth-update to overwrite it on the next run and is thus against recommendations. Alternatively, pam_pwquality (via /etc/security/pwquality.conf) fully supports the configuration of the maximum number of retries for a password change with the configuration entry retry = XXX. The issue is that the template /usr/share/pam-configs/pwquality contains retry=3 which will override any retry setting in /etc/security/pwquality.conf as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*minlen[\s]*=[\s]*(1[4-9]|[2-9][0-9])[\s]*$ file: /etc/security/pwquality.conf regex: ^[\s]*minlen[\s]*= system: Linux

Hosts

192.168.111.1

```
No files found: /etc/security/pwquality.conf
```

5.4.1 Ensure password creation requirements are configured - 'ocredit'

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

Rationale:

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

Solution

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy:

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy:

Option 1

minclass = 4

Option 2

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

Additional Information:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command pam-auth-update is used to manage certain PAM configurations via profiles, such as /etc/pam.d/common-password. Making a manual change to this file will cause pam-auth-update to overwrite it on the next run and is thus against recommendations. Alternatively, pam_pwquality (via /etc/security/pwquality.conf) fully supports the configuration of the maximum number of retries for a password change with the configuration entry retry = XXX. The issue is that the template /usr/share/pam-configs/pwquality contains retry=3 which will override any retry setting in /etc/security/pwquality.conf as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*ocredit[\s]*=[\s]*-[1-9][\s]*$ file: /etc/security/pwquality.conf regex: ^[\s]*ocredit[\s]*= system: Linux

Hosts

192.168.111.1

```
No files found: /etc/security/pwquality.conf
```

5.4.1 Ensure password creation requirements are configured - 'ucredit'

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

Rationale:

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

Solution

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy:

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy:

Option 1

minclass = 4

Option 2

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

Additional Information:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command pam-auth-update is used to manage certain PAM configurations via profiles, such as /etc/pam.d/common-password. Making a manual change to this file will cause pam-auth-update to overwrite it on the next run and is thus against recommendations. Alternatively, pam_pwquality (via /etc/security/pwquality.conf) fully supports the configuration of the maximum number of retries for a password change with the configuration entry retry = XXX. The issue is that the template /usr/share/pam-configs/pwquality contains retry=3 which will override any retry setting in /etc/security/pwquality.conf as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*ucredit[\s]*=[\s]*-[1-9][\s]*$ file: /etc/security/pwquality.conf regex: ^[\s]*ucredit[\s]*= system: Linux

Hosts

192.168.111.1

```
No files found: /etc/security/pwquality.conf
```

5.4.2 Ensure lockout for failed password attempts is configured

Info

Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the common PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

All configuration of faillock is located in /etc/security/faillock.conf and well commented.

deny - Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds n tries.

fail_interval - The length of the interval, in seconds, during which the consecutive authentication failures must happen for the user account to be locked out

unlock_time - The access will be re-enabled after n 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 command.

Set the lockout number and unlock time in accordance with local site policy.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Impact:

It is critical to test and validate any PAM changes before deploying. Any misconfiguration could cause the system to be inaccessible.

Solution

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. You configuration may differ based on previous changes to the files.

Common auth Edit /etc/pam.d/common-auth and ensure that faillock is configured.

Note: It is critical to understand each line and the relevant arguments for successful implementation. The order of these entries is very specific. The pam_faillock.so lines surround the pam_unix.so line. The comment 'Added to enable faillock' is shown to highlight the additional lines and their order in the file.

here are the per-package modules (the 'Primary' block) auth required pam_faillock.so preauth # Added to enable faillock auth [success=1 default=ignore] pam_unix.so nullok auth [default=die] pam_faillock.so authfail # Added to enable faillock auth sufficient pam_faillock.so authsucc # Added to enable faillock # here's the fallback if no module succeeds auth requisite pam_deny.so # prime the stack with a positive return value if there isn't one already;

this avoids us returning an error just because nothing sets a success code # since the modules above will each just jump around auth required pam_permit.so # and here are more per-package modules (the 'Additional' block) auth optional pam_cap.so # end of pam-auth-update config

Common account Edit /etc/pam.d/common-account and ensure that the following stanza is at the end of the file.

account required pam_faillock.so

Fail lock configuration Edit /etc/security/faillock.conf and configure it per your site policy.

Example:

deny = 4 fail_interval = 900 unlock time = 600

Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_faillock.so module, the user can be unlocked by issuing the command /usr/sbin/faillock --user username --reset. This command sets the failed count to 0, effectively unlocking the user.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.1
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
FAILED - common-auth preauth
The file "/etc/pam.d/common-auth" does not contain "^\h*auth\h+(required|requisite)\h+pam_faillock
\.so\h+([^#\n\r]+\h+)?preauth\b"

-------------------------
FAILED - common-auth authfail
The file "/etc/pam.d/common-auth" does not contain "^\h*auth\h+\[default=die\]\h+pam_faillock\.so\h
+([^#\n\r]+\h+)?authfail\b"

-------------------------
FAILED - common-auth authfail
The file "/etc/pam.d/common-auth" does not contain "^\h*auth\h+sufficient\h+pam_faillock\.so\h+([^#
\n\r]+\h+)?authsucc\b"

-------------------------
FAILED - faillock.conf deny
The file "/etc/security/faillock.conf" does not contain "^\h*deny\h*="

-------------------------
FAILED - faillock.conf fail_interval
The file "/etc/security/faillock.conf" does not contain "^\h*fail_interval\h*="

-------------------------
FAILED - faillock.conf unlock_time
The file "/etc/security/faillock.conf" does not contain "^\h*unlock_time\h*="

-------------------------
FAILED - common-account account pam_faillock.so
The file "/etc/pam.d/common-account" does not contain "^\h*account\h+(required|requisite)\h
+pam_faillock\.so\b"
```

5.4.3 Ensure password reuse is limited

Info

The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Solution

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. You configuration may differ based on previous changes to the files.

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

password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt remember=5

Additional Information:

Changes only apply to accounts configured on the local system.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^\h*password\h+([^# \r]+\h+)?pam_unix\.so\h+([^# \r]+\h+)?remember=([5-9]|[1-9][0-9]+)\b file: /etc/pam.d/common-password regex: ^\h*password\h+([^# \r]+\h+)?pam_unix\.so\h+ system: Linux

Hosts

192.168.111.1

```
Non-compliant file(s):
      /etc/pam.d/common-password - regex '^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\h+' found -
 expect '^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\h+([^#\n\r]+\h+)?remember=([5-9]|[1-9][0-9]+)\b'
 not found in the following lines:
          25: password[success=1 default=ignore]pam_unix.so obscure yescrypt
```

5.4.4 Ensure password hashing algorithm is up to date with the latest standards

Info

The commands below change password encryption to yescrypt. All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The yescrypt algorithm provides much stronger hashing than previous available algorithms, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

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

Solution

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. You configuration may differ based on previous changes to the files.

PAM Edit the /etc/pam.d/common-password file and ensure that no hashing algorithm option for pam_unix.so is set:

password[success=1 default=ignore]pam_unix.so obscure use_authtok try_first_pass remember=5

Login definitions Edit /etc/login.defs and ensure that ENCRYPT_METHOD is set to yescrypt.

Additional Information:

Additional module options may be set, recommendation only covers those listed here.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-171	3.13.16
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
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)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

FAILED

Hosts

192.168.111.1

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

-------------------------
PASSED - Specified or no hashing algorithm should be configured in /etc/pam.d/common-password
The command '/usr/bin/awk 'BEGIN { IGNORECASE=1 } /^\s*password.*pam_unix.so/ { if (/yescrypt/)
 {printf "pass: yescrypt configured"} else if (/(yescrypt|md5|bigcrypt|sha256|sha512|blowfish)/)
 {printf "fail: hashing configured"} else { printf "pass: no hashing configured" }; print ": "$0}'
  /etc/pam.d/common-password' returned :

pass: yescrypt configured: password[success=1 default=ignore]pam_unix.so obscure yescrypt

-------------------------
FAILED - Hashing algorithm in login.defs is yescrypt
Non-compliant file(s):
      /etc/login.defs - regex '^\s*ENCRYPT_METHOD\s+' found - expect '^\s*ENCRYPT_METHOD\s+(?
i)yescrypt(?-i)\s*$' not found in the following lines:
```

```
284: ENCRYPT_METHOD SHA512
```

5.5.1.1 Ensure minimum days between password changes is configured - login.defs

Info

The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 1 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Solution

Set the PASS_MIN_DAYS parameter to 1 in /etc/login.defs :

PASS_MIN_DAYS 1

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

chage --mindays 1 <user>

Default Value:

PASS_MIN_DAYS 0

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: PASS_MIN_DAYS[\s]+([1-9]|[1-9][0-9]+)[\s]*$ file: /etc/login.defs regex: ^[\s\t]*PASS_MIN_DAYS[\s]+ system: Linux

Hosts

192.168.111.1

```
Non-compliant file(s):
      /etc/login.defs - regex '^[\s\t]*PASS_MIN_DAYS[\s]+' found - expect 'PASS_MIN_DAYS[\s]+([1-9]|
[1-9][0-9]+)[\s]*$' not found in the following lines:
          166: PASS_MIN_DAYS0
```

5.5.1.1 Ensure minimum days between password changes is configured - users

Info

The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 1 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Solution

Set the PASS_MIN_DAYS parameter to 1 in /etc/login.defs :

PASS_MIN_DAYS 1

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

chage --mindays 1 <user>

Default Value:

PASS_MIN_DAYS 0

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: echo 'Username, Minimum number of days between password change'; output=""; failures=0; for i in $(egrep "^[^:]+:[^!*]" /etc/shadow | cut -d: -f1); do change_date=$(chage --list "$i" | grep 'Minimum number of days between password change' | cut -d: -f2 | awk '{$1=$1};1'); output="${i}, ${change_date}"; if [$change_date -ge 1]; then output="${output} - Pass"; else output="${output} - Fail"; failures=$((failures +1)); fi; echo "${output}"; done; echo "Number of failures: ${failures}"

expect: ^Number of failures: 0$ system: Linux

Hosts

192.168.111.1

```
The command 'echo 'Username, Minimum number of days between password change'; output=""; failures=0;
 for i in $(egrep "^[^:]+:[^!*]" /etc/shadow | cut -d: -f1); do change_date=$(chage --list "$i"
 | grep 'Minimum number of days between password change' | cut -d: -f2 | awk '{$1=$1};1');
 output="${i}, ${change_date}"; if [ $change_date -ge 1 ]; then output="${output} - Pass"; else
 output="${output} - Fail"; failures=$((failures+1)); fi; echo "${output}"; done; echo "Number of
 failures: ${failures}"' returned :

Username, Minimum number of days between password change
root, 0 - Fail
anapaya, 0 - Fail
scion, 0 - Fail
Number of failures: 3
```

5.5.1.2 Ensure password expiration is 365 days or less - login.defs

Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity. It is recommended that the PASS_MAX_DAYS parameter does not exceed 365 days and is greater than the value of PASS_MIN_DAYS.

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>

Default Value:

PASS_MAX_DAYS 99999

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*PASS_MAX_DAYS[\s]+([1-9]|[1-9][0-9]|[12][0-9][0-9]|3[0-5][0-9]|36[0-5])[\s]*$ file: /etc/login.defs regex: ^[\s]*PASS_MAX_DAYS[\s] system: Linux

Hosts

192.168.111.1

```
Non-compliant file(s):
      /etc/login.defs - regex '^[\s]*PASS_MAX_DAYS[\s]' found - expect
 '^[\s]*PASS_MAX_DAYS[\s]+([1-9]|[1-9][0-9]|[12][0-9][0-9]|3[0-5][0-9]|36[0-5])[\s]*$' not found in
 the following lines:
         165: PASS_MAX_DAYS99999
```

5.5.1.2 Ensure password expiration is 365 days or less - users

Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity. It is recommended that the PASS_MAX_DAYS parameter does not exceed 365 days and is greater than the value of PASS_MIN_DAYS.

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>

Default Value:

PASS_MAX_DAYS 99999

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^([^:]*:){4}([1-9]|[1-9][0-9]|[12][0-9][0-9]|3[0-5][0-9]|36[0-5]):

file: /etc/shadow regex: ^[^:]+:[^!*] string_required: NO system: Linux

Hosts

192.168.111.1

```
Non-compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){4}([1-9]|[1-9][0-9]|[12][0-9]
[0-9]|3[0-5][0-9]|36[0-5]):' not found in the following lines:
          1: root:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19047:0:99999:7:::
          26: anapaya:$6$Ykmswojd$lodHD1eD5i5i4FfSVEY/s/Yywnlw7cr9WTIOA/lnceFgak7Z6c5xs/i/wQkzkh/
WDy5R4w4ZFghZrAgOmud02.:19047:0:99999:7:::
          27: scion:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19361:0:99999:7:::
```

5.5.1.4 Ensure inactive password lock is 30 days or less - useradd

Info

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Solution

Run the following command to set the default password inactivity period to 30 days:

useradd -D -f 30

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

chage --inactive 30 <user>

Default Value:

INACTIVE=-1

Additional Information:

A value of -1 would disable this setting

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/sbin/useradd -D | /bin/grep INACTIVE expect: ^INACTIVE=(30|[1-2][0-9]|[0-9])$ system: Linux

Hosts

192.168.111.1

```
The command '/usr/sbin/useradd -D | /bin/grep INACTIVE' returned :

INACTIVE=-1
```

5.5.1.4 Ensure inactive password lock is 30 days or less - users

Info

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Solution

Run the following command to set the default password inactivity period to 30 days:

useradd -D -f 30

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

chage --inactive 30 <user>

Default Value:

INACTIVE=-1

Additional Information:

A value of -1 would disable this setting

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^([^:]*:){6}(30|[1-2][0-9]|[1-9]):

file: /etc/shadow regex: ^[^:]+:[^!*] string_required: NO system: Linux

Hosts

192.168.111.1

```
Non-compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){6}(30|[1-2][0-9]|[1-9]):' not
 found in the following lines:
          1: root:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19047:0:99999:7:::
          26: anapaya:$6$Ykmswojd$lodHD1eD5i5i4FfSVEY/s/Yywnlw7cr9WTIOA/lnceFgak7Z6c5xs/i/wQkzkh/
WDy5R4w4ZFghZrAgOmud02.:19047:0:99999:7:::
          27: scion:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19361:0:99999:7:::
```

5.5.4 Ensure default user umask is 027 or more restrictive - Default user umask

Info

The user file-creation mode mask (umask) is use to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). 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-----.

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 .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/bash.bashrc - System wide version of .bashrc. 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/bash.bashrc

User Shell Configuration Files:

~/.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

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Impact:

Setting USERGROUPS_ENAB no in /etc/login.defs may change the expected behavior of useradd and userdel.

Setting USERGROUPS_ENAB yes in /etc/login.defs

userdel will remove the user's group if it contains no more members

useradd will create by default a group with the name of the user.

Solution

Run the following command and remove or modify the umask of any returned files:

grep -RPi '(^|^[^#]*)s*umasks+([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]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*

Follow one of the following methods to set the default user umask:
Edit /etc/login.defs and edit the UMASK and USERGROUPS_ENAB lines as follows:

UMASK 027

USERGROUPS_ENAB no

Edit /etc/pam.d/common-session and add or edit the following:

session optional pam_umask.so

OR Configure umask in one of the following files:

A file in the /etc/profile.d/ directory ending in .sh

/etc/profile

/etc/bash.bashrc

Example: /etc/profile.d/set_umask.sh

umask 027

Note: 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.

Default Value:

UMASK 022

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: passing=""; /usr/bin/grep -Eiq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/login.defs && /usr/bin/grep -Eqi '^\s*USERGROUPS_ENAB\s*"?no"?\b' /etc/login.defs && /usr/bin/grep -Eq '^\s*session\s+(optional|requisite|required)\s+pam_umask\.so\b' /etc/pam.d/common-session && passing=true; /

usr/bin/grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-7]7|u=(r?|w?|x?)(r?|w?|x?)(r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile* /etc/bash.bashrc* && passing=true; ["$passing" = true] && echo "Default user umask is set";[-z "$passing"] && echo "Default user umask is not set"

expect: Default user umask is set system: Linux

Hosts

192.168.111.1

```
The command 'passing=""; /usr/bin/grep -Eiq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/
login.defs && /usr/bin/grep -Eqi '^\s*USERGROUPS_ENAB\s*"?no"?\b' /etc/login.defs && /usr/bin/grep
 -Eq '^\s*session\s+(optional|requisite|required)\s+pam_umask\.so\b' /etc/pam.d/common-session &&
 passing=true; /usr/bin/grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-7]7|u=(r?|w?|x?)(r?|w?|
x?)(r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile* /etc/bash.bashrc* && passing=true; [ "$passing"
 = true ] && echo "Default user umask is set";[ -z "$passing" ] && echo "Default user umask is not
 set"' returned :

Default user umask is not set
```

5.5.4 Ensure default user umask is 027 or more restrictive - Restrictive system umask

Info

The user file-creation mode mask (umask) is use to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). 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-----.

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 .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/bash.bashrc - System wide version of .bashrc. 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/bash.bashrc

User Shell Configuration Files:

~/.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

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Impact:

Setting USERGROUPS_ENAB no in /etc/login.defs may change the expected behavior of useradd and userdel.

Setting USERGROUPS_ENAB yes in /etc/login.defs

userdel will remove the user's group if it contains no more members

useradd will create by default a group with the name of the user.

Solution

Run the following command and remove or modify the umask of any returned files:

grep -RPi '(^|^[^#]*)s*umasks+([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]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*

Follow one of the following methods to set the default user umask:

Edit /etc/login.defs and edit the UMASK and USERGROUPS_ENAB lines as follows:

UMASK 027

USERGROUPS_ENAB no

Edit /etc/pam.d/common-session and add or edit the following:

session optional pam_umask.so

OR Configure umask in one of the following files:

A file in the /etc/profile.d/ directory ending in .sh

/etc/profile

/etc/bash.bashrc

Example: /etc/profile.d/set_umask.sh

umask 027

Note: 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.

Default Value:

UMASK 022

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/grep -RPi '(^|^[^#]*)\s*umask\s+([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]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /

etc/login.defs /etc/profile* /etc/bash.bashrc* | /usr/bin/awk '{print} END {if (NR == 0) print "pass - no less restrictive system umask set"; else print "fail"}'

expect: pass - no less restrictive system umask set system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/grep -RPi '(^|^[^#]*)\s*umask\s+([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]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]
{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc* | /usr/
bin/awk '{print} END {if (NR == 0) print "pass - no less restrictive system umask set"; else print
 "fail"}'' returned :

/etc/login.defs:UMASK022
fail
```

5.5.5 Ensure default user shell timeout is 900 seconds or less

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 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/bash.bashrc - System wide version of bash.bashrc. etc/bash.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/bash.bashrc.

Rationale:

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/bash.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 in .sh

/etc/profile

/etc/bash.bashrc

TMOUT configuration examples:

As multiple lines:

TMOUT=900 readonly TMOUT export TMOUT

As a single line:

readonly TMOUT=900 ; export TMOUT

Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files are also checked

Other methods of setting a timeout exist not covered here

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/grep -P '^[\s]*TMOUT[\s]*=' /etc/bash.bashrc /etc/profile /etc/profile.d/*.sh expect: : [\s]*TMOUT[\s]*=([1-9][0-9]|[1-8][0-9][0-9]|900) system: Linux

Hosts

192.168.111.1

```
The command '/bin/grep -P '^[\s]*TMOUT[\s]*=' /etc/bash.bashrc /etc/profile /etc/profile.d/*.sh' did
 not return any result
```

6.1.9 Ensure no world writable files exist

Info

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information.

Rationale:

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

Solution

Removing write access for the 'other' category (chmod o-w <filename>) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: find_world_writeable_files system: Linux timeout: 7200

Hosts

192.168.111.1

```
The following 54 files are world writeable:

  /var/lib/docker/overlay2/2c52d501f8efb9a88aa9b42222e1fa91423208e89032d13ab4c10833eb4579c3/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/da1e654a8b0e930d5adcd862cfe77026211d675977a06068f6cf5b85033f68eb/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276-init/
lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd-init/
lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/0c928a90d337b1dcc29f650cfe80d4163536fcdfbb7ab3f476446b1125baa8b9/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/ec077ba2363b072e1a1e56fec8004e31ff5b1aba235a3af33fb82066a1b71a44/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/3644b8375b5d397c6b34c83c025cab925abe5b185f0352267a1a1a1732356e1d/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/45b66544ed5c326970a918cce54381d2f13425ff651d2e2be465e76e32ff195e/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/5813459578d29b4301854a9713108c6e92186a9b6f23bf0a188be84fb5d149cf/lower
     owner: root, group: root, permissions: 0666

  /var/lib/docker/overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91-init/
lower
     owner: root, group: root, permissions: 0666
```

```
/var/lib/docker/overlay2/4496f9438ef363cc067e514ab3106999a43763e08fb4f1ab67354e0683ce64a5/lower
   owner: root, group: root, permissions: 0666

/var/lib/docker/overlay2/dd6440b7f8fab1706529d05c08c78c70a93c55 [...]
```

6.1.10 Ensure no unowned files or directories exist

Info

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up 'owning' these files, and thus have more access on the system than was intended.

Solution

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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	13.2
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

find_option: nouser name: find_orphan_files system: Linux timeout: 7200

Hosts

192.168.111.1

```
The following 2 files are orphaned:

  /var/lib/docker/overlay2/516a6ce48195777c88cdadfd9aff21a80e42e1dce88b59f8241dfc9be824d1c7/diff/
home
     owner: 65532, group: 65532, permissions: 0755

  /var/lib/docker/overlay2/516a6ce48195777c88cdadfd9aff21a80e42e1dce88b59f8241dfc9be824d1c7/diff/
home/nonroot
     owner: 65532, group: 65532, permissions: 0700
```

6.1.11 Ensure no ungrouped files or directories exist

Info

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up 'owning' these files, and thus have more access on the system than was intended.

Solution

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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	13.2
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

find_option: nogroup name: find_orphan_files system: Linux timeout: 7200

Hosts

192.168.111.1

```
The following 8 files are orphaned:

  /var/lib/docker/overlay2/516a6ce48195777c88cdadfd9aff21a80e42e1dce88b59f8241dfc9be824d1c7/diff/
home
     owner: 65532, group: 65532, permissions: 0755

  /var/lib/docker/overlay2/516a6ce48195777c88cdadfd9aff21a80e42e1dce88b59f8241dfc9be824d1c7/diff/
home/nonroot
     owner: 65532, group: 65532, permissions: 0700

  /var/lib/docker/overlay2/6b436efacb02870424cb9cd61cd87bb1e0e4549321069c083caee2beb4dc8fcc/diff/
pkgs/apk/x86_64
     owner: anapaya, group: 300, permissions: 0755

  /var/lib/docker/overlay2/6b436efacb02870424cb9cd61cd87bb1e0e4549321069c083caee2beb4dc8fcc/diff/
pkgs/apk/x86_64/APKINDEX.tar.gz
     owner: anapaya, group: 300, permissions: 0644

  /var/lib/docker/overlay2/6b436efacb02870424cb9cd61cd87bb1e0e4549321069c083caee2beb4dc8fcc/diff/
pkgs/apk/x86_64/frr-doc-8.5.3_git-r0.apk
     owner: anapaya, group: 300, permissions: 0644

  /var/lib/docker/overlay2/6b436efacb02870424cb9cd61cd87bb1e0e4549321069c083caee2beb4dc8fcc/diff/
pkgs/apk/x86_64/frr-dbg-8.5.3_git-r0.apk
     owner: anapaya, group: 300, permissions: 0644

  /var/lib/docker/overlay2/6b436efacb02870424cb9cd61cd87bb1e0e4549321069c083caee2beb4dc8fcc/diff/
pkgs/apk/x86_64/frr-8.5.3_git-r0.apk
     owner: anapaya, group: 300, permissions: 0644

  /var/lib/docker/overlay2/6b436efacb02870424cb9cd61cd87bb1e0e4549321069c083caee2beb4dc8fcc/diff/
pkgs/apk/x86_64/frr-dev-8.5.3_git-r0.apk
     owner: anapaya, group: 300, permissions: 0644
```

6.2.9 Ensure root PATH Integrity

Info

The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.

Rationale:

Including the current working directory (.) or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

Solution

Correct or justify any items discovered in the Audit step.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1204, T1204.002

TA0006

M1022

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: RPCV="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"; echo "$RPCV" | grep -q "::" && echo "root's path contains a empty directory (::)"; echo "$RPCV" | grep -q ":$" && echo "root's path contains a trailing (:)"; for x in $(echo "$RPCV" | tr ":" " "); do if [-d "$x"]; then ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working directory (.)"}; $3 != "root" {print $9, "is not owned by root"}; substr($1,6,1) != "-" {print $9, "is group writable"}; substr($1,9,1) != "-" {print $9, "is world writable"}'; else echo "$x is not a directory"; fi; done | /usr/bin/awk '{print} END {if (NR == 0) print "All results passing"; else print "fail"}'

expect: All results passing system: Linux

Hosts

192.168.111.1

```
The command 'RPCV="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"; echo "$RPCV" | grep -q
 "::" && echo "root's path contains a empty directory (::)"; echo "$RPCV" | grep -q ":$" && echo
 "root's path contains a trailing (:)"; for x in $(echo "$RPCV" | tr ":" " "); do if [ -d "$x" ];
 then ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working directory (.)"}; $3 !=
 "root" {print $9, "is not owned by root"}; substr($1,6,1) != "-" {print $9, "is group writable"};
 substr($1,9,1) != "-" {print $9, "is world writable"}'; else echo "$x is not a directory"; fi;
 done | /usr/bin/awk '{print} END {if (NR == 0) print "All results passing"; else print "fail"}''
 returned :

/snap/bin is not a directory
fail
```

6.2.13 Ensure local interactive user home directories are mode 750 or more restrictive

Info

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Solution

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

The following script can be used to remove permissions is excess of 750 from interactive user home directories:

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

{ perm_mask='0027'

maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'

valid_shells='^($( sed -rn '/^//{s,/,\\/,g;p}' /etc/shells | paste -s -d '|' - ))$'

awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | (while read -r user home; do mode=$( stat -L -c '%#a' '$home' ) if [ $(( $mode & $perm_mask )) -gt 0 ]; then echo -e '- modifying User $user home directory: '$home'

- removing excessive permissions from current mode of '$mode''

chmod g-w,o-rwx '$home'

fi done ) }
```

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

mask: 0027 name: accounts_bad_home_permissions system: Linux use_valid_shells: YES

Hosts

192.168.111.1

```
The following home directories have inappropriate permissions and/or ownership (mask:0027) (using /
etc/shells to determine valid interactive user shells):

 /home/anapaya  mode: 0755 (should be 0750 or stricter) owner: anapaya
 /home/scion  mode: 0755 (should be 0750 or stricter) owner: scion
 /home/william.blonay  mode: 0755 (should be 0750 or stricter) owner: william.blonay
```

6.2.17 Ensure local interactive user dot files are not group or world writable

Info

While the system administrator can establish secure permissions for users' 'dot' files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

The following script will remove excessive permissions on dot files within interactive users' home directories.

#!/usr/bin/env bash

{ perm_mask='0022'

valid_shells='^($(sed -rn '/^//{s,/,\\/,g;p}' /etc/shells | paste -s -d '|' -))$'

awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | while read -r user home; do find '$home' -type f -name '.*' | while read -r dfile; do mode=$(stat -L -c '%#a' '$dfile') if [$(($mode & $perm_mask)) -gt 0]; then echo -e '

- Modifying User '$user' file: '$dfile'

- removing group and other write permissions'

chmod go-w '$dfile'

fi done done }

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: ~/.[!.]* mask: 022 system: Linux

Hosts

192.168.111.1

```
The file /home/anapaya/.ansible with fmode owner: anapaya group: anapaya mode: 0775 uid: 1000 gid:
 1000 uneven permissions : FALSE  does not match the policy value mask: 0022 uneven permissions :
 TRUE
The file /home/anapaya/.local with fmode owner: anapaya group: anapaya mode: 0775 uid: 1000 gid:
 1000 uneven permissions : FALSE  does not match the policy value mask: 0022 uneven permissions :
 TRUE
The file /home/william.blonay/.ssh with fmode owner: william.blonay group: william.blonay mode: 0775
 uid: 1003 gid: 1003 uneven permissions : FALSE  does not match the policy value mask: 0022 uneven
 permissions : TRUE

/home/anapaya/.ansible, /home/anapaya/.local, /home/william.blonay/.ssh
```

Compliance 'SKIPPED'

Compliance 'PASSED'

1.1.3.2 Ensure nodev option set on /var partition

Info

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

Rationale:

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 the /var partition exists, 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,relatime 0 0

Run the following command to remount /var with the configured options:

mount -o remount /var

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nodev|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.3.3 Ensure nosuid option set on /var partition

Info

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

Rationale:

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 the /var partition exists, 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,relatime 0 0

Run the following command to remount /var with the configured options:

mount -o remount /var

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nosuid|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.4.2 Ensure noexec option set on /var/tmp partition

Info

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

Rationale:

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

Solution

IF the /var/tmp partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/tmp | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: (noexec|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/tmp | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.4.3 Ensure nosuid option set on /var/tmp partition

Info

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

Rationale:

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

Solution

IF the /var/tmp partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/tmp | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: (nosuid|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/tmp | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.4.4 Ensure nodev option set on /var/tmp partition

Info

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

Rationale:

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

Solution

IF the /var/tmp partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/tmp | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: (nodev|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/tmp | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.5.2 Ensure nodev option set on /var/log partition

Info

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

Rationale:

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 the /var/log partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/log | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nodev|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/log | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.5.3 Ensure noexec option set on /var/log partition

Info

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

Rationale:

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 the /var/log partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/log | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?noexec|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/log | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.5.4 Ensure nosuid option set on /var/log partition

Info

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

Rationale:

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 the /var/log partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/log | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nosuid|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/log | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.6.2 Ensure noexec option set on /var/log/audit partition

Info

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

Rationale:

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 the /var/log/audit partition exists, edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /var 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/log/audit | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'
expect: ([\s]*[,]?noexec|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/log/audit | /usr/bin/awk '{print} END {if (NR == 0)
 print "not mounted"}'' returned :

not mounted
```

1.1.6.3 Ensure nodev option set on /var/log/audit partition

Info

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

Rationale:

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 the /var/log/audit partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/log/audit | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'
expect: ([\s]*[,]?nodev|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/log/audit | /usr/bin/awk '{print} END {if (NR == 0)
 print "not mounted"}'' returned :

not mounted
```

1.1.6.4 Ensure nosuid option set on /var/log/audit partition

Info

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

Rationale:

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 the /var/log/audit partition exists, 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /var/log/audit | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'
expect: ([\s]*[,]?nosuid|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /var/log/audit | /usr/bin/awk '{print} END {if (NR == 0)
 print "not mounted"}'' returned :

not mounted
```

1.1.7.2 Ensure nodev option set on /home partition

Info

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

Rationale:

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 /var.

Solution

IF the /home partition exists, 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,relatime 0 0

Run the following command to remount /home with the configured options:

mount -o remount /home

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /home | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nodev|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /home | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.7.3 Ensure nosuid option set on /home partition

Info

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

Rationale:

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 the /home partition exists, 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,relatime 0 0

Run the following command to remount /home with the configured options:

mount -o remount /home

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/findmnt --kernel /home | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nosuid|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/findmnt --kernel /home | /usr/bin/awk '{print} END {if (NR == 0) print "not
 mounted"}'' returned :

not mounted
```

1.1.8.1 Ensure nodev option set on /dev/shm partition

Info

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

Rationale:

Since the /dev/shm filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in /dev/shm partitions.

Solution

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

Run the following command to remount /dev/shm using the updated options from /etc/fstab:

mount -o remount /dev/shm

Additional Information:

Some distributions mount /dev/shm through other means and require /dev/shm to be added to /etc/fstab even though it is already being mounted on boot. Others may configure /dev/shm in other locations and may override /etc/fstab configuration. Consult the documentation appropriate for your distribution.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/mount | /usr/bin/grep 'on /dev/shm ' | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nodev|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/mount | /usr/bin/grep 'on /dev/shm ' | /usr/bin/awk '{print} END {if (NR == 0)
 print "not mounted"}'' returned :

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

1.1.8.3 Ensure nosuid option set on /dev/shm partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /dev/shm using the updated options from /etc/fstab:

mount -o remount /dev/shm

Additional Information:

Some distributions mount /dev/shm through other means and require /dev/shm to be added to /etc/fstab even though it is already being mounted on boot. Others may configure /dev/shm in other locations and may override /etc/fstab configuration. Consult the documentation appropriate for your distribution.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/mount | /usr/bin/grep 'on /dev/shm ' | /usr/bin/awk '{print} END {if (NR == 0) print "not mounted"}'

expect: ([\s]*[,]?nosuid|not mounted) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/mount | /usr/bin/grep 'on /dev/shm ' | /usr/bin/awk '{print} END {if (NR == 0)
 print "not mounted"}'' returned :

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

1.1.9 Disable Automounting

Info

autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

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.

Solution

If there are no other packages that depends on autofs, remove the package with:

apt purge autofs

OR if there are dependencies on the autofs package:

Run the following commands to mask autofs:

systemctl stop autofs # systemctl mask autofs

Additional Information:

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/systemctl is-enabled autofs | /usr/bin/awk '{print} END {if(NR==0) print "disabled" }'
expect: (disabled|masked|static) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/systemctl is-enabled autofs | /usr/bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

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

1.1.10 Disable USB Storage - lsmod

Info

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

Rationale:

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

Solution

Run the following script to disable usb-storage:

#!/usr/bin/env bash

{ l_mname='usb-storage' # set module name if ! modprobe -n -v '$l_mname' | grep -P -- '^h*install /bin/(true|false)'; then echo -e ' - setting module: '$l_mname' to be not 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*blacklisth+$l_mnameb' /etc/modprobe.d/*; then echo -e ' - deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mname'.conf fi }

Additional Information:

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

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /sbin/lsmod | /bin/grep usb-storage | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/sbin/lsmod | /bin/grep usb-storage | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass"; else print "fail"}'' returned :

pass
```

1.4.3 Ensure authentication required for single user mode

Info

Single user mode is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

Rationale:

Requiring authentication in single user mode prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Solution

Run the following command and follow the prompts to set a password for the root user:

passwd root

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^root:[*!]:

file: /etc/shadow regex: ^root:

system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /etc/shadow - regex '^root:' found - expect '^root:[\*!]:' not found in the following lines:
          1: root:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19047:0:99999:7:::
```

1.5.1 Ensure address space layout randomization (ASLR) is enabled - config

Info

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

Rationale:

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

Solution

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

Example:

printf '

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

Default Value:

kernel.randomize_va_space = 2

See Also

https://workbench.cisecurity.org/files/4068

References

800-53	SI-16
800-53R5	SI-16
CSCV7	8.3
CSCV8	10.5
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1A

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: grep -Es "^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-9]|[1-9][0-9]+)" /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | /usr/bin/awk '{print} END {if (NR == 0) print "pass - no invalid randomzie_va_space results found"; else print "fail"}'

expect: pass - no invalid randomzie_va_space results found system: Linux

Hosts

192.168.111.1

```
The command 'grep -Es "^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-9]|[1-9][0-9]+)" /etc/
sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /
run/sysctl.d/*.conf | /usr/bin/awk '{print} END {if (NR == 0) print "pass - no invalid
 randomzie_va_space results found"; else print "fail"}'' returned :

pass - no invalid randomzie_va_space results found
```

1.5.1 Ensure address space layout randomization (ASLR) is enabled - sysctl

Info

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

Rationale:

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

Solution

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

Example:

printf '

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

Default Value:

kernel.randomize_va_space = 2

See Also

https://workbench.cisecurity.org/files/4068

References

800-53	SI-16
800-53R5	SI-16
CSCV7	8.3
CSCV8	10.5
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1A

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /sbin/sysctl kernel.randomize_va_space expect: ^[\s]*kernel\.randomize_va_space[\s]*=[\s]*2[\s]*$
system: Linux

Hosts

192.168.111.1

```
The command '/sbin/sysctl kernel.randomize_va_space' returned :

kernel.randomize_va_space = 2
```

1.5.2 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.

Rationale:

The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.

Solution

Run the following command to restore binaries to normal:

prelink -ua

Uninstall prelink using the appropriate package manager or manual installation:

apt purge prelink

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s prelink 2>&1 expect: (?:(^[\s]*dpkg-query: package 'prelink' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$))* system: Linux

Hosts

192.168.111.1

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

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

1.5.3 Ensure Automatic Error Reporting is not enabled

Info

The Apport Error Reporting Service automatically generates crash reports for debugging

Rationale:

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 disable the apport service

systemctl stop apport.service # systemctl --now disable apport.service

-- OR -- Run the following command to remove the apport package:

apt purge apport

Default Value:

enabled=1

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - Apport is installed and enabled not 0
The command 'output=$(/usr/bin/dpkg-query -s apport > /dev/null 2>&1 && /usr/bin/grep -Psi -- '^
\h*enabled\h*=\h*[^0]\b' /etc/default/apport); echo $output | /usr/bin/awk '{print} END {if (NF ==
 0) print "pass" ; else print "fail"}'' returned :

pass

-------------------------
PASSED - Apport is not active
The command '/usr/bin/systemctl is-enabled apport.service | /usr/bin/grep '^active' | /usr/bin/awk
 '{print} END {if(NR==0) print "Pass"}'' returned :

Failed to get unit file state for apport.service: No such file or directory
Pass
```

1.5.4 Ensure core dumps are restricted - processsizemax

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

IF systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1005, T1005.000

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.5.4 Ensure core dumps are restricted - storage

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

IF systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1005, T1005.000

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.5.4 Ensure core dumps are restricted - sysctl

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

IF systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1005, T1005.000

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /sbin/sysctl fs.suid_dumpable expect: ^[\s]*fs\.suid_dumpable[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.111.1

```
The command '/sbin/sysctl fs.suid_dumpable' returned :

fs.suid_dumpable = 0
```

1.6.1.1 Ensure AppArmor is installed

Info

AppArmor provides Mandatory Access Controls.

Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Solution

Install AppArmor.

apt install apparmor

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s apparmor | /bin/grep Status: 2>&1 expect: ^[\s]*Status: install ok installed[\s]* system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s apparmor | /bin/grep Status: 2>&1' returned :

Status: install ok installed
```

1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration - apparmor

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.

Rationale:

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

Solution

Edit /etc/default/grub and add the 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: [Aa][Pp][Pp][Aa][Rr][Mm][Oo][Rr]=0 file: /boot/grub/grub.cfg regex: ^[\s]*linux[\s]* system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /boot/grub/grub.cfg - regex '^[\s]*linux[\s]*' found - expect '[Aa][Pp][Pp][Aa][Rr][Mm][Oo]
[Rr]=0' not found in the following lines:
          155: linux/boot/vmlinuz-5.15.0-100-generic root=/dev/mapper/anapaya--v3--vg-root ro
 noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal nofb nomodeset video=vesafb:off
 i915.modeset=0  quiet
          175: linux/boot/vmlinuz-5.15.0-100-generic root=/dev/mapper/anapaya--v3--vg-root ro
 noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal nofb nomodeset video=vesafb:off
 i915.modeset=0  quiet
          194: linux/boot/vmlinuz-5.15.0-100-generic root=/dev/mapper/anapaya--v3--vg-root ro
 recovery nomodeset dis_ucode_ldr noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal
 nofb nomodeset video=vesafb:off i915.modeset=0
          214: linux/boot/vmlinuz-5.15.0-86-generic root=/dev/mapper/anapaya--v3--vg-root ro
 noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal nofb nomodeset video=vesafb:off
 i915.modeset=0  quiet
          233: linux/boot/vmlinuz-5.15.0-86-generic root=/dev/mapper/anapaya--v3--vg-root ro
 recovery nomodeset dis_ucode_ldr noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal
 nofb nomodeset video=vesafb:off i915.modeset=0
```

1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration - security

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.

Rationale:

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

Solution

Edit /etc/default/grub and add the 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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
Compliant file(s):
      /boot/grub/grub.cfg - regex '^[\s]*linux[\s]*' found - expect '[Ss][Ee][Cc][Uu][Rr][Ii][Tt]
[Yy]=[^Aa][^Pp][^Pp][^Aa][^Rr][^Mm][^Oo][^Rr]' not found in the following lines:
          155: linux/boot/vmlinuz-5.15.0-100-generic root=/dev/mapper/anapaya--v3--vg-root ro
 noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal nofb nomodeset video=vesafb:off
 i915.modeset=0  quiet
          175: linux/boot/vmlinuz-5.15.0-100-generic root=/dev/mapper/anapaya--v3--vg-root ro
 noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal nofb nomodeset video=vesafb:off
 i915.modeset=0  quiet
          194: linux/boot/vmlinuz-5.15.0-100-generic root=/dev/mapper/anapaya--v3--vg-root ro
 recovery nomodeset dis_ucode_ldr noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal
 nofb nomodeset video=vesafb:off i915.modeset=0
          214: linux/boot/vmlinuz-5.15.0-86-generic root=/dev/mapper/anapaya--v3--vg-root ro
 noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal nofb nomodeset video=vesafb:off
 i915.modeset=0  quiet
          233: linux/boot/vmlinuz-5.15.0-86-generic root=/dev/mapper/anapaya--v3--vg-root ro
 recovery nomodeset dis_ucode_ldr noquiet nosplash console=tty0 console=ttyS0,115200n8 vga=normal
 nofb nomodeset video=vesafb:off i915.modeset=0
```

1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode - loaded

Info

AppArmor profiles define what resources applications are able to access.

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that any policies that exist on the system are activated.

Solution

Run the following command to set all profiles to enforce mode:

aa-enforce /etc/apparmor.d/*

OR Run the following command to set all profiles to complain mode:

aa-complain /etc/apparmor.d/*

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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/sbin/apparmor_status expect: ^[\s]*[1-9][0-9]*[\s]+profiles[\s]+are[\s]+loaded system: Linux

Hosts

192.168.111.1

```
The command '/usr/sbin/apparmor_status' returned :

apparmor module is loaded.
12 profiles are loaded.
12 profiles are in enforce mode.
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /{,usr/}sbin/dhclient
   docker-default
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
   tcpdump
0 profiles are in complain mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
5 processes have profiles defined.
5 processes are in enforce mode.
   /app/appliance (553563) docker-default
   /app/scion-all (553809) docker-default
   /app/scion-all (553855) docker-default
   /otelcol-contrib (1199321) docker-default
   /app/scion-all (1200785) docker-default
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode - unconfined

Info

AppArmor profiles define what resources applications are able to access.

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that any policies that exist on the system are activated.

Solution

Run the following command to set all profiles to enforce mode:

aa-enforce /etc/apparmor.d/*

OR Run the following command to set all profiles to complain mode:

aa-complain /etc/apparmor.d/*

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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/sbin/apparmor_status expect: ^[\s]*0[\s]+processes[\s]+are[\s]+unconfined system: Linux

Hosts

192.168.111.1

```
The command '/usr/sbin/apparmor_status' returned :

apparmor module is loaded.
12 profiles are loaded.
12 profiles are in enforce mode.
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /{,usr/}sbin/dhclient
   docker-default
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
   tcpdump
0 profiles are in complain mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
5 processes have profiles defined.
5 processes are in enforce mode.
   /app/appliance (553563) docker-default
   /app/scion-all (553809) docker-default
   /app/scion-all (553855) docker-default
   /otelcol-contrib (1199321) docker-default
   /app/scion-all (1200785) docker-default
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

1.7.1 Ensure message of the day is configured properly - banner

Info

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

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

Rationale:

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

Solution

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

Run the following command to remove the motd file:

rm /etc/motd

See Also

https://workbench.cisecurity.org/files/4068

References

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

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.7.1 Ensure message of the day is configured properly - platform flags

Info

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

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

Rationale:

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

Solution

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

Run the following command to remove the motd file:

rm /etc/motd

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1082, T1082.000, T1592, T1592.004

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1

GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: \\[mrsv] file: /etc/motd regex: \\[mrsv] required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
```

1.7.2 Ensure local login warning banner is configured properly - platform flags

Info

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

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

Rationale:

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

Solution

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

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1082, T1082.000, T1592, T1592.004

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
GDPR	32.1.b

HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: \\[mrsv] file: /etc/issue regex: \\[mrsv] system: Linux

Hosts

192.168.111.1

```
The file "/etc/issue" does not contain "\\[mrsv]"
```

1.7.3 Ensure remote login warning banner is configured properly - platform flags

Info

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

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

Rationale:

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

Solution

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

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1018, T1018.000, T1082, T1082.000, T1592, T1592.004

TA0007

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
GDPR	32.1.b

HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: \\[mrsv] file: /etc/issue.net regex: \\[mrsv] system: Linux

Hosts

192.168.111.1

```
The file "/etc/issue.net" does not contain "\\[mrsv]"
```

1.7.4 Ensure permissions on /etc/motd are configured

Info

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

Rationale:

If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set permissions on /etc/motd :

chown root:root $(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

Default Value:

File doesn't exist

Additional Information:

If Message of the day is not needing, this file can be removed.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/motd group: root mask: 133 owner: root required: NO system: Linux

Hosts

192.168.111.1

1.7.5 Ensure permissions on /etc/issue are configured

Info

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

Rationale:

If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set permissions on /etc/issue :

chown root:root $(readlink -e /etc/issue) # chmod u-x,go-wx $(readlink -e /etc/issue)

Default Value:

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

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/issue group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
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
```

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

Info

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

Rationale:

If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set permissions on /etc/issue.net :

chown root:root $(readlink -e /etc/issue.net) # chmod u-x,go-wx $(readlink -e /etc/issue.net)

Default Value:

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

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/issue.net group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
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
```

1.8.2 Ensure GDM login banner is configured - banner-message-enable

Info

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

Rationale:

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

Solution

Run the following script to verify that the banner message is enabled and set:

#!/usr/bin/env bash

{ l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done if [-n '$l_pkgoutput']; then

l_gdmprofile='gdm' # Set this to desired profile name IaW Local site policy l_bmessage=''Authorized uses only. All activity may be monitored and reported'' # Set to desired banner message if [! -f '/etc/dconf/profile/$l_gdmprofile']; then echo 'Creating profile '$l_gdmprofile''

echo -e 'user-db:user system-db:$l_gdmprofile file-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults' > /etc/dconf/profile/$l_gdmprofile fi if [! -d '/etc/dconf/db/$l_gdmprofile.d/']; then echo 'Creating dconf database directory '/etc/dconf/db/$l_gdmprofile.d/''

mkdir /etc/dconf/db/$l_gdmprofile.d/ fi if ! grep -Piq '^h*banner-message-enableh*=h*trueb' /etc/dconf/db/$l_gdmprofile.d/*; then echo 'creating gdm keyfile for machine-wide settings'

if ! grep -Piq -- '^h*banner-message-enableh*=h*' /etc/dconf/db/$l_gdmprofile.d/*; then l_kfile='/etc/dconf/db/$l_gdmprofile.d/01-banner-message'

echo -e '

[org/gnome/login-screen] banner-message-enable=true' >> '$l_kfile'

else l_kfile='$(grep -Pil -- '^h*banner-message-enableh*=h*' /etc/dconf/db/$l_gdmprofile.d/*)'

! grep -Pq '^h*[org/gnome/login-screen]' '$l_kfile' && sed -ri '/^s*banner-message-enable/ i[org/gnome/login-screen]' '$l_kfile'

! grep -Pq '^h*banner-message-enableh*=h*trueb' '$l_kfile' && sed -ri 's/^s*(banner-message-enables*=s*)(S+)(s*.*$)/1true 3//' '$l_kfile'

sed -ri '/^s*[org/gnome/login-screen]/ a banner-message-enable=true' '$l_kfile'

fi fi if ! grep -Piq '^h*banner-message-text=['']+S+' '$l_kfile'; then sed -ri '/^s*banner-message-enable/ abanner-message-text=$l_bmessage' '$l_kfile'

fi dconf update else echo -e '

- GNOME Desktop Manager isn't installed
- Recommendation is Not Applicable
- No remediation required '

fi }

Note:

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.

OR

Run the following command to remove the gdm3 package:

apt purge gdm3

Default Value:

disabled

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.9
800-53	AC-8a.
800-53R5	AC-8a.
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8a.
LEVEL	1A
NESA	M5.2.5
NESA	T5.5.1
NIAV2	AM10a
NIAV2	AM10b
NIAV2	AM10c
NIAV2	AM10d
NIAV2	AM10e
TBA-FIISB	45.2.4

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.2 Ensure GDM login banner is configured - banner-message-text

Info

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

Rationale:

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

Solution

Run the following script to verify that the banner message is enabled and set:

#!/usr/bin/env bash

{ l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done if [-n '$l_pkgoutput']; then

l_gdmprofile='gdm' # Set this to desired profile name IaW Local site policy l_bmessage=''Authorized uses only. All activity may be monitored and reported'' # Set to desired banner message if [! -f '/etc/dconf/profile/$l_gdmprofile']; then echo 'Creating profile '$l_gdmprofile''

echo -e 'user-db:user system-db:$l_gdmprofile file-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults' > /etc/dconf/profile/$l_gdmprofile fi if [! -d '/etc/dconf/db/$l_gdmprofile.d/']; then echo 'Creating dconf database directory '/etc/dconf/db/$l_gdmprofile.d/''

mkdir /etc/dconf/db/$l_gdmprofile.d/ fi if ! grep -Piq '^h*banner-message-enableh*=h*trueb' /etc/dconf/db/$l_gdmprofile.d/*; then echo 'creating gdm keyfile for machine-wide settings'

if ! grep -Piq -- '^h*banner-message-enableh*=h*' /etc/dconf/db/$l_gdmprofile.d/*; then l_kfile='/etc/dconf/db/$l_gdmprofile.d/01-banner-message'

echo -e '

[org/gnome/login-screen] banner-message-enable=true' >> '$l_kfile'

else l_kfile='$(grep -Pil -- '^h*banner-message-enableh*=h*' /etc/dconf/db/$l_gdmprofile.d/*)'

! grep -Pq '^h*[org/gnome/login-screen]' '$l_kfile' && sed -ri '/^s*banner-message-enable/ i[org/gnome/login-screen]' '$l_kfile'

! grep -Pq '^h*banner-message-enableh*=h*trueb' '$l_kfile' && sed -ri 's/^s*(banner-message-enables*=s*)(S+)(s*.*$)/1true 3//' '$l_kfile'

sed -ri '/^s*[org/gnome/login-screen]/ a banner-message-enable=true' '$l_kfile'

fi fi if ! grep -Piq '^h*banner-message-text=['']+S+' '$l_kfile'; then sed -ri '/^s*banner-message-enable/ abanner-message-text=$l_bmessage' '$l_kfile'

fi dconf update else echo -e '

- GNOME Desktop Manager isn't installed
- Recommendation is Not Applicable
- No remediation required '

fi }

Note:

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.

OR

Run the following command to remove the gdm3 package:

apt purge gdm3

Default Value:

disabled

See Also

https://workbench.cisecurity.org/files/4068

References

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

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.3 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

Rationale:

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Solution

Run the following script to enable the disable-user-list option:

Note: the l_gdm_profile variable in the script can be changed if a different profile name is desired in accordance with local site policy.

#!/usr/bin/env bash

{ l_gdmprofile='gdm'

if [! -f '/etc/dconf/profile/$l_gdmprofile']; then echo 'Creating profile '$l_gdmprofile''

echo -e 'user-db:user system-db:$l_gdmprofile file-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults' > /etc/dconf/profile/$l_gdmprofile fi if [! -d '/etc/dconf/db/$l_gdmprofile.d/']; then echo 'Creating dconf database directory '/etc/dconf/db/$l_gdmprofile.d/''

mkdir /etc/dconf/db/$l_gdmprofile.d/ fi if ! grep -Piq '^h*disable-user-listh*=h*trueb' /etc/dconf/db/$l_gdmprofile.d/*; then echo 'creating gdm keyfile for machine-wide settings'

if ! grep -Piq -- '^h*[org/gnome/login-screen]' /etc/dconf/db/$l_gdmprofile.d/*; then echo -e '

[org/gnome/login-screen] # Do not show the user list disable-user-list=true' >> /etc/dconf/db/$l_gdmprofile.d/00-login-screen else sed -ri '/^s*[org/gnome/login-screen]/ a# Do not show the user list disable-user-list=true' $(grep -Pil -- '^h*[org/gnome/login-screen]' /etc/dconf/db/$l_gdmprofile.d/*) fi fi 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.

OR Run the following command to remove the GNOME package:

apt purge gdm3

Default Value:

false

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.6
800-171	3.4.7
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
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.4 Ensure GDM screen locks when the user is idle - idle-delay

Info

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

idle-delay=uint32 {n} - Number of seconds of inactivity before the screen goes blank

lock-delay=uint32 {n} - Number of seconds after the screen is blank before locking the screen

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 900

Specify the dconf path

[org/gnome/desktop/screensaver]

Number of seconds after the screen is blank before locking the screen

lock-delay=uint32 5

Rationale:

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

Create or edit a file 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.

Example:

echo -e '

user-db:user system-db:local' >> /etc/dconf/profile/user

Create the directory /etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/ if it doesn't already exist:

Example:

mkdir /etc/dconf/db/local.d

Create the key file '/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/{FILE_NAME} to provide information for the {NAME_OF_DCONF_DATABASE} database:

Example script:

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

{ l_key_file='/etc/dconf/db/local.d/00-screensaver'
l_idmv='900' # Set max value for idle-delay in seconds (between 1 and 900) l_ldmv='5' # Set max value for lock-delay in seconds (between 0 and 5) { echo '# Specify the dconf path'
echo '[org/gnome/desktop/session]'
echo ''
echo '# Number of seconds of inactivity before the screen goes blank'
echo '# Set to 0 seconds if you want to deactivate the screensaver.'
echo 'idle-delay=uint32 $l_idmv'
echo ''
echo '# Specify the dconf path'
echo '[org/gnome/desktop/screensaver]'
echo ''
echo '# Number of seconds after the screen is blank before locking the screen'
echo 'lock-delay=uint32 $l_ldmv'
} > '$l_key_file'
}
```

Note: You must include the uint32 along with the integer key values as shown.

Run the following command to update the system 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/files/4068

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.4 Ensure GDM screen locks when the user is idle - lock-delay

Info

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

idle-delay=uint32 {n} - Number of seconds of inactivity before the screen goes blank

lock-delay=uint32 {n} - Number of seconds after the screen is blank before locking the screen

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 900

Specify the dconf path

[org/gnome/desktop/screensaver]

Number of seconds after the screen is blank before locking the screen

lock-delay=uint32 5

Rationale:

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

Create or edit a file 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.

Example:

echo -e '

user-db:user system-db:local' >> /etc/dconf/profile/user

Create the directory /etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/ if it doesn't already exist:

Example:

mkdir /etc/dconf/db/local.d

Create the key file '/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/{FILE_NAME} to provide information for the {NAME_OF_DCONF_DATABASE} database:

Example script:

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

{ l_key_file='/etc/dconf/db/local.d/00-screensaver'

l_idmv='900' # Set max value for idle-delay in seconds (between 1 and 900) l_ldmv='5' # Set max value for lock-delay in seconds (between 0 and 5) { echo '# Specify the dconf path'

echo '[org/gnome/desktop/session]'

echo ''

echo '# Number of seconds of inactivity before the screen goes blank'

echo '# Set to 0 seconds if you want to deactivate the screensaver.'

echo 'idle-delay=uint32 $l_idmv'

echo ''

echo '# Specify the dconf path'

echo '[org/gnome/desktop/screensaver]'

echo ''

echo '# Number of seconds after the screen is blank before locking the screen'

echo 'lock-delay=uint32 $l_ldmv'

} > '$l_key_file'

}
```

Note: You must include the uint32 along with the integer key values as shown.

Run the following command to update the system 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/files/4068

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.5 Ensure GDM screen locks cannot be overridden - idle-delay

Info

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

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.

Example Lock File:

Lock desktop screensaver settings

/org/gnome/desktop/session/idle-delay

/org/gnome/desktop/screensaver/lock-delay

Rationale:

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

Run the following script to ensure screen locks can not be overridden:

#!/usr/bin/env bash

{ # Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for idle-delay to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*idle-delayh*=h*uint32h +d+b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked # Look for lock-delay to determine profile in use, needed for remaining tests l_kfd2='/etc/dconf/db/$(grep -Psril '^h*lock-delayh*=h*uint32h+d+b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -Prilq '^h*/org/gnome/desktop/session/idle-delayb' '$l_kfd'; then echo ' - 'idle-delay' is locked in '$(grep -Pril '^h*/org/gnome/desktop/session/idle-delayb' '$l_kfd')''

else echo 'creating entry to lock 'idle-delay''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop screensaver idle-delay setting'

echo '/org/gnome/desktop/session/idle-delay'

} >> '$l_kfd'/locks/00-screensaver fi else echo -e ' - 'idle-delay' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM screen locks when the user is idle' and follow this Recommendation again'

fi if [-d '$l_kfd2']; then # If key file directory doesn't exist, options can't be locked if grep -Prilq '^h*/org/gnome/desktop/screensaver/lock-delayb' '$l_kfd2'; then echo ' - 'lock-delay' is locked in '$(grep -Pril '^h*/org/gnome/desktop/screensaver/lock-delayb' '$l_kfd2')''

else echo 'creating entry to lock 'lock-delay''

[! -d '$l_kfd2'/locks] && echo 'creating directory $l_kfd2/locks' && mkdir '$l_kfd2'/locks { echo -e '

Lock desktop screensaver lock-delay setting'

echo '/org/gnome/desktop/screensaver/lock-delay'

} >> '$l_kfd2'/locks/00-screensaver fi else echo -e ' - 'lock-delay' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM screen locks when the user is idle' and follow this Recommendation again'

fi else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

Run the following command to update the system 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/files/4068

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.5 Ensure GDM screen locks cannot be overridden - lock-delay

Info

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

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.

Example Lock File:

Lock desktop screensaver settings

/org/gnome/desktop/session/idle-delay

/org/gnome/desktop/screensaver/lock-delay

Rationale:

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

Run the following script to ensure screen locks can not be overridden:

#!/usr/bin/env bash

{ # Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for idle-delay to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*idle-delayh*=h*uint32h +d+b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked # Look for lock-delay to determine profile in use, needed for remaining tests l_kfd2='/etc/dconf/db/$(grep -Psril '^h*lock-delayh*=h*uint32h+d+b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -Prilq '^h*/org/gnome/desktop/session/idle-delayb' '$l_kfd'; then echo ' - 'idle-delay' is locked in '$(grep -Pril '^h*/org/gnome/desktop/session/idle-delayb' '$l_kfd')''

else echo 'creating entry to lock 'idle-delay''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop screensaver idle-delay setting'

echo '/org/gnome/desktop/session/idle-delay'

} >> '$l_kfd'/locks/00-screensaver fi else echo -e ' - 'idle-delay' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM screen locks when the user is idle' and follow this Recommendation again'

fi if [-d '$l_kfd2']; then # If key file directory doesn't exist, options can't be locked if grep -Prilq '^h*/org/gnome/desktop/screensaver/lock-delayb' '$l_kfd2'; then echo ' - 'lock-delay' is locked in '$(grep -Pril '^h*/org/gnome/desktop/screensaver/lock-delayb' '$l_kfd2')''

else echo 'creating entry to lock 'lock-delay''

[! -d '$l_kfd2'/locks] && echo 'creating directory $l_kfd2/locks' && mkdir '$l_kfd2'/locks { echo -e '

Lock desktop screensaver lock-delay setting'

echo '/org/gnome/desktop/screensaver/lock-delay'

} >> '$l_kfd2'/locks/00-screensaver fi else echo -e ' - 'lock-delay' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM screen locks when the user is idle' and follow this Recommendation again'

fi else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

Run the following command to update the system 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/files/4068

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.6 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.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

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.

Solution

Run the following script to disable automatic mounting of media for all GNOME users:

#!/usr/bin/env bash

{ l_pkgoutput='' l_output='' l_output2=''

l_gpbame='local' # Set to desired dconf profile name (defaule is local) # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done echo -e '$l_packageout'

Check configuration (If applicable) if [-n '$l_pkgoutput']; then echo -e '$l_pkgoutput'

Look for existing settings and set variables if they exist l_kfile='$(grep -Prils -- '^h*automountb' /etc/dconf/db/*.d)'

l_kfile2='$(grep -Prils -- '^h*automount-openb' /etc/dconf/db/*.d)'

Set profile name based on dconf db directory ({PROFILE_NAME}.d) if [-f '$l_kfile']; then l_gpname='$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile')'

echo ' - updating dconf profile name to '$l_gpname''

elif [-f '$l_kfile2']; then l_gpname='$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile2')'

echo ' - updating dconf profile name to '$l_gpname''

fi # check for consistency (Clean up configuration if needed) if [-f '$l_kfile'] && ['$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile')' != '$l_gpname']; then sed -ri '/^s*automounts*=/s/^/# /' '$l_kfile'

l_kfile='/etc/dconf/db/$l_gpname.d/00-media-automount'

fi if [-f '$l_kfile2'] && ['$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile2')' != '$l_gpname']; then sed -ri '/^s*automount-opens*=/s/^/# /' '$l_kfile2'

fi [-n '$l_kfile'] && l_kfile='/etc/dconf/db/$l_gpname.d/00-media-automount'

Check if profile file exists if grep -Pq -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*; then echo -e '

- dconf database profile exists in: '$(grep -Pl -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*)''

else [! -f '/etc/dconf/profile/user'] && l_gpfile='/etc/dconf/profile/user' || l_gpfile='/etc/dconf/profile/user2'

echo -e ' - creating dconf database profile'

{ echo -e '

user-db:user'

echo 'system-db:$l_gpname'

} >> '$l_gpfile'

fi # create dconf directory if it doesn't exists l_gpdir='/etc/dconf/db/$l_gpname.d'

if [-d '$l_gpdir']; then echo ' - The dconf database directory '$l_gpdir' exists'

else echo ' - creating dconf database directory '$l_gpdir''

mkdir '$l_gpdir'

fi # check automount-open setting if grep -Pqs -- '^h*automount-openh*=h*falseb' '$l_kfile'; then echo ' - 'automount-open' is set to false in: '$l_kfile''

else echo ' - creating 'automount-open' entry in '$l_kfile''

! grep -Psq -- '^h*[org/gnome/desktop/media-handling]b' '$l_kfile' && echo '[org/gnome/desktop/media-handling]' >> '$l_kfile'

sed -ri '/^s*[org/gnome/desktop/media-handling]/a automount-open=false'

fi # check automount setting if grep -Pqs -- '^h*automounth*=h*falseb' '$l_kfile'; then echo ' - 'automount' is set to false in: '$l_kfile''

else echo ' - creating 'automount' entry in '$l_kfile''

! grep -Psq -- '^h*[org/gnome/desktop/media-handling]b' '$l_kfile' && echo '[org/gnome/desktop/media-handling]' >> '$l_kfile'

sed -ri '/^s*[org/gnome/desktop/media-handling]/a automount=false'

fi else echo -e '

- GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi # update dconf database dconf update }

OR Run the following command to uninstall the GNOME desktop Manager package:

apt purge gdm3

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.7 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.

Example Lock File:

Lock desktop screensaver settings

/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users

Solution

Run the following script to lock disable automatic mounting of media for all GNOME users:

#!/usr/bin/env bash

{ # Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for automount to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*automountb' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked # Look for automount-open to determine profile in use, needed for remaining tests l_kfd2='/etc/dconf/db/$(grep -Psril '^h*automount-openb' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -

Priq '^h*/org/gnome/desktop/media-handling/automountb' '$l_kfd'; then echo ' - 'automount' is locked in '$(grep -Pril '^h*/org/gnome/desktop/media-handling/automountb' '$l_kfd')''

else echo ' - creating entry to lock 'automount''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop media-handling automount setting'

echo '/org/gnome/desktop/media-handling/automount'

} >> '$l_kfd'/locks/00-media-automount fi else echo -e ' - 'automount' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM automatic mounting of removable media is disabled' and follow this Recommendation again'

fi if [-d '$l_kfd2']; then # If key file directory doesn't exist, options can't be locked if grep -Priq '^h*/org/gnome/desktop/media-handling/automount-openb' '$l_kfd2'; then echo ' - 'automount-open' is locked in '$(grep -Pril '^h*/org/gnome/desktop/media-handling/automount-openb' '$l_kfd2')''

else echo ' - creating entry to lock 'automount-open''

[! -d '$l_kfd2'/locks] && echo 'creating directory $l_kfd2/locks' && mkdir '$l_kfd2'/locks { echo -e '

Lock desktop media-handling automount-open setting'

echo '/org/gnome/desktop/media-handling/automount-open'

} >> '$l_kfd2'/locks/00-media-automount fi else echo -e ' - 'automount-open' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM automatic mounting of removable media is disabled' and follow this Recommendation again'

fi # update dconf database dconf update else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A

LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.8 Ensure GDM autorun-never is enabled

Info

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

Rationale:

Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.

Solution

Run the following script to set autorun-never to true for GDM users:

#!/usr/bin/env bash

{ l_pkgoutput='' l_output='' l_output2=''

l_gpname='local' # Set to desired dconf profile name (default is local) # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space separated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done echo -e '$l_pkgoutput'

Check configuration (If applicable) if [-n '$l_pkgoutput']; then echo -e '$l_pkgoutput'

Look for existing settings and set variables if they exist l_kfile='$(grep -Prils -- '^h*autorun-neverb' /etc/dconf/db/*.d)'

Set profile name based on dconf db directory ({PROFILE_NAME}.d) if [-f '$l_kfile']; then l_gpname='$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile')'

echo ' - updating dconf profile name to '$l_gpname''

fi [! -f '$l_kfile'] && l_kfile='/etc/dconf/db/$l_gpname.d/00-media-autorun'

Check if profile file exists if grep -Pq -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*; then echo -e '

- dconf database profile exists in: '$(grep -Pl -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*)''

else [! -f '/etc/dconf/profile/user'] && l_gpfile='/etc/dconf/profile/user' || l_gpfile='/etc/dconf/profile/user2'

echo -e ' - creating dconf database profile'

{ echo -e '

user-db:user'

echo 'system-db:$l_gpname'

} >> '$l_gpfile'

fi # create dconf directory if it doesn't exists l_gpdir='/etc/dconf/db/$l_gpname.d'

if [-d '$l_gpdir']; then echo ' - The dconf database directory '$l_gpdir' exists'

else echo ' - creating dconf database directory '$l_gpdir''

mkdir '$l_gpdir'

fi # check autorun-never setting if grep -Pqs -- '^h*autorun-neverh*=h*trueb' '$l_kfile'; then echo ' - 'autorun-never' is set to true in: '$l_kfile''

else echo ' - creating or updating 'autorun-never' entry in '$l_kfile''

if grep -Psq -- '^h*autorun-never' '$l_kfile'; then sed -ri 's/(^s*autorun-nevers*=s*)(S+)(s*.*)$/1true 3/' '$l_kfile'

else ! grep -Psq -- '^h*[org/gnome/desktop/media-handling]b' '$l_kfile' && echo '[org/gnome/desktop/media-handling]' >> '$l_kfile'

sed -ri '/^s*[org/gnome/desktop/media-handling]/a autorun-never=true' '$l_kfile'

fi fi else echo -e '

- GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi # update dconf database dconf update }

Default Value:

false

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.9 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.

Example Lock File:

Lock desktop media-handling settings

/org/gnome/desktop/media-handling/autorun-never

Rationale:

Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.

Solution

Run the following script to ensure that autorun-never=true cannot be overridden:

#!/usr/bin/env bash

{ # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space separated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for autorun to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*autorun-neverb' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -Priq '^h*/org/gnome/desktop/media-handling/autorun-neverb' '$l_kfd'; then echo ' - 'autorun-never' is locked in '$(grep -Pril '^h*/org/gnome/desktop/media-handling/autorun-neverb' '$l_kfd')''

else echo ' - creating entry to lock 'autorun-never''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop media-handling autorun-never setting'

echo '/org/gnome/desktop/media-handling/autorun-never'

} >> '$l_kfd'/locks/00-media-autorun fi else echo -e ' - 'autorun-never' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM autorun-never is enabled' and follow this Recommendation again'

fi # update dconf database dconf update else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.8.10 Ensure XDCMP is not enabled

Info

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

Rationale:

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 the file /etc/gdm3/custom.conf and remove the line:

Enable=true

Default Value:

false (This is denoted by no Enabled= entry in the file /etc/gdm3/custom.conf in the [xdmcp] section

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

1.9 Ensure updates, patches, and additional security software are installed

Info

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Rationale:

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

Solution

Run the following command to update all packages following local site policy guidance on applying updates and patches:

apt upgrade

OR

apt dist-upgrade

Additional Information:

Site policy may mandate a testing period before install onto production systems for available updates.

upgrade - is used to install the newest versions of all packages currently installed on the system from the sources enumerated in /etc/apt/sources.list. Packages currently installed with new versions available are retrieved and upgraded; under no circumstances are currently installed packages removed, or packages not already installed retrieved and installed. New versions of currently installed packages that cannot be upgraded without changing the install status of another package will be left at their current version. An update must be performed first so that apt knows that new versions of packages are available.

dist-upgrade - in addition to performing the function of upgrade, also intelligently handles changing dependencies with new versions of packages; apt has a 'smart' conflict resolution system, and it will attempt to upgrade the most important packages at the expense of less important ones if necessary. So, dist-upgrade command may remove some packages. The /etc/apt/sources.list file contains a list of locations from which to retrieve desired package files. See also apt_preferences(5) for a mechanism for overriding the general settings for individual packages.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.11.2
800-171	3.11.3

800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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
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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/apt-get -s upgrade | egrep -v '(Reading|Building|Calculating)'

expect: ^[\s]*0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/apt-get -s upgrade | egrep -v '(Reading|Building|Calculating)'' returned :

0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

2.1.1.1 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

Rationale:

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 three time synchronization daemons; chrony (1), systemd-timesyncd (2), or ntp (3), 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 --now mask systemd-timesyncd.service

Run the following command to remove the ntp package:

apt purge ntp

NOTE:

Subsection: Configure chrony should be followed

Subsections: Configure systemd-timesyncd and Configure ntp should be skipped

systemd-timesyncd

Run the following command to remove the chrony package:

apt purge chrony

Run the following command to remove the ntp package:

apt purge ntp

NOTE:

Subsection: Configure systemd-timesyncd should be followed

Subsections: Configure chrony and Configure ntp should be skipped

ntp

Run the following command to install ntp:

apt install ntp

Run the following commands to stop and mask the systemd-timesyncd daemon:

systemctl stop systemd-timesyncd.service

systemctl --now mask systemd-timesyncd.service

Run the following command to remove the chrony package:

apt purge chrony

NOTE:

Subsection: Configure ntp should be followed

Subsections: Configure chrony and Configure systemd-timesyncd should be skipped

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.2.1 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.

Rationale:

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 in .sources in /etc/chrony/sources.d/ and add or edit server or pool lines as appropriate according to local site policy:

<[server|pool]> <[remote-server|remote-pool]>

Examples:
pool directive:

pool time.nist.gov iburst maxsources 4 #The maxsources option is unique to the pool directive

server directive:

server time-a-g.nist.gov iburst server 132.163.97.3 iburst server time-d-b.nist.gov iburst

Run one of the following commands to load the updated time sources into chronyd running config:

systemctl restart chronyd

- OR if sources are in a .sources file -

chronyc reload sources

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
```

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.2.2 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

Rationale:

The chronyd service should run with only the required privileges

Solution

Add or edit the user line to /etc/chrony/chrony.conf or a file ending in .conf 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

Default Value:

user _chrony

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.2.3 Ensure chrony is enabled and running - enabled

Info

chrony is a daemon for synchronizing the system clock across the network

Rationale:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.2.3 Ensure chrony is enabled and running - running

Info

chrony is a daemon for synchronizing the system clock across the network

Rationale:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver - FallbackNTP

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.

Rationale:

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 or create a file in /etc/systemd/timesyncd.conf.d ending in .conf and add the NTP= and/or FallbackNTP= lines to the [Time] section:

Example:

[Time] NTP=time.nist.gov # Uses the generic name for NIST's time servers

-AND/OR- FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov # Space separated list of NIST time servers

Note: Servers added to these line(s) should follow local site policy. NIST servers are for example. The timesyncd.conf.d directory may need to be created Example script: The following example script will create the systemd-timesyncd drop-in configuration snippet:

#!/usr/bin/env bash

ntp_ts='time.nist.gov'

ntp_fb='time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov'

disfile='/etc/systemd/timesyncd.conf.d/50-timesyncd.conf'

if ! find /etc/systemd -type f -name '*.conf' -exec grep -Ph '^h*NTP=H+' {} +; then [! -d /etc/systemd/timesyncd.conf.d] && mkdir /etc/systemd/timesyncd.conf.d ! grep -Pqs '^h*[Time]' '$disfile' && echo '[Time]' >> '$disfile'

echo 'NTP=$ntp_ts' >> '$disfile'

fi if ! find /etc/systemd -type f -name '*.conf' -exec grep -Ph '^h*FallbackNTP=H+' {} +; then [! -d /etc/systemd/timesyncd.conf.d] && mkdir /etc/systemd/timesyncd.conf.d ! grep -Pqs '^h*[Time]' '$disfile' && echo '[Time]' >> '$disfile'

echo 'FallbackNTP=$ntp_fb' >> '$disfile'

fi

Run the following command to reload the systemd-timesyncd configuration:

systemctl try-reload-or-restart systemd-timesyncd

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

Default Value:

#NTP=

#FallbackNPT=

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^FallbackNTP[\s]*=ntp.ubuntu.com file: /etc/systemd/timesyncd.conf regex: ^FallbackNTP[\s]*= system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /etc/systemd/timesyncd.conf - regex '^FallbackNTP[\s]*=' found - expect
 '^FallbackNTP[\s]*=ntp.ubuntu.com' found in the following lines:
          16: FallbackNTP=ntp.ubuntu.com
```

2.1.3.2 Ensure systemd-timesyncd is enabled and running - enabled

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network

Rationale:

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/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl is-enabled systemd-timesyncd expect: enabled system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl is-enabled systemd-timesyncd' returned :

enabled
```

2.1.3.2 Ensure systemd-timesyncd is enabled and running - running

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network

Rationale:

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/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl is-active systemd-timesyncd expect: active system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl is-active systemd-timesyncd' returned :

active
```

2.1.4.1 Ensure ntp access control is configured - restrict -4

Info

ntp Access Control Commands:

restrict address [mask mask] [ippeerlimit int] [flag ...]

The address argument expressed in dotted-quad form is the address of a host or network. Alternatively, the address argument can be a valid host DNS name.

The mask argument expressed in dotted-quad form defaults to 255.255.255.255, meaning that the address is treated as the address of an individual host. A default entry (address 0.0.0.0, mask 0.0.0.0) is always included and is always the first entry in the list. Note: the text string default, with no mask option, may be used to indicate the default entry.

The ippeerlimit directive limits the number of peer requests for each IP to int, where a value of -1 means 'unlimited', the current default. A value of 0 means 'none'. There would usually be at most 1 peering request per IP, but if the remote peering requests are behind a proxy there could well be more than 1 per IP. In the current implementation, flag always restricts access, i.e., an entry with no flags indicates that free access to the server is to be given.

The flags are not orthogonal, in that more restrictive flags will often make less restrictive ones redundant. The flags can generally be classed into two categories, those which restrict time service and those which restrict informational queries and attempts to do run-time reconfiguration of the server.

One or more of the following flags may be specified:

kod - If this flag is set when an access violation occurs, a kiss-o'-death (KoD) packet is sent. KoD packets are rate limited to no more than one per second. If another KoD packet occurs within one second after the last one, the packet is dropped.

limited - Deny service if the packet spacing violates the lower limits specified in the discard command. A history of clients is kept using the monitoring capability of ntpd. Thus, monitoring is always active as long as there is a restriction entry with the limited flag.

lowpriotrap - Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.

noepeer - Deny ephemeral peer requests, even if they come from an authenticated source. Note that the ability to use a symmetric key for authentication may be restricted to one or more IPs or subnets via the third field of the ntp.keys file. This restriction is not enabled by default, to maintain backward compatibility. Expect noepeer to become the default in ntp-4.4.

nomodify - Deny ntpq and ntpdc queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

noquery - Deny ntpq and ntpdc queries. Time service is not affected.

nopeer - Deny unauthenticated packets which would result in mobilizing a new association. This includes broadcast and symmetric active packets when a configured association does not exist. It also includes pool associations, so if you want to use servers from a pool directive and also want to use nopeer by default, you'll want a restrict source ... line as well that does not include the nopeer directive.

noserve - Deny all packets except ntpq and ntpdc queries.

notrap - Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the ntpq control message protocol which is intended for use by remote event logging programs.

notrust - Deny service unless the packet is cryptographically authenticated.

ntpport - This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both ntpport and non-ntpport may be specified. The ntpport is considered more specific and is sorted later in the list.

Rationale:

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

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:

restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery

OR If another time synchronization service is in use on the system, run the following command to remove ntp from the system:

apt purge ntp

Default Value:

restrict -4 default kod notrap nomodify nopeer noquery limited

restrict -6 default kod notrap nomodify nopeer noquery limited

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.4.1 Ensure ntp access control is configured - restrict -6

Info

ntp Access Control Commands:

restrict address [mask mask] [ippeerlimit int] [flag ...]

The address argument expressed in dotted-quad form is the address of a host or network. Alternatively, the address argument can be a valid host DNS name.

The mask argument expressed in dotted-quad form defaults to 255.255.255.255, meaning that the address is treated as the address of an individual host. A default entry (address 0.0.0.0, mask 0.0.0.0) is always included and is always the first entry in the list. Note: the text string default, with no mask option, may be used to indicate the default entry.

The ippeerlimit directive limits the number of peer requests for each IP to int, where a value of -1 means 'unlimited', the current default. A value of 0 means 'none'. There would usually be at most 1 peering request per IP, but if the remote peering requests are behind a proxy there could well be more than 1 per IP. In the current implementation, flag always restricts access, i.e., an entry with no flags indicates that free access to the server is to be given.

The flags are not orthogonal, in that more restrictive flags will often make less restrictive ones redundant. The flags can generally be classed into two categories, those which restrict time service and those which restrict informational queries and attempts to do run-time reconfiguration of the server.

One or more of the following flags may be specified:

kod - If this flag is set when an access violation occurs, a kiss-o'-death (KoD) packet is sent. KoD packets are rate limited to no more than one per second. If another KoD packet occurs within one second after the last one, the packet is dropped.

limited - Deny service if the packet spacing violates the lower limits specified in the discard command. A history of clients is kept using the monitoring capability of ntpd. Thus, monitoring is always active as long as there is a restriction entry with the limited flag.

lowpriotrap - Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.

noepeer - Deny ephemeral peer requests, even if they come from an authenticated source. Note that the ability to use a symmetric key for authentication may be restricted to one or more IPs or subnets via the third field of the ntp.keys file. This restriction is not enabled by default, to maintain backward compatibility. Expect noepeer to become the default in ntp-4.4.

nomodify - Deny ntpq and ntpdc queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.

noquery - Deny ntpq and ntpdc queries. Time service is not affected.

nopeer - Deny unauthenticated packets which would result in mobilizing a new association. This includes broadcast and symmetric active packets when a configured association does not exist. It also includes pool associations, so if you want to use servers from a pool directive and also want to use nopeer by default, you'll want a restrict source ... line as well that does not include the nopeer directive.

noserve - Deny all packets except ntpq and ntpdc queries.

notrap - Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the ntpq control message protocol which is intended for use by remote event logging programs.

notrust - Deny service unless the packet is cryptographically authenticated.

ntpport - This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both ntpport and non-ntpport may be specified. The ntpport is considered more specific and is sorted later in the list.

Rationale:

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

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:

restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery

OR If another time synchronization service is in use on the system, run the following command to remove ntp from the system:

apt purge ntp

Default Value:

restrict -4 default kod notrap nomodify nopeer noquery limited

restrict -6 default kod notrap nomodify nopeer noquery limited

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.4.2 Ensure ntp is configured with authorized timeserver

Info

The various modes are determined by the command keyword and the type of the required IP address. Addresses are classed by type as (s) a remote server or peer (IPv4 class A, B and C), (b) the broadcast address of a local interface, (m) a multicast address (IPv4 class D), or (r) a reference clock address (127.127.x.x).

Note: That only those options applicable to each command are listed below. Use of options not listed may not be caught as an error, but may result in some weird and even destructive behavior.

If the Basic Socket Interface Extensions for IPv6 (RFC-2553) is detected, support for the IPv6 address family is generated in addition to the default support of the IPv4 address family. In a few cases, including the reslist billboard generated by ntpq or ntpdc, IPv6 addresses are automatically generated. IPv6 addresses can be identified by the presence of colons ':' in the address field. IPv6 addresses can be used almost everywhere where IPv4 addresses can be used, with the exception of reference clock addresses, which are always IPv4.

Note: In contexts where a host name is expected, a -4 qualifier preceding the host name forces DNS resolution to the IPv4 namespace, while a -6 qualifier forces DNS resolution to the IPv6 namespace. See IPv6 references for the equivalent classes for that address family.

pool - For type s addresses, this command mobilizes a persistent client mode association with a number of remote servers. In this mode the local clock can synchronized to the remote server, but the remote server can never be synchronized to the local clock.

server - For type s and r addresses, this command mobilizes a persistent client mode association with the specified remote server or local radio clock. In this mode the local clock can synchronized to the remote server, but the remote server can never be synchronized to the local clock. This command should not be used for type b or m addresses.

Rationale:

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/ntp.conf and add or edit server or pool lines as appropriate according to local site policy:

<[server|pool]> <[remote-server|remote-pool]>

Examples:

pool mode:

pool time.nist.gov iburst

server mode:

server time-a-g.nist.gov iburst server 132.163.97.3 iburst server time-d-b.nist.gov iburst

Run the following command to load the updated time sources into ntp running config:

systemctl restart ntp

OR If another time synchronization service is in use on the system, run the following command to remove ntp from the system:

apt purge ntp

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.4.3 Ensure ntp is running as user ntp

Info

The ntp package is installed with a dedicated user account ntp. This account is granted the access required by the ntpd daemon

Note:

If chrony or systemd-timesyncd are used, ntp should be removed and this section skipped

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

Only one time synchronization method should be in use on the system

Rationale:

The ntpd daemon should run with only the required privlidge

Solution

Add or edit the following line in /etc/init.d/ntp:

RUNASUSER=ntp

Run the following command to restart ntp.servocee:

systemctl restart ntp.service

OR If another time synchronization service is in use on the system, run the following command to remove ntp from the system:

apt purge ntp

Default Value:

user ntp

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.4.4 Ensure ntp is enabled and running - active

Info

ntp is a daemon for synchronizing the system clock across the network

Rationale:

ntp 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 ntp is in use on the system, run the following commands:

Run the following command to unmask ntp.service:

systemctl unmask ntp.service

Run the following command to enable and start ntp.service:

systemctl --now enable ntp.service

OR If another time synchronization service is in use on the system, run the following command to remove ntp:

apt purge ntp

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.1.4.4 Ensure ntp is enabled and running - enabled

Info

ntp is a daemon for synchronizing the system clock across the network

Rationale:

ntp 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 ntp is in use on the system, run the following commands:

Run the following command to unmask ntp.service:

systemctl unmask ntp.service

Run the following command to enable and start ntp.service:

systemctl --now enable ntp.service

OR If another time synchronization service is in use on the system, run the following command to remove ntp:

apt purge ntp

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.2.1 Ensure X Window System is not installed

Info

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

Rationale:

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

Impact:

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the 'headless' Java packages for your specific Java runtime, if provided by your distribution.

Solution

Remove the X Windows System packages:

apt purge xserver-xorg*

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -l | /bin/grep xserver-xorg* | /usr/bin/awk '{print} END {if(NR==0) print "none" }'
expect: ^none$ system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -l | /bin/grep xserver-xorg* | /usr/bin/awk '{print} END {if(NR==0) print
 "none" }'' returned :

none
```

2.2.2 Ensure Avahi Server is not installed

Info

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

Rationale:

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

Solution

Run the following commands to remove avahi-daemon:

systemctl stop avahi-daaemon.service # systemctl stop avahi-daemon.socket # apt purge avahi-daemon

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s avahi-demon | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'avahi-demon' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s avahi-demon | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.3 Ensure CUPS is not installed

Info

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

Rationale:

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

Impact:

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

Solution

Run one of the following commands to remove cups :

apt purge cups

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
LEVEL	2A
NIAV2	SS15a

PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s cups | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'cups' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s cups | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.4 Ensure DHCP Server is not installed - isc-dhcp-server

Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that this package be removed to reduce the potential attack surface.

Solution

Run the following command to remove isc-dhcp-server:

apt purge isc-dhcp-server

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s isc-dhcp-server | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'isc-dhcp-server' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s isc-dhcp-server | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.5 Ensure LDAP server is not installed

Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP server, it is recommended that the software be removed to reduce the potential attack surface.

Solution

Run one of the following commands to remove slapd:

apt purge slapd

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s slapd | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'slapd' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s slapd | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.6 Ensure NFS is not installed

Info

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not export NFS shares or act as an NFS client, it is recommended that these services be removed to reduce the remote attack surface.

Solution

Run the following command to remove nfs:

apt purge nfs-kernel-server

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s nfs-kernel-server | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'nfs-kernel-server' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s nfs-kernel-server | /bin/grep -E '(Status:|not installed)''
 returned :

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

2.2.7 Ensure DNS Server is not installed

Info

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following commands to disable DNS server:

apt purge bind9

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s bind9 | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'bind9' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s bind9 | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'bind9' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.2.8 Ensure FTP Server is not installed

Info

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following command to remove vsftpd:

apt purge vsftpd

Additional Information:

Additional FTP servers also exist and should be audited.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s vsftpd | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'vsftpd' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s vsftpd | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.9 Ensure HTTP server is not installed

Info

HTTP or web servers provide the ability to host web site content.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following command to remove apache:

apt purge apache2

Additional Information:

Several httpd servers exist and can use other service names. apache2 and nginx are example services that provide an HTTP server. These and other services should also be audited

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s apache2 | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'apache2' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s apache2 | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'apache2' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.2.10 Ensure IMAP and POP3 server are not installed - dovecot-imapd

Info

dovecot-imapd and dovecot-pop3d are an open source IMAP and POP3 server for Linux based systems.

Rationale:

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

Solution

Run one of the following commands to remove dovecot-imapd and dovecot-pop3d:

apt purge dovecot-imapd dovecot-pop3d

Additional Information:

Several IMAP/POP3 servers exist and can use other service names. courier-imap and cyrus-imap are example services that provide a mail server. These and other services should also be audited.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s dovecot-imapd | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'dovecot-imapd' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s dovecot-imapd | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.10 Ensure IMAP and POP3 server are not installed - dovecot-pop3d

Info

dovecot-imapd and dovecot-pop3d are an open source IMAP and POP3 server for Linux based systems.

Rationale:

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

Solution

Run one of the following commands to remove dovecot-imapd and dovecot-pop3d:

apt purge dovecot-imapd dovecot-pop3d

Additional Information:

Several IMAP/POP3 servers exist and can use other service names. courier-imap and cyrus-imap are example services that provide a mail server. These and other services should also be audited.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s dovecot-pop3d | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'dovecot-pop3d' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s dovecot-pop3d | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'dovecot-pop3d' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.2.11 Ensure Samba is not installed

Info

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service should be deleted to reduce the potential attack surface.

Solution

Run the following command to remove samba:

apt purge samba

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s samba | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'samba' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s samba | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.12 Ensure HTTP Proxy Server is not installed

Info

Squid is a standard proxy server used in many distributions and environments.

Rationale:

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

Solution

Run the following command to remove squid:

apt purge squid

Additional Information:

Several HTTP proxy servers exist. These and other services should be checked

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s squid | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'squid' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s squid | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.13 Ensure SNMP Server is not installed

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.

Rationale:

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 net-snmp 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 command to remove snmp:

apt purge snmp

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

2.2.14 Ensure NIS Server is not installed

Info

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

Rationale:

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

Solution

Run the following command to remove nis:

apt purge nis

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s nis | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'nis' is not installed and no information is available system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg -s nis | /bin/grep -E '(Status:|not installed)'' returned :

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

2.2.15 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.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

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.

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/ss -lntu | /bin/grep -E ':25s' | /bin/grep -E -v 's(127.0.0.1|::1):25s' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.111.1

```
The command '/bin/ss -lntu | /bin/grep -E ':25s' | /bin/grep -E -v 's(127.0.0.1|::1):25s' | /usr/
bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'' returned :

pass
```

2.3.1 Ensure NIS Client is not installed

Info

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

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

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.

Solution

Uninstall nis:

apt purge nis

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s nis 2>&1 expect: (?:(^[\s]*dpkg-query: package 'nis' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$)) system: Linux

Hosts

192.168.111.1

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

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

2.3.2 Ensure rsh client is not installed

Info

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

Rationale:

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

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.

Solution

Uninstall rsh:

apt purge rsh-client

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s rsh-client 2>&1 expect: (?:(^[\s]*dpkg-query: package 'rsh-client' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$)) system: Linux

Hosts

192.168.111.1

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

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

2.3.3 Ensure talk client is not installed

Info

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

Rationale:

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

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.

Solution

Uninstall talk:

```
# apt purge talk
```

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s talk 2>&1 expect: (?:(^[\s]*dpkg-query: package 'talk' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$)) system: Linux

Hosts

192.168.111.1

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

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

2.3.5 Ensure LDAP client is not installed

Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Impact:

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

Solution

Uninstall ldap-utils:

apt purge ldap-utils

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s ldap-utils 2>&1 expect: (?:(^[\s]*dpkg-query: package 'ldap-utils' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$)) system: Linux

Hosts

192.168.111.1

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

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

2.3.6 Ensure RPC is not installed

Info

Remote Procedure Call (RPC) is a method for creating low level client server applications across different system architectures. It requires an RPC compliant client listening on a network port. The supporting package is rpcbind.'

Rationale:

If RPC is not required, it is recommended that this services be removed to reduce the remote attack surface.

Solution

Run the following command to remove rpcbind:

apt purge rpcbind

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg -s rpcbind 2>&1 expect: (?:(^[\s]*dpkg-query: package 'rpcbind' is not installed.*$)|(^[\s]*Status: deinstall ok config-files.*$)) system: Linux

Hosts

192.168.111.1

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

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

2.8 Enable user namespace support - /etc/subgid

Info

Enable user namespace support in Docker daemon to utilize container user to host user re-mapping. This recommendation is beneficial where containers you are using do not have an explicit container user defined in the container image. If container images that you are using have a pre-defined non-root user, this recommendation may be skipped since this feature is still in its infancy and might give you unpredictable issues and complexities.

Rationale:

The Linux kernel user namespace support in Docker daemon provides additional security for the Docker host system. It allows a container to have a unique range of user and group IDs which are outside the traditional user and group range utilized by the host system.

For example, the root user will have expected administrative privilege inside the container but can effectively be mapped to an unprivileged UID on the host system.

Solution

Please consult Docker documentation for various ways in which this can be configured depending upon your requirements. Your steps might also vary based on platform - For example, on Red Hat, sub-UIDs and sub-GIDs mapping creation does not work automatically. You might have to create your own mapping.

However, the high-level steps are as below:

Step 1: Ensure that the files /etc/subuid and /etc/subgid exist.

touch /etc/subuid /etc/subgid Step 2: Start the docker daemon with --userns-remap flag dockerd --userns-remap=default Impact:

User namespace remapping makes quite a few Docker features incompatible and also currently breaks a few functionalities. Check out the Docker documentation and referenced links for details.

Default Value:

By default, user namespace is not remapped.

See Also

https://workbench.cisecurity.org/files/1726

References

CSCV6	18
LEVEL	2A

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

file: /etc/subgid

Hosts

192.168.111.1

```
The file /etc/subgid with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/subgid
```

2.8 Enable user namespace support - /etc/subuid

Info

Enable user namespace support in Docker daemon to utilize container user to host user re-mapping. This recommendation is beneficial where containers you are using do not have an explicit container user defined in the container image. If container images that you are using have a pre-defined non-root user, this recommendation may be skipped since this feature is still in its infancy and might give you unpredictable issues and complexities.

Rationale:

The Linux kernel user namespace support in Docker daemon provides additional security for the Docker host system. It allows a container to have a unique range of user and group IDs which are outside the traditional user and group range utilized by the host system.

For example, the root user will have expected administrative privilege inside the container but can effectively be mapped to an unprivileged UID on the host system.

Solution

Please consult Docker documentation for various ways in which this can be configured depending upon your requirements. Your steps might also vary based on platform - For example, on Red Hat, sub-UIDs and sub-GIDs mapping creation does not work automatically. You might have to create your own mapping.

However, the high-level steps are as below:

Step 1: Ensure that the files /etc/subuid and /etc/subgid exist.

touch /etc/subuid /etc/subgid Step 2: Start the docker daemon with --userns-remap flag dockerd --userns-remap=default Impact:

User namespace remapping makes quite a few Docker features incompatible and also currently breaks a few functionalities. Check out the Docker documentation and referenced links for details.

Default Value:

By default, user namespace is not remapped.

See Also

https://workbench.cisecurity.org/files/1726

References

CSCV6	18
LEVEL	2A

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

file: /etc/subuid

Hosts

192.168.111.1

```
The file /etc/subuid with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/subuid
```

2.9 Enable user namespace support - /etc/subgid

Info

You should enable user namespace support in Docker daemon to utilize container user to host user re-mapping. This recommendation is beneficial where the containers you are using do not have an explicit container user defined in the container image. If the container images that you are using have a pre-defined non-root user, this recommendation may be skipped as this feature is still in its infancy, and might result in unpredictable issues or difficulty in configuration.

Rationale:

The Linux kernel 'user namespace' support within the Docker daemon provides additional security for the Docker host system. It allows a container to have a unique range of user and group IDs which are outside the traditional user and group range utilized by the host system.

For example, the root user can have the expected administrative privileges inside the container but can effectively be mapped to an unprivileged UID on the host system.

Impact:

User namespace remapping is incompatible with a number of Docker features and also currently breaks some of its functionalities. Reference the Docker documentation and included links for details.

Solution

Please consult the Docker documentation for various ways in which this can be configured depending upon your requirements. Your steps might also vary based on platform - For example, on Red Hat, sub-UIDs and sub-GIDs mapping creation do not work automatically. You might have to create your own mapping.

The high-level steps are as below:

Step 1: Ensure that the files /etc/subuid and /etc/subgid exist.

touch /etc/subuid /etc/subgid

Step 2: Start the docker daemon with --userns-remap flag

dockerd --userns-remap=default

Default Value:

By default, user namespace is not remapped. Consideration should be given to implementing this in line with the requirements of the applications being used and the organization's security policy.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-171	3.13.2
800-53	SA-8

800-53R5	SA-8
CSCV7	18
CSCV8	6
CSF	PR.IP-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SA-8
ITSG-33	SA-8a.
LEVEL	2M
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.6.5
NIAV2	SS3
NIAV2	VL2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/subgid

Hosts

192.168.111.1

```
The file /etc/subgid with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/subgid
```

2.9 Enable user namespace support - /etc/subuid

Info

You should enable user namespace support in Docker daemon to utilize container user to host user re-mapping. This recommendation is beneficial where the containers you are using do not have an explicit container user defined in the container image. If the container images that you are using have a pre-defined non-root user, this recommendation may be skipped as this feature is still in its infancy, and might result in unpredictable issues or difficulty in configuration.

Rationale:

The Linux kernel 'user namespace' support within the Docker daemon provides additional security for the Docker host system. It allows a container to have a unique range of user and group IDs which are outside the traditional user and group range utilized by the host system.

For example, the root user can have the expected administrative privileges inside the container but can effectively be mapped to an unprivileged UID on the host system.

Impact:

User namespace remapping is incompatible with a number of Docker features and also currently breaks some of its functionalities. Reference the Docker documentation and included links for details.

Solution

Please consult the Docker documentation for various ways in which this can be configured depending upon your requirements. Your steps might also vary based on platform - For example, on Red Hat, sub-UIDs and sub-GIDs mapping creation do not work automatically. You might have to create your own mapping.

The high-level steps are as below:

Step 1: Ensure that the files /etc/subuid and /etc/subgid exist.

touch /etc/subuid /etc/subgid

Step 2: Start the docker daemon with --userns-remap flag

dockerd --userns-remap=default

Default Value:

By default, user namespace is not remapped. Consideration should be given to implementing this in line with the requirements of the applications being used and the organization's security policy.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-171	3.13.2
800-53	SA-8

800-53R5	SA-8
CSCV7	18
CSCV8	6
CSF	PR.IP-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SA-8
ITSG-33	SA-8a.
LEVEL	2M
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.6.5
NIAV2	SS3
NIAV2	VL2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/subuid

Hosts

192.168.111.1

```
The file /etc/subuid with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/subuid
```

2.9 Ensure the default cgroup usage has been confirmed

Info

The --cgroup-parent option allows you to set the default cgroup parent to use for all the containers. If there is no specific use case, this setting should be left at its default.

Rationale:

System administrators typically define cgroups under which containers are supposed to run. Even if cgroups are not explicitly defined by the system administrators, containers run under docker cgroup by default.

It is possible to attach to a different cgroup other than that is the default. This usage should be monitored and confirmed. By attaching to a different cgroup than the one that is a default, it is possible to share resources unevenly and thus might starve the host for resources.

Solution

The default setting is good enough and can be left as-is. If you want to specifically set a non-default cgroup, pass --cgroup-parent parameter to the docker daemon when starting it.

For Example, dockerd --cgroup-parent=/foobar Impact:

None.

Default Value:

By default, docker daemon uses /docker for fs cgroup driver and system.slice for systemd cgroup driver.

See Also

https://workbench.cisecurity.org/files/1726

References

800-53	SC-39
800-53R5	SC-39
CSCV6	18
GDPR	32.1.b
HIPAA	164.306(a)(1)
LEVEL	2A
QCSC-V1	5.2.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: ps -ef | grep docker | grep [-][-]cgroup-parent | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'

expect: (--cgroup-parent=/foobar|none)

Hosts

192.168.111.1

```
The command 'ps -ef | grep docker | grep [-][-]cgroup-parent | /usr/bin/awk '{print} END {if (NR ==
 0) print "none"}'' returned :

none
```

2.10 Ensure the default cgroup usage has been confirmed - daemon.json

Info

The --cgroup-parent option allows you to set the default cgroup parent to use for all containers. If there is no specific usage requirement for this, the setting should be left at its default.

Rationale:

System administrators typically define cgroups under which containers are supposed to run. Even if cgroups are not explicitly defined by the system administrators, containers run under docker cgroup by default.

It is possible to attach to a different cgroup other than the one which is the default, however this type of usage should be monitored and confirmed because attaching to a different cgroup other than the one that is a default, it could be possible to share resources unevenly causing resource utilization problems on the host.

Impact:

None.

Solution

The default setting is in line with good security practice and can be left in situ. If you wish to specifically set a non-default cgroup, pass the --cgroup-parent parameter to the Docker daemon when starting it.

For example,

dockerd --cgroup-parent=/foobar

Default Value:

By default, docker daemon uses /docker for fs cgroup driver and system.slice for systemd cgroup driver.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-171	3.13.2
800-53	SA-8
800-53R5	SA-8
CSCV7	18
CSCV8	6
CSF	PR.IP-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SA-8

ITSG-33	SA-8a.
LEVEL	2M
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.6.5
NIAV2	SS3
NIAV2	VL2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

expect: ['"]*cgroup-parent['"]*[\s]*:

file: /etc/docker/daemon.json regex: ['"]*cgroup-parent['"]*[\s]*:

Hosts

192.168.111.1

```
The file "/etc/docker/daemon.json" does not contain "['"]*cgroup-parent['"]*[\s]*:"
```

2.10 Ensure the default cgroup usage has been confirmed - dockerd

Info

The --cgroup-parent option allows you to set the default cgroup parent to use for all containers. If there is no specific usage requirement for this, the setting should be left at its default.

Rationale:

System administrators typically define cgroups under which containers are supposed to run. Even if cgroups are not explicitly defined by the system administrators, containers run under docker cgroup by default.

It is possible to attach to a different cgroup other than the one which is the default, however this type of usage should be monitored and confirmed because attaching to a different cgroup other than the one that is a default, it could be possible to share resources unevenly causing resource utilization problems on the host.

Impact:

None.

Solution

The default setting is in line with good security practice and can be left in situ. If you wish to specifically set a non-default cgroup, pass the --cgroup-parent parameter to the Docker daemon when starting it.

For example,

dockerd --cgroup-parent=/foobar

Default Value:

By default, docker daemon uses /docker for fs cgroup driver and system.slice for systemd cgroup driver.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.13.1
800-171	3.13.2
800-53	SA-8
800-53R5	SA-8
CSCV7	18
CSCV8	6
CSF	PR.IP-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SA-8

ITSG-33	SA-8a.
LEVEL	2M
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.6.5
NIAV2	SS3
NIAV2	VL2

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: ps -ef | grep dockerd | grep -v grep expect: ^((?!--cgroup-parent=*).)*$

Hosts

192.168.111.1

```
The command 'ps -ef | grep dockerd | grep -v grep' returned :

root      506653       1  0 Mar18 ?        00:42:45 /usr/bin/dockerd -H fd:// --containerd=/run/
containerd/containerd.sock
```

2.11 Ensure base device size is not changed until needed - daemon.json

Info

Under certain circumstances, you might need containers larger than 10G. Where this applies you should carefully choose the base device size.

Rationale:

The base device size can be increased on daemon restart. Increasing the base device size allows all future images and containers to be of the new base device size. A user can use this option to expand the base device size, however shrinking is not permitted. This value affects the system wide 'base' empty filesystem that may already be initialized and therefore inherited by pulled images.

Although the file system does not allocate the increased size as long as it is empty, more space will be allocated for extra images. This may cause a denial of service condition if the allocated partition becomes full.

Impact:

None.

Solution

Do not set --storage-opt dm.basesize until needed.

Default Value:

The default base device size is 10G.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	18
CSCV8	16.7
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	2M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

expect: ['"]*dm.basesize['"]* file: /etc/docker/daemon.json regex: ['"]*dm.basesize['"]*

Hosts

192.168.111.1

```
The file "/etc/docker/daemon.json" does not contain "['"]*dm.basesize['"]*"
```

2.11 Ensure base device size is not changed until needed - dockerd

Info

Under certain circumstances, you might need containers larger than 10G. Where this applies you should carefully choose the base device size.

Rationale:

The base device size can be increased on daemon restart. Increasing the base device size allows all future images and containers to be of the new base device size. A user can use this option to expand the base device size, however shrinking is not permitted. This value affects the system wide 'base' empty filesystem that may already be initialized and therefore inherited by pulled images.

Although the file system does not allocate the increased size as long as it is empty, more space will be allocated for extra images. This may cause a denial of service condition if the allocated partition becomes full.

Impact:

None.

Solution

Do not set --storage-opt dm.basesize until needed.

Default Value:

The default base device size is 10G.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	18
CSCV8	16.7
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	2M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: ps -ef | grep dockerd | grep -v grep expect: ^((?!dm.basesize*).)*$

Hosts

192.168.111.1

```
The command 'ps -ef | grep dockerd | grep -v grep' returned :

root      506653       1  0 Mar18 ?        00:42:45 /usr/bin/dockerd -H fd:// --containerd=/run/
containerd/containerd.sock
```

3.1 Ensure that the docker.service file ownership is set to root:root

Info

You should verify that the docker.service file ownership and group ownership are correctly set to root.

Rationale:

The docker.service file contains sensitive parameters that may alter the behavior of the Docker daemon. It should therefore be individually and group owned by the root user in order to ensure that it is not modified or corrupted by a less privileged user.

Impact:

None.

Solution

Step 1: Find out the file location:

systemctl show -p FragmentPath docker.service

Step 2: If the file does not exist, this recommendation is not applicable. If the file does exist, you should execute the command below, including the correct file path, in order to set the ownership and group ownership for the file to root.

For example,

chown root:root /usr/lib/systemd/system/docker.service

Default Value:

This file may not be present on the system and if it is not, this recommendation is not applicable. By default, if the file is present, the correct permissions are for the ownership and group ownership to be set to 'root'.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /usr/lib/systemd/system/docker.service file_required: NO group: root owner: root

Hosts

192.168.111.1

```
The file /usr/lib/systemd/system/docker.service with fmode owner: root group: root mode: 0644 uid: 0
 gid: 0 uneven permissions : FALSE is compliant with the policy value

/usr/lib/systemd/system/docker.service
```

3.1.2 Ensure wireless interfaces are disabled

Info

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

Rationale:

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

Impact:

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

Solution

Run the following script to disable any wireless interfaces:

#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then nmcli radio all off else if [-n '$(find /sys/class/net/*/ -type d -name wireless)']; then mname=$(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 dm in $mname; do echo 'install $dm /bin/true' >> /etc/modprobe.d/disable_wireless.conf done fi fi

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

ITSG-33	CM-7
LEVEL	1A
LEVEL	2A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: if command -v nmcli >/dev/null 2>&1 ; then nmcli radio all | grep -Eq '\s*\S+\s+disabled\s+\S+\s+disabled\b' && echo "Wireless is not enabled" || nmcli radio all; elif [-n "$(find /sys/class/net/*/ -type d -name wireless)"]; then t=0; drivers=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do basename "$(readlink -f "$driverdir"/device/driver)";done | sort -u); for dm in $drivers; do if grep -Eq "^\s*install\s+$dm\s+/bin/(true|false)" /etc/modprobe.d/*.conf; then /bin/true; else echo "$dm is not disabled"; t=1; fi; done; [[$t -eq 0]] && echo "Wireless is not enabled"; else echo "Wireless is not enabled"; fi expect: Wireless is not enabled system: Linux timeout: 7200

Hosts

192.168.111.1

```
The command 'if command -v nmcli >/dev/null 2>&1 ; then nmcli radio all | grep -Eq '\s*\S+\s
+disabled\s+\S+\s+disabled\b' && echo "Wireless is not enabled" || nmcli radio all; elif [ -
n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then t=0; drivers=$(for driverdir in
 $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do basename "$(readlink -f
 "$driverdir"/device/driver)";done | sort -u); for dm in $drivers; do if grep -Eq "^\s*install\s+$dm
\s+/bin/(true|false)" /etc/modprobe.d/*.conf; then /bin/true; else echo "$dm is not disabled"; t=1;
 fi; done; [[ $t -eq 0 ]] && echo "Wireless is not enabled"; else echo "Wireless is not enabled";
 fi' returned :

Wireless is not enabled
```

3.2 Ensure that docker.service file permissions are appropriately set

Info

You should verify that the docker.service file permissions are either set to 644 or to a more restrictive value.

Rationale:

The docker.service file contains sensitive parameters that may alter the behavior of the Docker daemon. It should therefore not be writable by any other user other than root in order to ensure that it can not be modified by less privileged users.

Impact:

None.

Solution

Step 1: Find out the file location:

systemctl show -p FragmentPath docker.service

Step 2: If the file does not exist, this recommendation is not applicable. If the file exists, execute the command below including the correct file path to set the file permissions to 644.

For example,

chmod 644 /usr/lib/systemd/system/docker.service

Default Value:

This file may not be present on the system. In that case, this recommendation is not applicable. By default, if the file is present, the file permissions are correctly set to 644.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /usr/lib/systemd/system/docker.service file_required: NO mask: 133

Hosts

192.168.111.1

```
The file /usr/lib/systemd/system/docker.service with fmode owner: root group: root mode: 0644 uid: 0
 gid: 0 uneven permissions : FALSE is compliant with the policy value

/usr/lib/systemd/system/docker.service
```

3.2.1 Ensure packet redirect sending is disabled - sysctl net.ipv4.conf.all.send_redirects

Info

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

Rationale:

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

Solution

Run the following script to set:

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

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

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.all.send_redirects = 1

net.ipv4.conf.default.send_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.2.2 Ensure IP forwarding is disabled - ipv4 (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

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

Solution

Run the following script to set:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.ip_forward=0 net.ipv6.conf.all.forwarding=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*net\.ipv4\.ip_forward[\s]*=[\s]*1[\s]*$ file: /etc/sysctl.conf /etc/sysctl.d/* regex: ^[\s]*net \.ipv4\.ip_forward[\s]* system: Linux

Hosts

192.168.111.1

```
The file "/etc/sysctl.conf" does not contain "^[\s]*net\.ipv4\.ip_forward[\s]*"
```

3.2.2 Ensure IP forwarding is disabled - ipv6 (sysctl.conf/sysctl.d)

Info

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

Rationale:

Setting:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

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

Solution

Run the following script to set:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.ip_forward=0 net.ipv6.conf.all.forwarding=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*net\.ipv6\.conf\.all\.forwarding[\s]*=[\s]*1[\s]*$ file: /etc/sysctl.conf /etc/sysctl.d/* regex: ^[\s]*net\.ipv6\.conf\.all\.forwarding[\s]* system: Linux

Hosts

192.168.111.1

```
The file "/etc/sysctl.conf" does not contain "^[\s]*net\.ipv6\.conf\.all\.forwarding[\s]*"
```

3.2.2 Ensure IP forwarding is disabled - sysctl ipv6

Info

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

Rationale:

Setting:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

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

Solution

Run the following script to set:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.ip_forward=0 net.ipv6.conf.all.forwarding=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv6.conf.all.forwarding' returned :

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

3.3 Ensure that docker.socket file ownership is set to root:root

Info

You should verify that the docker.socket file ownership and group ownership are correctly set to root.

Rationale:

The docker.socket file contains sensitive parameters that may alter the behavior of the Docker remote API. For this reason, it should be owned and group owned by root in order to ensure that it is not modified by less privileged users.

Impact:

None.

Solution

Step 1: Find out the file location:

systemctl show -p FragmentPath docker.socket

Step 2: If the file does not exist, this recommendation is not applicable. If the file exists, execute the command below, including the correct file path to set the ownership and group ownership for the file to root.

For example,

chown root:root /usr/lib/systemd/system/docker.socket

Default Value:

This file may not be present on the system. In that case, this recommendation is not applicable. By default, if the file is present, the ownership and group ownership for it should be set to root.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /usr/lib/systemd/system/docker.socket file_required: NO group: root owner: root

Hosts

192.168.111.1

```
The file /usr/lib/systemd/system/docker.socket with fmode owner: root group: root mode: 0644 uid: 0
 gid: 0 uneven permissions : FALSE is compliant with the policy value
```

```
/usr/lib/systemd/system/docker.socket
```

3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv4.conf.all.accept_source_route

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

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

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv6.conf.all.accept_source_route

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_source_route' returned :
```

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

3.3.1 Ensure source routed packets are not accepted - sysctl net.ipv6.conf.default.accept_source_route

Info

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

Rationale:

Setting:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 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

Run the following script to set:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0 net.ipv6.conf.default.accept_source_route=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

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

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

Rationale:

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

By setting:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

The system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Solution

Run the following script to set:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } IPV6F_CHK() { l_ipv6s=''

grubfile=$(find /boot -type f (-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg') -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} ;) if [-s '$grubfile']; then ! grep -P -- '^h*(kernelopts=|linux|kernel)' '$grubfile' | grep -vq -- ipv6.disable=1 && l_ipv6s='disabled'

fi if grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$' $l_searchloc && sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.all.disable_ipv6h*=h*1h*(#.*)?$' && sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- '^h*net.ipv6.conf.default.disable_ipv6h*=h*1h*(#.*)?$'; then l_ipv6s='disabled'

fi if [-n '$l_ipv6s']; then echo -e '

- IPv6 is disabled on the system, '$l_kpname' is not applicable'

else KPF fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

if grep -q '^net.ipv6.' <<< '$l_kpe'; then l_kpfile='/etc/sysctl.d/60-netipv6_sysctl.conf'

IPV6F_CHK else l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF fi done }

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

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

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

3.3.5 Ensure broadcast ICMP requests are ignored - sysctl exec

Info

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

Rationale:

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

Solution

Run the following script to set net.ipv4.icmp_echo_ignore_broadcasts = 1:

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.icmp_echo_ignore_broadcasts=1'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.conf.default.log_martians = 0

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts' returned :

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

3.3.6 Ensure bogus ICMP responses are ignored - (sysctl exec)

Info

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

Rationale:

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

Solution

Run the following script to set icmp_ignore_bogus_error_responses = 1:

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='icmp_ignore_bogus_error_responses=1'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'

l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'

KPF done }

Default Value:

net.ipv4.icmp_ignore_bogus_error_responses = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses' returned :

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

3.3.8 Ensure TCP SYN Cookies is enabled - sysctl exec

Info

When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. Setting net.ipv4.tcp_syncookies = 1 enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

Solution

Run the following script to set net.ipv4.tcp_syncookies = 1:

#!/usr/bin/env bash

{ l_output='' l_output2=''

l_parlist='net.ipv4.tcp_syncookies=1'

l_searchloc='/run/sysctl.d/*.conf /etc/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf $([-f /etc/default/ufw] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)'

l_kpfile='/etc/sysctl.d/60-netipv4_sysctl.conf'

KPF() { # comment out incorrect parameter(s) in kernel parameter file(s) l_fafile='$(grep -s -- '^s*$l_kpname' $l_searchloc | grep -Pv -- 'h*=h*$l_kpvaluebh*' | awk -F: '{print $1}')'

for l_bkpf in $l_fafile; do echo -e '

- Commenting out '$l_kpname' in '$l_bkpf''

sed -ri '/$l_kpname/s/^/# /' '$l_bkpf'

done # Set correct parameter in a kernel parameter file if ! grep -Pslq -- '^h*$l_kpnameh*=h* $l_kpvaluebh*(#.*)?$' $l_searchloc; then echo -e '

- Setting '$l_kpname' to '$l_kpvalue' in '$l_kpfile''

echo '$l_kpname = $l_kpvalue' >> '$l_kpfile'

fi # Set correct parameter in active kernel parameters l_krp='$(sysctl '$l_kpname' | awk -F= '{print $2}' | xargs)'

if ['$l_krp' != '$l_kpvalue']; then echo -e '

- Updating '$l_kpname' to '$l_kpvalue' in the active kernel parameters'

sysctl -w '$l_kpname=$l_kpvalue'

sysctl -w '$(awk -F'.' '{print $1'.'$2'.route.flush=1'}' <<< '$l_kpname')'

fi } for l_kpe in $l_parlist; do l_kpname='$(awk -F= '{print $1}' <<< '$l_kpe')'
l_kpvalue='$(awk -F= '{print $2}' <<< '$l_kpe')'
KPF done }

Default Value:

net.ipv4.tcp_syncookies = 1

Additional Information:

NIST SP 800-53 Rev. 5:

CM-1

CM-2

CM-6

CM-7

IA-5

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf

This behavior can be changed by updating the IPT_SYSCTL parameter in /etc/default/ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command '/sbin/sysctl net.ipv4.tcp_syncookies' returned :

net.ipv4.tcp_syncookies = 1
```

3.4 Ensure that docker.socket file permissions are set to 644 or more restrictive

Info

You should verify that the file permissions on the docker.socket file are correctly set to 644 or more restrictively.

Rationale:

The docker.socket file contains sensitive parameters that may alter the behavior of the Docker remote API. It should therefore be writeable only by root in order to ensure that it is not modified by less privileged users.

Impact:

None.

Solution

Step 1: Find out the file location:

systemctl show -p FragmentPath docker.socket

Step 2: If the file does not exist, this recommendation is not applicable. If the file does exist, you should execute the command below, including the correct file path to set the file permissions to 644.

For example,

chmod 644 /usr/lib/systemd/system/docker.socket

Default Value:

This file may not be present on the system and in that case, this recommendation is not applicable. By default, if the file is present, the permissions should be set to 644 or more restrictively.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /usr/lib/systemd/system/docker.socket file_required: NO mask: 133

Hosts

192.168.111.1

```
The file /usr/lib/systemd/system/docker.socket with fmode owner: root group: root mode: 0644 uid: 0
 gid: 0 uneven permissions : FALSE is compliant with the policy value

/usr/lib/systemd/system/docker.socket
```

3.5 Ensure that the /etc/docker directory ownership is set to root:root

Info

You should verify that the /etc/docker directory ownership and group ownership is correctly set to root.

Rationale:

The /etc/docker directory contains certificates and keys in addition to various other sensitive files. It should therefore be individual owned and group owned by root in order to ensure that it can not be modified by less privileged users.

Impact:

None.

Solution

To resolve this issue you should run the following command:

chown root:root /etc/docker

This sets the ownership and group ownership for the directory to root.

Default Value:

By default, the ownership and group ownership for this directory is correctly set to root.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker group: root owner: root

Hosts

192.168.111.1

```
The file /etc/docker with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/docker
```

3.5.1.1 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

Rationale:

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/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.2 Ensure iptables-persistent is not installed with ufw

Info

The iptables-persistent is a boot-time loader for netfilter rules, iptables plugin

Rationale:

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/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.3 Ensure ufw service is enabled - systemctl

Info

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.

Notes:

When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.

Run the following command before running ufw enable.

ufw allow proto tcp from any to any port 22

The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy)

By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable

Rationale:

The ufw service must be enabled and running in order for ufw to protect the system

Impact:

Changing firewall settings while connected over network can result in being locked out of 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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.3 Ensure ufw service is enabled - ufw

Info

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.

Notes:

When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.

Run the following command before running ufw enable.

ufw allow proto tcp from any to any port 22

The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy)

By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable

Rationale:

The ufw service must be enabled and running in order for ufw to protect the system

Impact:

Changing firewall settings while connected over network can result in being locked out of 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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.4 Ensure ufw loopback traffic is configured - v4

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo # ufw allow out on lo # ufw deny in from 127.0.0.0/8 # ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b

GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.4 Ensure ufw loopback traffic is configured - v6

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo # ufw allow out on lo # ufw deny in from 127.0.0.0/8 # ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b

GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.5 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.

Rationale:

If rules are not in place for new outbound connections all packets will be dropped by the default policy preventing network usage.

Solution

Configure ufw in accordance with site policy. The following commands will implement a policy to allow all outbound connections on all interfaces:

ufw allow out on all

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.6 Ensure ufw firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

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

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Solution

For each port identified in the audit which does not have a firewall rule, add rule for accepting or denying inbound connections:

Example:

ufw allow in <port>/<tcp or udp protocol>

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.1.7 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

Rationale:

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

Impact:

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

ufw allow git

ufw allow in http

ufw allow out http <- required for apt to connect to repository

ufw allow in https

ufw allow out https

ufw allow out 53

ufw logging on

Solution

Run the following commands to implement a default deny policy:

ufw default deny incoming # ufw default deny outgoing # ufw default deny routed

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.1 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

Rationale:

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.

Solution

Run the following command to install nftables:

apt install nftables

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.2 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.

Rationale:

Running both the nftables service and ufw may lead to conflict and unexpected results.

Solution

Run one of the following commands to either remove ufw or disable ufw Run the following command to remove ufw:

apt purge ufw

Run the following command to disable ufw:

ufw disable

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b

GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.3 Ensure iptables are flushed with nftables - ip6tables

Info

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

Solution

Run the following commands to flush iptables:

For iptables:

iptables -F

For ip6tables:

ip6tables -F

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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

GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.3 Ensure iptables are flushed with nftables - iptables

Info

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

Solution

Run the following commands to flush iptables:

For iptables:

iptables -F

For ip6tables:

ip6tables -F

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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

GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.4 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.

Rationale:

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

Solution

Run the following command to create a table in nftables

nft create table inet <table name>

Example:

nft create table inet filter

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.5 Ensure nftables base chains exist - forward

Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

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

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 ; }

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.5 Ensure nftables base chains exist - input

Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

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

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 ; }

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.5 Ensure nftables base chains exist - output

Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

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

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 ; }

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.6 Ensure nftables loopback traffic is configured - lo

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

nft add rule inet filter input iif lo accept

nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

IF IPv6 is enabled on the system:

Run the following command to implement the IPv6 loopback rule:

nft add rule inet filter input ip6 saddr ::1 counter drop

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.6 Ensure nftables loopback traffic is configured - v4

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

nft add rule inet filter input iif lo accept

nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

IF IPv6 is enabled on the system:

Run the following command to implement the IPv6 loopback rule:

nft add rule inet filter input ip6 saddr ::1 counter drop

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.6 Ensure nftables loopback traffic is configured - v6

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

nft add rule inet filter input iif lo accept

nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

IF IPv6 is enabled on the system:

Run the following command to implement the IPv6 loopback rule:

nft add rule inet filter input ip6 saddr ::1 counter drop

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.7 Ensure nftables outbound and established connections are configured - input

Info

Configure the firewall rules for new outbound, and established connections

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Solution

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

nft add rule inet filter input ip protocol tcp ct state established accept

nft add rule inet filter input ip protocol udp ct state established accept

nft add rule inet filter input ip protocol icmp ct state established accept

nft add rule inet filter output ip protocol tcp ct state new,related,established accept

nft add rule inet filter output ip protocol udp ct state new,related,established accept

nft add rule inet filter output ip protocol icmp ct state new,related,established accept

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.7 Ensure nftables outbound and established connections are configured - output

Info

Configure the firewall rules for new outbound, and established connections

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Solution

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

nft add rule inet filter input ip protocol tcp ct state established accept

nft add rule inet filter input ip protocol udp ct state established accept

nft add rule inet filter input ip protocol icmp ct state established accept

nft add rule inet filter output ip protocol tcp ct state new,related,established accept

nft add rule inet filter output ip protocol udp ct state new,related,established accept

nft add rule inet filter output ip protocol icmp ct state new,related,established accept

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.8 Ensure nftables default deny firewall policy - forward

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

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

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 ; }

Default Value:

accept

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.8 Ensure nftables default deny firewall policy - input

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

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

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 ; }

Default Value:

accept

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.8 Ensure nftables default deny firewall policy - output

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

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

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 ; }

Default Value:

accept

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.9 Ensure nftables service is enabled

Info

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

Rationale:

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

Solution

Run the following command to enable the nftables service:

systemctl enable nftables

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2

HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.10 Ensure nftables rules are permanent - forward

Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/ datagrams/frames.

The nftables service reads the /etc/nftables.conf file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Solution

Edit the /etc/nftables.conf file and un-comment or add a line with include <Absolute path to nftables rules file> for each nftables file you want included in the nftables ruleset on boot Example:

vi /etc/nftables.conf

Add the line:

include '/etc/nftables.rules'

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.10 Ensure nftables rules are permanent - input

Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/ datagrams/frames.

The nftables service reads the /etc/nftables.conf file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Solution

Edit the /etc/nftables.conf file and un-comment or add a line with include <Absolute path to nftables rules file> for each nftables file you want included in the nftables ruleset on boot Example:

vi /etc/nftables.conf

Add the line:

include '/etc/nftables.rules'

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.2.10 Ensure nftables rules are permanent - output

Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/ datagrams/frames.

The nftables service reads the /etc/nftables.conf file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Solution

Edit the /etc/nftables.conf file and un-comment or add a line with include <Absolute path to nftables rules file> for each nftables file you want included in the nftables ruleset on boot Example:

vi /etc/nftables.conf

Add the line:

include '/etc/nftables.rules'

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.1.1 Ensure iptables packages are installed - iptables

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.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Solution

Run the following command to install iptables and iptables-persistent

apt install iptables iptables-persistent

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d

GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.1.1 Ensure iptables packages are installed - iptables-persistent

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.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Solution

Run the following command to install iptables and iptables-persistent

apt install iptables iptables-persistent

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d

GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.1.2 Ensure nftables is not installed 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.

Rationale:

Running both iptables and nftables may lead to conflict.

Solution

Run the following command to remove nftables:

apt purge nftables

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)

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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.1.3 Ensure ufw is uninstalled or disabled 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

Rationale:

Running iptables.persistent with ufw enabled may lead to conflict and unexpected results.

Solution

Run one of the following commands to either remove ufw or stop and mask ufw Run the following command to remove ufw:

apt purge ufw

OR Run the following commands to disable ufw:

ufw disable # systemctl stop ufw # systemctl mask ufw

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.2.1 Ensure iptables default deny firewall policy - 'Chain FORWARD'

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.2.1 Ensure iptables default deny firewall policy - 'Chain INPUT'

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.2.1 Ensure iptables default deny firewall policy - 'Chain OUTPUT'

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.2.2 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

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

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/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.2.3 Ensure iptables outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established connections.

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

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

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 OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT # iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.2.4 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.

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

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.3.1 Ensure ip6tables default deny firewall policy - 'Chain FORWARD'

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.3.1 Ensure ip6tables default deny firewall policy - 'Chain INPUT'

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.3.1 Ensure ip6tables default deny firewall policy - 'Chain OUTPUT'

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.3.2 Ensure ip6tables 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

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ip6tables -A INPUT -i lo -j ACCEPT # ip6tables -A OUTPUT -o lo -j ACCEPT # ip6tables -A INPUT -s ::1 -j DROP

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.3.3 Ensure ip6tables 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

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.5.3.3.4 Ensure ip6tables firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

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

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

3.6 Ensure that /etc/docker directory permissions are set to 755 or more restrictively

Info

You should verify that the /etc/docker directory permissions are correctly set to 755 or more restrictively.

Rationale:

The /etc/docker directory contains certificates and keys in addition to various sensitive files. It should therefore only be writeable by root to ensure that it can not be modified by a less privileged user.

Impact:

None.

Solution

You should run the following command:

chmod 755 /etc/docker

This sets the permissions for the directory to 755.

Default Value:

By default, the permissions for this directory are set to 755.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker mask: 022

Hosts

192.168.111.1

```
The file /etc/docker with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/docker
```

3.15 Ensure that the Docker socket file ownership is set to root:docker

Info

You should verify that the Docker socket file is owned by root and group owned by docker.

Rationale:

The Docker daemon runs as root. The default Unix socket therefore must be owned by root. If any other user or process owns this socket, it might be possible for that non-privileged user or process to interact with the Docker daemon. Additionally, in this case a non-privileged user or process might be able to interact with containers which is neither a secure nor desired behavior.

Additionally, the Docker installer creates a Unix group called docker. You can add users to this group, and in this case, those users would be able to read and write to the default Docker Unix socket. The membership of the docker group is tightly controlled by the system administrator. However, ff any other group owns this socket, then it might be possible for members of that group to interact with the Docker daemon. Such a group might not be as tightly controlled as the docker group. Again, this is not in line with good security practice.

For these reason, the default Docker Unix socket file should be owned by root and group owned by docker to maintain the integrity of the socket file.

Impact:

None.

Solution

You should execute the following command:

chown root:docker /var/run/docker.sock

This sets the ownership to root and group ownership to docker for the default Docker socket file.

Default Value:

By default, the ownership and group ownership for the Docker socket file is correctly set to root:docker.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /var/run/docker.sock group: docker owner: root

Hosts

192.168.111.1

```
The file /var/run/docker.sock with fmode owner: root group: docker mode: 0660 uid: 0 gid: 999 uneven
 permissions : FALSE is compliant with the policy value

/var/run/docker.sock
```

3.16 Ensure that the Docker socket file permissions are set to 660 or more restrictively

Info

You should verify that the Docker socket file has permissions of 660 or are configured more restrictively.

Rationale:

Only root and the members of the docker group should be allowed to read and write to the default Docker Unix socket. The Docker socket file should therefore have permissions of 660 or more restrictive permissions.

Impact:

None.

Solution

You should execute the command below.

chmod 660 /var/run/docker.sock

This sets the file permissions of the Docker socket file to 660.

Default Value:

By default, the permissions for the Docker socket file is correctly set to 660.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /var/run/docker.sock mask: 117

Hosts

192.168.111.1

```
The file /var/run/docker.sock with fmode owner: root group: docker mode: 0660 uid: 0 gid: 999 uneven
 permissions : FALSE is compliant with the policy value

/var/run/docker.sock
```

3.17 Ensure that the daemon.json file ownership is set to root:root

Info

You should verify that the daemon.json file individual ownership and group ownership is correctly set to root, if it is in use.

Rationale:

The daemon.json file contains sensitive parameters that could alter the behavior of the docker daemon. It should therefore be owned and group owned by root to ensure it can not be modified by less privileged users.

Impact:

None.

Solution

If the daemon.json file is present, you should execute the command below:

chown root:root /etc/docker/daemon.json

This sets the ownership and group ownership for the file to root.

Default Value:

This file may not be present on the system, and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/daemon.json file_required: NO group: root owner: root

Hosts

192.168.111.1

```
The file /etc/docker/daemon.json with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/docker/daemon.json
```

3.18 Ensure that daemon.json file permissions are set to 644 or more restrictive

Info

You should verify that if the daemon.json is present its file permissions are correctly set to 644 or more restrictively.

Rationale:

The daemon.json file contains sensitive parameters that may alter the behavior of the docker daemon. Therefore it should be writeable only by root to ensure it is not modified by less privileged users.

Impact:

None.

Solution

If the file is present, you should execute the command below:

chmod 644 /etc/docker/daemon.json

This sets the file permissions for this file to 644.

Default Value:

This file may not be present on the system, and in that case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/docker/daemon.json file_required: NO mask: 133

Hosts

192.168.111.1

```
The file /etc/docker/daemon.json with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/docker/daemon.json
```

3.19 Ensure that the /etc/default/docker file ownership is set to root:root

Info

You should verify that the /etc/default/docker file ownership and group-ownership is correctly set to root.

Rationale:

The /etc/default/docker file contains sensitive parameters that may alter the behavior of the Docker daemon. It should therefore be individually owned and group owned by root to ensure that it cannot be modified by less privileged users.

Impact:

None.

Solution

You should execute the following command

chown root:root /etc/default/docker

This sets the ownership and group ownership of the file to root.

Default Value:

This file may not be present on the system, and in this case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/default/docker file_required: NO group: root owner: root

Hosts

192.168.111.1

```
The file /etc/default/docker with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/default/docker
```

3.20 Ensure that the /etc/default/docker file permissions are set to 644 or more restrictively

Info

You should verify that the /etc/default/docker file permissions are correctly set to 644 or more restrictively.

Rationale:

The /etc/default/docker file contains sensitive parameters that may alter the behavior of the Docker daemon. It should therefore be writeable only by root in order to ensure that it is not modified by less privileged users.

Impact:

None.

Solution

You should execute the following command:

chmod 644 /etc/default/docker

This sets the file permissions for this file to 644.

Default Value:

This file may not be present on the system and in this case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/default/docker file_required: NO mask: 133

Hosts

192.168.111.1

```
The file /etc/default/docker with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/default/docker
```

3.21 Ensure that the /etc/sysconfig/docker file permissions are set to 644 or more restrictively

Info

You should verify that the /etc/sysconfig/docker file permissions are correctly set to 644 or more restrictively.

Rationale:

The /etc/sysconfig/docker file contains sensitive parameters that may alter the behavior of the Docker daemon. It should therefore be writeable only by root in order to ensure that it is not modified by less privileged users.

Impact:

None.

Solution

You should execute the following command:

chmod 644 /etc/sysconfig/docker

This sets the file permissions for this file to 644.

Default Value:

This file may not be present on the system and in this case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/sysconfig/docker file_required: NO mask: 133

Hosts

192.168.111.1

3.22 Ensure that the /etc/sysconfig/docker file ownership is set to root:root

Info

You should verify that the /etc/sysconfig/docker file individual ownership and group ownership is correctly set to root.

Rationale:

The /etc/sysconfig/docker file contains sensitive parameters that may alter the behavior of the Docker daemon. It should therefore be individually owned and group owned by root to ensure that it is not modified by less privileged users.

Impact:

None.

Solution

You should execute the following command:

chown root:root /etc/sysconfig/docker

This sets the ownership and group ownership for the file to root.

Default Value:

This file may not be present on the system, and in this case, this recommendation is not applicable.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /etc/sysconfig/docker file_required: NO group: root owner: root

Hosts

192.168.111.1

3.23 Ensure that the Containerd socket file ownership is set to root:root

Info

You should verify that the Containerd socket file is owned by root and group owned by root.

Rationale:

Containerd is an underlying component used by Docker to create and manage containers. It provides a socket file similar to the Docker socket, which must be protected from unauthorized access. If any other user or process owns this socket, it might be possible for that non-privileged user or process to interact with the Containerd daemon. Additionally, in this case a non-privileged user or process might be able to interact with containers which is neither a secure nor desired behavior.

Unlike the Docker socket, there is usually no requirement for non-privileged users to connect to the socket, so the ownership should be root:root.

Impact:

None.

Solution

You should execute the following command:

chown root:root /run/containerd/containerd.sock

This sets the ownership to root and group ownership to root for the default Containerd socket file.

Default Value:

By default, the ownership and group ownership for the Containerd socket file is correctly set to root:root.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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

CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /run/containerd/containerd.sock file_required: NO group: root owner: root

Hosts

192.168.111.1

```
The file /run/containerd/containerd.sock with fmode owner: root group: root mode: 0660 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
```

```
/run/containerd/containerd.sock
```

3.24 Ensure that the Containerd socket file permissions are set to 660 or more restrictively

Info

You should verify that the Containerd socket file has permissions of 660 or are configured more restrictively.

Rationale:

Only root and the members of the root group should be allowed to read and write to the default Containerd Unix socket. The Containerd socket file should therefore have permissions of 660 or more restrictive permissions.

Impact:

None.

Solution

You should execute the command below.

chmod 660 /run/containerd/containerd.sock

This sets the file permissions of the Containerd socket file to 660.

Default Value:

By default, the permissions for the Containerd socket file is correctly set to 660.

See Also

https://workbench.cisecurity.org/benchmarks/11818

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
LEVEL	2A
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

file: /run/containerd/containerd.sock file_required: NO mask: 117

Hosts

192.168.111.1

```
The file /run/containerd/containerd.sock with fmode owner: root group: root mode: 0660 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/run/containerd/containerd.sock
```

4.1.4.2 Ensure only authorized users own audit log files

Info

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Solution

Run the following command to configure the audit log files to be owned by the root user:

find $(dirname $(awk -F'=' '/^s*log_files*=s*/ {print $2}' /etc/audit/auditd.conf | xargs)) -type f ! -user root -exec chown root {} +

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/stat -Lc "%n %U" "$(dirname $(awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /etc/audit/auditd.conf | xargs))"/* | /bin/grep -Pv -- '^\H+\h+root\b' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/stat -Lc "%n %U" "$(dirname $(awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /
etc/audit/auditd.conf | xargs))"/* | /bin/grep -Pv -- '^\H+\h+root\b' | /usr/bin/awk '{print} END
 { if(NR==0) print "pass" ; else print "fail"}'' returned :

awk: fatal: cannot open file `/etc/audit/auditd.conf' for reading: No such file or directory
dirname: missing operand
Try 'dirname --help' for more information.
pass
```

4.1.4.3 Ensure only authorized groups are assigned ownership of audit log files

Info

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Solution

Run the following command to configure the audit log files to be owned by adm group:

find $(dirname $(awk -F'=' '/^s*log_files*=s*/ {print $2}' /etc/audit/auditd.conf | xargs)) -type f (! -group adm -a ! -group root) -exec chgrp adm {} +

Run the following command to configure the audit log files to be owned by the adm group:

chgrp adm /var/log/audit/

Run the following command to set the log_group parameter in the audit configuration file to log_group = adm:

sed -ri 's/^s*#?s*log_groups*=s*S+(s*#.*)?.*$/log_group = adm1/' /etc/audit/auditd.conf

Run the following command to restart the audit daemon to reload the configuration file:

systemctl restart auditd

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/stat -c "%n %G" "$(dirname $(awk -F"=" '/^[\s]*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))"/* | /bin/grep -Pv '^\h*\H+\h+(adm|root)\b' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/stat -c "%n %G" "$(dirname $(awk -F"=" '/^[\s]*log_file/ {print $2}' /etc/
audit/auditd.conf | xargs))"/* | /bin/grep -Pv '^\h*\H+\h+(adm|root)\b' | /usr/bin/awk '{print} END
 { if(NR==0) print "pass" ; else print "fail"}'' returned :

awk: fatal: cannot open file `/etc/audit/auditd.conf' for reading: No such file or directory
dirname: missing operand
Try 'dirname --help' for more information.
pass
```

4.1.4.4 Ensure the audit log directory is 0750 or more restrictive

Info

The audit log directory contains audit log files.

Rationale:

Audit information includes all information including: audit records, audit settings and audit reports. This information is needed to successfully audit system activity. This information must be protected from unauthorized modification or deletion. If this information were to be compromised, forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

Solution

Run the following command to configure the audit log directory to have a mode of '0750' or less permissive:

chmod g-w,o-rwx '$(dirname $(awk -F'=' '/^s*log_files*=s*/ {print $2}' /etc/audit/auditd.conf))'

Default Value:

750

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/stat -Lc "%n %a" "$(dirname $(/bin/awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /etc/audit/auditd.conf))" | /bin/grep -Pv -- '^\h*\H+\h+([0-7][0,1,4,5]0)' | /bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

192.168.111.1

```
The command '/bin/stat -Lc "%n %a" "$(dirname $( /bin/awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}' /
etc/audit/auditd.conf))" | /bin/grep -Pv -- '^\h*\H+\h+([0-7][0,1,4,5]0)' | /bin/awk '{print} END
 { if(NR==0) print "pass" ; else print "fail"}'' returned :

awk: fatal: cannot open file `/etc/audit/auditd.conf' for reading: No such file or directory
dirname: missing operand
Try 'dirname --help' for more information.
/bin/stat: cannot statx '': No such file or directory
pass
```

4.1.4.5 Ensure audit configuration files are 640 or more restrictive

Info

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Solution

Run the following command to remove more permissive mode than 0640 from the audit configuration files:

```
# find /etc/audit/ -type f ( -name '*.conf' -o -name '*.rules' ) -exec chmod u-x,g-wx,o-rwx {} +
```

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules' \) -exec /usr/bin/stat -Lc "%n %a" {} + | /bin/grep -Pv -- '^\h*\H+\h*([0,2,4,6][0,4]0)\h*$' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux timeout: 7200

Hosts

192.168.111.1

```
The command '/usr/bin/find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) -exec /
usr/bin/stat -Lc "%n %a" {} + | /bin/grep -Pv -- '^\h*\H+\h*([0,2,4,6][0,4]0)\h*$' | /usr/bin/awk
 '{print} END { if(NR==0) print "pass" ; else print "fail"}'' returned :

/usr/bin/find: ‘/etc/audit/’: No such file or directory
pass
```

4.1.4.6 Ensure audit configuration files are owned by root

Info

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Solution

Run the following command to change ownership to root user:

find /etc/audit/ -type f (-name '*.conf' -o -name '*.rules') ! -user root -exec chown root {} +

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules' \) ! -user root | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux timeout: 7200

Hosts

192.168.111.1

```
The command '/usr/bin/find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -user root
 | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'' returned :

/usr/bin/find: ‘/etc/audit/’: No such file or directory
pass
```

4.1.4.7 Ensure audit configuration files belong to group root

Info

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Solution

Run the following command to change group to root:

find /etc/audit/ -type f (-name '*.conf' -o -name '*.rules') ! -group root -exec chgrp root {} +

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules' \) ! -group root | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux timeout: 7200

Hosts

192.168.111.1

```
The command '/usr/bin/find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -group root
 | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'' returned :

/usr/bin/find: ‘/etc/audit/’: No such file or directory
pass
```

4.1.4.8 Ensure audit tools are 755 or more restrictive

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Solution

Run the following command to remove more permissive mode from the audit tools:

chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/stat -c "%n %a" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules | /bin/grep -Pv -- '^\h*\H+\h+([0-7][0,1,4,5][0,1,4,5])\h*$' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/stat -c "%n %a" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /
sbin/auditd /sbin/augenrules | /bin/grep -Pv -- '^\h*\H+\h+([0-7][0,1,4,5][0,1,4,5])\h*$' | /usr/
bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'' returned :

/usr/bin/stat: cannot statx '/sbin/auditctl': No such file or directory
/usr/bin/stat: cannot statx '/sbin/aureport': No such file or directory
/usr/bin/stat: cannot statx '/sbin/ausearch': No such file or directory
/usr/bin/stat: cannot statx '/sbin/autrace': No such file or directory
/usr/bin/stat: cannot statx '/sbin/auditd': No such file or directory
/usr/bin/stat: cannot statx '/sbin/augenrules': No such file or directory
pass
```

4.1.4.9 Ensure audit tools are owned by root

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Solution

Run the following command to change the owner of the audit tools to the root user:

chown root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/stat -c "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules | grep -Pv -- '^\h*\H+\h+root\h*$' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/stat -c "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /
sbin/auditd /sbin/augenrules | grep -Pv -- '^\h*\H+\h+root\h*$' | /usr/bin/awk '{print} END
 { if(NR==0) print "pass" ; else print "fail"}'' returned :

/usr/bin/stat: cannot statx '/sbin/auditctl': No such file or directory
/usr/bin/stat: cannot statx '/sbin/aureport': No such file or directory
/usr/bin/stat: cannot statx '/sbin/ausearch': No such file or directory
/usr/bin/stat: cannot statx '/sbin/autrace': No such file or directory
/usr/bin/stat: cannot statx '/sbin/auditd': No such file or directory
/usr/bin/stat: cannot statx '/sbin/augenrules': No such file or directory
pass
```

4.1.4.10 Ensure audit tools belong to group root

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Solution

Run the following command to remove more permissive mode from the audit tools:

chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules

Run the following command to change owner and group of the audit tools to root user and group:

chown root:root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/stat -c "%n %a %U %G" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules | /bin/grep -Pv -- '^\h*\H+\h+([0- 7][0,1,4,5][0,1,4,5])\h+root\h+root\h*$' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/stat -c "%n %a %U %G" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/
autrace /sbin/auditd /sbin/augenrules | /bin/grep -Pv -- '^\h*\H+\h+([0- 7][0,1,4,5][0,1,4,5])\h
+root\h+root\h*$' | /usr/bin/awk '{print} END { if(NR==0) print "pass" ; else print "fail"}''
 returned :

/bin/grep: range out of order in character class
/usr/bin/stat: cannot statx '/sbin/auditctl': No such file or directory
/usr/bin/stat: cannot statx '/sbin/aureport': No such file or directory
/usr/bin/stat: cannot statx '/sbin/ausearch': No such file or directory
/usr/bin/stat: cannot statx '/sbin/autrace': No such file or directory
/usr/bin/stat: cannot statx '/sbin/auditd': No such file or directory
/usr/bin/stat: cannot statx '/sbin/augenrules': No such file or directory
pass
```

4.2.1.1.1 Ensure systemd-journal-remote is installed

Info

Journald (via 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 centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Solution

Run the following command to install systemd-journal-remote:

apt install systemd-journal-remote

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}' systemd-journal-remote
expect: ^[\s]*systemd-journal-remote[\s]+install[\s]+ok[\s]+installed[\s]+installed[\s]*$ system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}' systemd-
journal-remote' returned :

systemd-journal-remoteinstall ok installedinstalled
```

4.2.1.1.4 Ensure journald is not configured to receive logs from a remote client

Info

Journald 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.

Rationale:

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.

Solution

Run the following command to disable systemd-journal-remote.socket:

systemctl --now disable systemd-journal-remote.socket

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53	CM-6
800-53	CM-7
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
800-53R5	CM-6
800-53R5	CM-7

CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV7	9.2
CSCV8	4.8
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.IP-1
CSF	PR.PT-1
CSF	PR.PT-3
CSF	RS.AN-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS15a
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	2.2.2
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	2.3

SWIFT-CSCV1 6.4

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/systemctl is-enabled systemd-journal-remote.socket | /usr/bin/awk '{print} END {if(NR==0) print "disabled" }'

expect: (disabled|masked|static) system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/systemctl is-enabled systemd-journal-remote.socket | /usr/bin/awk '{print} END
 {if(NR==0) print "disabled" }'' returned :

disabled
```

4.2.1.2 Ensure journald service is enabled

Info

Ensure that the systemd-journald service is enabled to allow capturing of logging events.

Rationale:

If the systemd-journald service is not enabled to start on boot, the system will not capture logging events.

Solution

By default the systemd-journald service does not have an [Install] section and thus cannot be enabled / disabled. It is meant to be referenced as Requires or Wants by other unit files. As such, if the status of systemd-journald is not static, investigate why.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl is-enabled systemd-journald.service expect: static system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl is-enabled systemd-journald.service' returned :

static
```

4.2.1.5 Ensure journald is not configured to send logs to rsyslog

Info

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

Rationale:

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.

Solution

Edit the /etc/systemd/journald.conf file and files in /etc/systemd/journald.conf.d/ and ensure that ForwardToSyslog=yes is removed.

Restart the service:

systemctl restart systemd-journald

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.5
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-6(3)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*ForwardToSyslog[\s]*=[\s]*['"]?yes['"]?[\s]*$ file: /etc/systemd/journald.conf /etc/systemd/journald.conf.d/* regex: ^[\s]*ForwardToSyslog[\s]*= system: Linux

Hosts

192.168.111.1

```
The file "/etc/systemd/journald.conf" does not contain "^[\s]*ForwardToSyslog[\s]*="
```

4.2.2.1 Ensure rsyslog is installed

Info

The rsyslog software is recommended in environments where journald does not meet operation requirements.

Rationale:

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/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}' rsyslog expect: ^[\s]*rsyslog[\s]+install[\s]+ok[\s]+installed[\s]+installed[\s]*$ system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}' rsyslog'
 returned :

rsysloginstall ok installedinstalled
```

4.2.2.2 Ensure rsyslog service is enabled

Info

Once the rsyslog package is installed, ensure that the service is enabled.

Rationale:

If the rsyslog service is not enabled to start on boot, the system will not capture logging events.

Solution

Run the following command to enable rsyslog:

systemctl --now enable rsyslog

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl is-enabled rsyslog | /usr/bin/awk '{print} END {if(NR==0) print "disabled" }'

expect: enabled system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl is-enabled rsyslog | /usr/bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

enabled
```

4.2.2.4 Ensure rsyslog default file permissions are configured

Info

RSyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

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

Impact:

The systems global umask could override, but only making the file permissions stricter, what is configured in RSyslog with the FileCreateMode directive. RSyslog also has it's own $umask directive that can alter the intended file creation mode. In addition, consideration should be given to how FileCreateMode is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in /etc/rsyslog.conf, /etc/rsyslog.d/*conf files and that FileCreateMode is set before any file is created.

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

Restart the service:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: \$FileCreateMode 0[0246][024]0[\s]*$ file: /etc/rsyslog.conf /etc/rsyslog.d/*.conf min_occurrences: 1 regex: ^[\s]*\$FileCreateMode string_required: NO system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /etc/rsyslog.conf - regex '^[\s]*\$FileCreateMode' found - expect '\$FileCreateMode 0[0246]
[024]0[\s]*$' found in the following lines:
          45: $FileCreateMode 0640
      /etc/rsyslog.d/21-cloudinit.conf - regex not found
      /etc/rsyslog.d/50-default.conf - regex not found
```

4.2.2.7 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.

Rationale:

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.

Solution

Should there be any active log server configuration found in the auditing section, modify those files and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of /etc/rsyslog.conf or /etc/rsyslog.d/*.conf.

Old format

$ModLoad imtcp $InputTCPServerRun

New format

module(load='imtcp') input(type='imtcp' port='514')

Restart the service:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53	CM-6
800-53	CM-7
800-53R5	AU-2
800-53R5	AU-7

800-53R5	AU-12
800-53R5	CM-6
800-53R5	CM-7
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV7	9.2
CSCV8	4.8
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.IP-1
CSF	PR.PT-1
CSF	PR.PT-3
CSF	RS.AN-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS15a
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	2.2.2
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	2.3
SWIFT-CSCV1	6.4

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - Old format ModLoad imtcp
The file "/etc/rsyslog.conf" does not contain "^[\s]*\$ModLoad imtcp"

-------------------------
PASSED - Old format InputTCPServerRun
The file "/etc/rsyslog.conf" does not contain "^[\s]*\$InputTCPServerRun"

-------------------------
PASSED - New format module load imtcp
The file "/etc/rsyslog.conf" does not contain "^\h*module\(load="imtcp"\)"

-------------------------
PASSED - New format input imtcp
The file "/etc/rsyslog.conf" does not contain "^\h*input\(type="imtcp" port="514"\)"
```

5.1 Ensure swarm mode is not Enabled, if not needed

Info

Do not enable swarm mode on a Docker engine instance unless this is needed.

Rationale:

By default, a Docker engine instance will not listen on any network ports, with all communications with the client coming over the Unix socket. When Docker swarm mode is enabled on a Docker engine instance, multiple network ports are opened on the system and made available to other systems on the network for the purposes of cluster management and node communications.

Opening network ports on a system increases its attack surface and this should be avoided unless required.

It should be noted that swarm mode is required for the operation of Docker Enterprise components.

Impact:

Disabling swarm mode will impact the operation of Docker Enterprise components if these are in use.

Solution

If swarm mode has been enabled on a system in error, you should run the command below:

docker swarm leave

Default Value:

By default, Docker swarm mode is not enabled.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b

HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1M
LEVEL	2M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: docker info | egrep 'Swarm: active' | awk '{ print } END { if (NR==0) print "none" }'
expect: ^none$

Hosts

192.168.111.1

```
The command 'docker info | egrep 'Swarm: active' | awk '{ print } END { if (NR==0) print "none" }''
 returned :

WARNING: bridge-nf-call-iptables is disabled
WARNING: bridge-nf-call-ip6tables is disabled
none
```

5.1.1 Ensure cron daemon is enabled and running - enabled

Info

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

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

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

Solution

Run the following command to enable and start cron:

systemctl --now enable cron

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1562, T1562.001

TA0005

M1018

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl is-enabled cron expect: enabled system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl is-enabled cron' returned :

enabled
```

5.1.1 Ensure cron daemon is enabled and running - running

Info

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

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

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

Solution

Run the following command to enable and start cron:

systemctl --now enable cron

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1562, T1562.001

TA0005

M1018

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/systemctl status cron expect: ^[\s]*Active[\s]*:[\s]*active[\s]*\(running\) system: Linux

Hosts

192.168.111.1

```
The command '/bin/systemctl status cron' returned :

# cron.service - Regular background program processing daemon
     Loaded: loaded (/lib/systemd/system/cron.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-12-13 21:13:26 UTC; 4 months 22 days ago
       Docs: man:cron(8)
   Main PID: 556 (cron)
      Tasks: 1 (limit: 76858)
     Memory: 500.0K
        CPU: 53.103s
     CGroup: /system.slice/cron.service
             ##556 /usr/sbin/cron -f -P

May 06 07:15:01 s01-chzrh1-arma CRON[1523218]: pam_unix(cron:session): session closed for user root
May 06 07:17:01 s01-chzrh1-arma CRON[1523230]: pam_unix(cron:session): session opened for user
 root(uid=0) by (uid=0)
May 06 07:17:01 s01-chzrh1-arma CRON[1523231]: (root) CMD (   cd / && run-parts --report /etc/
cron.hourly)
May 06 07:17:01 s01-chzrh1-arma CRON[1523230]: pam_unix(cron:session): session closed for user root
May 06 07:25:01 s01-chzrh1-arma CRON[1523292]: pam_unix(cron:session): session opened for user
 root(uid=0) by (uid=0)
May 06 07:25:01 s01-chzrh1-arma CRON[1523293]: (root) CMD (command -v debian-sa1 > /dev/null &&
 debian-sa1 1 1)
May 06 07:25:01 s01-chzrh1-arma CRON[1523292]: pam_unix(cron:session): session closed for user root
May 06 07:35:01 s01-chzrh1-arma CRON[1523462]: pam_unix(cron:session): session opened for user
 root(uid=0) by (uid=0)
May 06 07:35:01 s01-chzrh1-arma CRON[1523463]: (root) CMD (command -v debian-sa1 > /dev/null &&
 debian-sa1 1 1)
May 06 07:35:01 s01-chzrh1-arma CRON[1523462]: pam_unix(cron:session): session closed for user root
```

5.1.8 Ensure cron is restricted to authorized users - '/etc/cron.deny'

Info

Configure /etc/cron.allow to allow specific users to use this service. If /etc/cron.allow does not exist, then /etc/cron.deny is checked. Any user not specifically defined in this file is allowed to use cron. By removing the file, only users in /etc/cron.allow are allowed to use cron.

Note:

Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

Even though a given user is not listed in cron.allow, cron jobs can still be run as that user

The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

Run the following commands to remove /etc/cron.deny:

rm /etc/cron.deny

Run the following command to create /etc/cron.allow

touch /etc/cron.allow

Run the following commands to set permissions and ownership for /etc/cron.allow:

chmod g-wx,o-rwx /etc/cron.allow

chown root:root /etc/cron.allow

See Also

https://workbench.cisecurity.org/files/4068

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

800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/cron.deny system: Linux

Hosts

192.168.111.1

```
No files found: /etc/cron.deny
```

5.1.9 Ensure at is restricted to authorized users - '/etc/at.deny'

Info

Configure /etc/at.allow to allow specific users to use this service. If /etc/at.allow does not exist, then /etc/at.deny is checked. Any user not specifically defined in this file is allowed to use at. By removing the file, only users in /etc/at.allow are allowed to use at.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, at should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

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

Run the following commands to remove /etc/at.deny:

rm /etc/at.deny

Run the following command to create /etc/at.allow

touch /etc/at.allow

Run the following commands to set permissions and ownership for /etc/at.allow:

chmod g-wx,o-rwx /etc/at.allow

chown root:root /etc/at.allow

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/at.deny system: Linux

Hosts

192.168.111.1

```
No files found: /etc/at.deny
```

5.2.2 Ensure permissions on SSH private host key files are configured

Info

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Solution

Run the following script to set mode, ownership, and group on the private SSH host key files:

#!/usr/bin/env bash

{ l_skgn='ssh_keys' # Group designated to own openSSH keys l_skgid='$(awk -F: '($1 == "'$l_skgn'"){print $3}' /etc/group)'

awk '{print}' <<< '$(find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat -L -c '%n %#a %U %G %g' {} +)' | (while read -r l_file l_mode l_owner l_group l_gid; do [-n '$l_skgid'] && l_cga='$l_skgn' || l_cga='root'

['$l_gid' = '$l_skgid'] && l_pmask='0137' || l_pmask='0177'

l_maxperm='$(printf '%o' $((0777 & ~$l_pmask)))'

if [$(($l_mode & $l_pmask)) -gt 0]; then echo -e ' - File: '$l_file' is mode '$l_mode' changing to mode: '$l_maxperm''

if [-n '$l_skgid']; then chmod u-x,g-wx,o-rwx '$l_file'

else chmod u-x,go-rwx '$l_file'

fi fi if ['$l_owner' != 'root']; then echo -e ' - File: '$l_file' is owned by: '$l_owner' changing owner to 'root''

chown root '$l_file'

fi if ['$l_group' != 'root'] && ['$l_gid' != '$l_skgid']; then echo -e ' - File: '$l_file' is owned by group '$l_group' should belong to group '$l_cga''

chgrp '$l_cga' '$l_file'

fi done) }

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command script with multiple lines returned :

- Audit Result:
  *** PASS ***
- * Correctly set * :

 - File: "/etc/ssh/ssh_host_ed25519_key"
  - Correct: mode (0600), owner (root), and group owner (root) configured
```

5.2.3 Ensure permissions on SSH public host key files are configured

Info

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Solution

Run the following commands to set permissions and ownership on the SSH host public key files

find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod u-x,go-wx {} ;

find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root {} ;

Default Value:

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

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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	5.1
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/ssh/ssh_host_*_key.pub group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/ssh/ssh_host_ecdsa_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_ed25519_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid:
 0 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_rsa_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/etc/ssh/ssh_host_ecdsa_key.pub, /etc/ssh/ssh_host_ed25519_key.pub, /etc/ssh/ssh_host_rsa_key.pub
```

5.2.5 Ensure SSH LogLevel is appropriate

Info

INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Solution

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

LogLevel VERBOSE

OR

LogLevel INFO

Default Value:

LogLevel INFO

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: loglevel INFO
Pass

-------------------------
PASSED - sshd_config
No matching files were found
```

5.2.8 Ensure SSH HostbasedAuthentication is disabled

Info

The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of .rhosts, or /etc/hosts.equiv, along with successful public key client host authentication.

Rationale:

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

Solution

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

HostbasedAuthentication no

Default Value:

HostbasedAuthentication no

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	16.3
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: hostbasedauthentication no
Pass

-------------------------
PASSED - sshd_config
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)HostbasedAuthentication(?-i)[\s]"
```

5.2.9 Ensure SSH PermitEmptyPasswords is disabled

Info

The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

Solution

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

PermitEmptyPasswords no

Default Value:

PermitEmptyPasswords no

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	16.3
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: permitemptypasswords no
Pass

-------------------------
PASSED - sshd_config
Compliant file(s):
      /etc/ssh/sshd_config - regex '^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]' found - expect
 '^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]+yes[\s]*$' not found in the following lines:
          59: PermitEmptyPasswords no
      /etc/ssh/sshd_config.d/90-anapaya.conf - regex '^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]' found
 - expect '^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]+yes[\s]*$' not found in the following lines:
          2: PermitEmptyPasswords no
```

5.2.10 Ensure SSH PermitUserEnvironment is disabled

Info

The PermitUserEnvironment option allows users to present environment options to the SSH daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

Solution

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

PermitUserEnvironment no

Default Value:

PermitUserEnvironment no

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b

NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: permituserenvironment no
Pass

-------------------------
PASSED - sshd_config
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitUserEnvironment(?-i)[\s]"
```

5.2.11 Ensure SSH IgnoreRhosts is enabled

Info

The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication.

Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

Solution

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

IgnoreRhosts yes

Default Value:

IgnoreRhosts yes

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	CM-1
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	9.2
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b

NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: ignorerhosts yes
Pass

-------------------------
PASSED - sshd_config
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)IgnoreRhosts(?-i)[\s]"
```

5.2.13 Ensure only strong Ciphers are used

Info

This variable limits the ciphers that SSH can use during communication.

Note:

Some organizations may have stricter requirements for approved ciphers.

Ensure that ciphers used are in compliance with site policy.

The only 'strong' ciphers currently FIPS 140-2 compliant are:

aes256-ctr

aes192-ctr

aes128-ctr

Supported ciphers in openSSH 8.2:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

aes128-ctr

aes192-ctr

aes256-ctr

aes128-gcm@openssh.com

aes256-gcm@openssh.com

chacha20-poly1305@openssh.com

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

The 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.

Solution

Edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers.

Example:

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

Default Value:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: ports=$(grep -s -P "^(Port|Match)" /etc/ssh/sshd_config /etc/sshd_config.d/*.conf | grep -P -o "(Port|LocalPort)[\s]+[\d]+" | /usr/bin/awk '{print $2}; END {if (NR == 0) print "22"}'); for port in ${ports[@]}; do /usr/sbin/sshd -T -C user=root -C host="$(hostname)" -C addr="$(/usr/bin/grep $(hostname) /etc/hosts | /usr/bin/awk '{print $1}')" -C lport=$port | echo "port $port: $(/usr/bin/grep -i ciphers)"; done | /usr/bin/grep -E "(3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc)" | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.111.1

```
The command 'ports=$(grep -s -P "^(Port|Match)" /etc/ssh/sshd_config /etc/sshd_config.d/*.conf
 | grep -P -o "(Port|LocalPort)[\s]+[\d]+" | /usr/bin/awk '{print $2}; END {if (NR == 0) print
 "22"}'); for port in ${ports[@]}; do /usr/sbin/sshd -T -C user=root -C host="$(hostname)" -C
 addr="$(/usr/bin/grep $(hostname) /etc/hosts | /usr/bin/awk '{print $1}')" -C lport=$port | echo
 "port $port: $(/usr/bin/grep -i ciphers)"; done | /usr/bin/grep -E "(3des-cbc|aes128-cbc|aes192-
cbc|aes256-cbc)" | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}''
 returned :

sh: 1: Bad substitution
pass
```

5.2.14 Ensure only strong MAC algorithms are used

Info

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

Note:

Some organizations may have stricter requirements for approved MACs.

Ensure that MACs used are in compliance with site policy.

The only 'strong' MACs currently FIPS 140-2 approved are:

hmac-sha2-256

hmac-sha2-512

The Supported MACs are:

hmac-md5

hmac-md5-96

hmac-sha1

hmac-sha1-96

hmac-sha2-256

hmac-sha2-512

umac-64@openssh.com

umac-128@openssh.com

hmac-md5-etm@openssh.com

hmac-md5-96-etm@openssh.com

hmac-sha1-etm@openssh.com

hmac-sha1-96-etm@openssh.com

hmac-sha2-256-etm@openssh.com

hmac-sha2-512-etm@openssh.com

umac-64-etm@openssh.com

umac-128-etm@openssh.com

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

Solution

Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs.

Example:

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

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: ports=$(grep -s -P "^(Port|Match)" /etc/ssh/sshd_config /etc/sshd_config.d/*.conf | grep -P -o "(Port|LocalPort)[\s]+[\d]+" | /usr/bin/awk '{print $2}; END {if (NR == 0) print "22"}'); for port in ${ports[@]}; do /usr/sbin/sshd -T -C user=root -C host="$(hostname)" -C addr="$(/usr/bin/grep $(hostname) /etc/hosts | /usr/bin/awk '{print $1}')" -C lport=$port | echo "port $port: $(/usr/bin/grep -i MACs)"; done | /usr/bin/grep -E "(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|hmac-sha1-96|umac-64@openssh.com|umac-128@openssh.com|hmac-md5-etm@openssh.com|hmac-md5-96-etm@openssh.com|hmac-ripemd160-etm@openssh.com|hmac-sha1-etm@openssh.com|hmac-sha1-96-etm@openssh.com|umac-64-etm@openssh.com|umac-128-etm@openssh.com)" | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.111.1

```
The command 'ports=$(grep -s -P "^(Port|Match)" /etc/ssh/sshd_config /etc/sshd_config.d/*.conf
 | grep -P -o "(Port|LocalPort)[\s]+[\d]+" | /usr/bin/awk '{print $2}; END {if (NR == 0) print
 "22"}'); for port in ${ports[@]}; do /usr/sbin/sshd -T -C user=root -C host="$(hostname)" -C
 addr="$(/usr/bin/grep $(hostname) /etc/hosts | /usr/bin/awk '{print $1}')" -C lport=$port | echo
 "port $port: $(/usr/bin/grep -i MACs)"; done | /usr/bin/grep -E "(hmac-md5|hmac-md5-96|hmac-
ripemd160|hmac-sha1|hmac-sha1-96|umac-64@openssh.com|umac-128@openssh.com|hmac-md5-etm@openssh.com|
hmac-md5-96-etm@openssh.com|hmac-ripemd160-etm@openssh.com|hmac-sha1-etm@openssh.com|hmac-sha1-96-
etm@openssh.com|umac-64-etm@openssh.com|umac-128-etm@openssh.com)" | /usr/bin/awk '{print} END {if
 (NR == 0) print "pass"; else print "fail"}'' returned :

sh: 1: Bad substitution
pass
```

5.2.15 Ensure only strong Key Exchange algorithms are used

Info

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Notes:

Kex algorithms have a higher preference the earlier they appear in the list

Some organizations may have stricter requirements for approved Key exchange algorithms

Ensure that Key exchange algorithms used are in compliance with site policy

The only Key Exchange Algorithms currently FIPS 140-2 approved are:

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group16-sha512

diffie-hellman-group18-sha512

diffie-hellman-group14-sha256

The Key Exchange algorithms supported by OpenSSH 8.2 are:

curve25519-sha256

curve25519-sha256@libssh.org

diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group14-sha256

diffie-hellman-group16-sha512

diffie-hellman-group18-sha512

diffie-hellman-group-exchange-sha1

diffie-hellman-group-exchange-sha256

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

sntrup4591761x25519-sha512@tinyssh.org

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Solution

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example:

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

Default Value:

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

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: ports=$(grep -s -P "^(Port|Match)" /etc/ssh/sshd_config /etc/sshd_config.d/*.conf | grep -P -o "(Port|LocalPort)[\s]+[\d]+" | /usr/bin/awk '{print $2}; END {if (NR == 0) print "22"}'); for port in ${ports[@]}; do /usr/sbin/sshd -T -C user=root -C host="$(hostname)" -C addr="$(/usr/bin/grep $(hostname) /etc/hosts | /usr/bin/awk '{print $1}')" -C lport=$port | echo "port $port: $(/usr/bin/grep -i kexalgorithms)"; done | /usr/bin/grep -E "(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)" | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.111.1

```
The command 'ports=$(grep -s -P "^(Port|Match)" /etc/ssh/sshd_config /etc/sshd_config.d/*.conf
 | grep -P -o "(Port|LocalPort)[\s]+[\d]+" | /usr/bin/awk '{print $2}; END {if (NR == 0) print
 "22"}'); for port in ${ports[@]}; do /usr/sbin/sshd -T -C user=root -C host="$(hostname)" -C
 addr="$(/usr/bin/grep $(hostname) /etc/hosts | /usr/bin/awk '{print $1}')" -C lport=$port | echo
 "port $port: $(/usr/bin/grep -i kexalgorithms)"; done | /usr/bin/grep -E "(diffie-hellman-group1-
sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)" | /usr/bin/awk '{print} END
 {if (NR == 0) print "pass"; else print "fail"}'' returned :

sh: 1: Bad substitution
pass
```

5.2.20 Ensure SSH MaxSessions is set to 10 or less

Info

The MaxSessions parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

Solution

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

MaxSessions 10

Default Value:

MaxSessions 10

See Also

https://workbench.cisecurity.org/files/4068

References

800-53	AC-10
800-53R5	AC-10
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

-------------------------
PASSED - sshd output
The command script with multiple lines returned :

port 22: maxsessions 10
Pass

-------------------------
PASSED - sshd_config
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)MaxSessions(?-i)[\s]"
```

5.3 Ensure that, if applicable, SELinux security options are set

Info

SELinux is an effective and easy-to-use Linux application security system. It is available by default on some distributions such as Red Hat and Fedora.

Rationale:

SELinux provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. You can therefore add an extra layer of safety to your containers by enabling SELinux on your Linux host.

Impact:

Any restrictions defined in the SELinux policy will be applied to your containers. It should be noted that if your SELinux policy is misconfigured, this may have an impact on the correct operation of the affected containers.

Solution

If SELinux is applicable for your Linux OS, you should use it.

Set the SELinux State.

Set the SELinux Policy.

Create or import a SELinux policy template for Docker containers.

Start Docker in daemon mode with SELinux enabled. For example:

docker daemon --selinux-enabled

or by adding the following to the daemon.json configuration file:

{ 'selinux-enabled': true }

Start your Docker container using the security options. For example,

docker run --interactive --tty --security-opt label=level:TopSecret centos /bin/bash

Default Value:

By default, no SELinux security options are applied on containers.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-53	SI-16
800-53R5	SI-16
CSCV7	5.2

CSCV8	10.5
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	2M

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: SecurityOpt={{ .HostConfig.SecurityOpt }} MountLabel={{ .MountLabel }} ProcessLabel={{ .ProcessLabel }}'

expect: ^((?!SecurityOpt=<no value>*).)*$

Hosts

192.168.111.1

```
The command 'docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}:
 SecurityOpt={{ .HostConfig.SecurityOpt }} MountLabel={{ .MountLabel }}
 ProcessLabel={{ .ProcessLabel }}'' returned :

dea9d413aa4e6c81cc50bc0a2abf83136224ba98f3c7b340aa3d582d1c726a49: SecurityOpt=[label=disable]
 MountLabel= ProcessLabel=
467c702d266a24f7161dde71be5bd7ac23fcd74f757f308f99da46c9b50f9601: SecurityOpt=[label=disable]
 MountLabel= ProcessLabel=
59307a95ce1ad9c488f6e3251d1ea27dc4899fcaecac3fff7da743889de3d7a4: SecurityOpt=<no value> MountLabel=
 ProcessLabel=
55c0c98a006f9fbc64dd01749f51cfb4bc953ee4292ccd480145ac7fd8def28f: SecurityOpt=[label=disable]
 MountLabel= ProcessLabel=
aecec6366a92cad27e3a0575c38855dbf3d5b6a27c6e816ec4197eca0afa08f6: SecurityOpt=[label=disable]
 MountLabel= ProcessLabel=
9e9bcdda183bdb00d257d0406ae9d6709c281e3b9efff8aa66209643a44311ce: SecurityOpt=<no value> MountLabel=
 ProcessLabel=
1d776cbdd0d463dd04f1a9d93d43ebc7daab59cbaaa9adc1c362b4f4b853c9fe: SecurityOpt=<no value> MountLabel=
 ProcessLabel=
e2cc5042a66ba3dfd375ca872c8c5fcc42a69e6a189937737df0d867bbb3704e: SecurityOpt=<no value> MountLabel=
 ProcessLabel=
26617ac9f29bc37ef6aab11cd2bd6bca652b084eb3c185c6903e974ae561f1eb: SecurityOpt=[label=disable]
 MountLabel= ProcessLabel=
66387d931de837fd56c2f7dbba0a620de1474743eb45239a0e3963e8bb78cfac: SecurityOpt=[label=disable]
 MountLabel= ProcessLabel=
3a339e36fe870fb2de2ca39ca4951443698d7579023a7063769d8af50f60e428: SecurityOpt=<no value> MountLabel=
 ProcessLabel=
```

5.3.1 Ensure sudo is installed

Info

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

Rationale:

sudo supports a 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 is LDAP functionality is required. If so, then install sudo-ldap, else install sudo.

Example:

apt install sudo

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
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: important
Section: admin
Installed-Size: 2508
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Version: 1.9.9-1ubuntu2.4
Replaces: sudo-ldap
```

```
Depends: libaudit1 (>= 1:2.2.1), libc6 (>= 2.34), libpam0g (>= 0.99.7.1), libselinux1 (>= 3.1~),
 zlib1g (>= 1:1.2.0.2), libpam-modules, lsb-base
Conflicts: sudo-ldap
Conffiles:
 /etc/pam.d/sudo b3a1b916bf62a2cc3280f7f9b94844ff
 /etc/pam.d/sudo-i ce9740f66cedf7716e26950abfe556fa
 /etc/sudo.conf efb56b1b282fa4cad1b6c0f05137bb08
 /etc/sudo_logsrvd.conf 09ceda2c98f43e0fbb79bed7c82dba45
 /etc/sudoers 791aa979aa5e859f9ba0112a9512158c
 /etc/sudoers.d/README 44c75ff004a18eeefdde4c998914d6d3
Description: Provide limited super user privileges to specific users
 Sudo is a program designed to allow a sysadmin to give limited root
 privileges to users and log root activity.  The basic philosophy is to give
 as few privileges as possible but still allow people to get their work done.
 .
 This version is built with minimal shared library dependencies, use the
 sudo-ldap package instead if you need LDAP support for sudoers.
Homepage: https://www.sudo.ws/
Original-Maintainer: Sudo Maintainers <sudo@packages.debian.org>

Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

5.3.5 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.

Rationale:

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/files/4068

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/grep -r "^[^#].*!authenticate" /etc/sudoers* | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/grep -r "^[^#].*!authenticate" /etc/sudoers* | /usr/bin/awk '{print} END {if
 (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

5.3.6 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.

Rationale:

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 its 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/files/4068

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: sudo -V | /usr/bin/grep "Authentication timestamp timeout:" | awk '{print $4}'

expect: (([1-9]|1[0-4]).[0-9]+|15.0)$ system: Linux

Hosts

192.168.111.1

```
The command 'sudo -V | /usr/bin/grep "Authentication timestamp timeout:" | awk '{print $4}''
 returned :

15.0
```

5.5.1.3 Ensure password expiration warning days is 7 or more - login.defs

Info

The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Solution

Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs :

PASS_WARN_AGE 7

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

chage --warndays 7 <user>

Default Value:

PASS_WARN_AGE 7

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^[\s]*PASS_WARN_AGE[\s]+([7-9]|[1-9][0-9]+)[\s]*$ file: /etc/login.defs regex: ^[\s]*PASS_WARN_AGE[\s]+ system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /etc/login.defs - regex '^[\s]*PASS_WARN_AGE[\s]+' found - expect
 '^[\s]*PASS_WARN_AGE[\s]+([7-9]|[1-9][0-9]+)[\s]*$' found in the following lines:
          167: PASS_WARN_AGE7
```

5.5.1.3 Ensure password expiration warning days is 7 or more - users

Info

The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Solution

Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs :

PASS_WARN_AGE 7

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

chage --warndays 7 <user>

Default Value:

PASS_WARN_AGE 7

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^([^:]*:){5}([7-9]|[1-9][0-9]+):

file: /etc/shadow regex: ^[^:]+:[^!*] string_required: NO system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){5}([7-9]|[1-9][0-9]+):' found in
 the following lines:
          1: root:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19047:0:99999:7:::
          26: anapaya:$6$Ykmswojd$lodHD1eD5i5i4FfSVEY/s/Yywnlw7cr9WTIOA/lnceFgak7Z6c5xs/i/wQkzkh/
WDy5R4w4ZFghZrAgOmud02.:19047:0:99999:7:::
          27: scion:$6$cHxy3rQ.Bf50$uYOrh7oOEHJfdggS.93HTMqhJGmQI/P9c3ecD9IYjRJpirYJmfLY3V6uXDa/
cwZDEHp6ltyl7z5yWg1hT1qLG0:19361:0:99999:7:::
```

5.5.1.5 Ensure all users last password change date is in the past

Info

All users should have a password change date in the past.

Rationale:

If a users recorded password change date is in the future then they could bypass any set password expiration.

Solution

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: echo 'Username, Current Days, Last Password Change Days'; output=""; failures=0; for i in $(cut -d: -f1 < /etc/shadow); do now=$(($(date +%s) / 86400)); change_date=$(chage --list "$i" | grep 'Last

password change' | cut -d: -f2 | awk '{$1=$1};1'); if [[$change_date != "never"]]; then epoch_change_date=$(($(date -d "${change_date}" +%s) / 86400)); else epoch_change_date='Never'; fi; output="${i}, ${now}, ${epoch_change_date}"; if [[$epoch_change_date -le $now]]; then output="${output} - Pass"; else output="${output} - Fail"; ((failures++)); fi; echo "${output}"; done; echo "Number of failures: ${failures}"

expect: ^Number of failures: 0$ system: Linux

Hosts

192.168.111.1

```
The command 'echo 'Username, Current Days, Last Password Change Days'; output=""; failures=0;
 for i in $(cut -d: -f1 < /etc/shadow); do now=$(($(date +%s) / 86400)); change_date=
$(chage --list "$i" | grep 'Last password change' | cut -d: -f2 | awk '{$1=$1};1'); if
 [[ $change_date != "never" ]]; then epoch_change_date=$(($(date -d "${change_date}" +%s) /
 86400)); else epoch_change_date='Never'; fi; output="${i}, ${now}, ${epoch_change_date}"; if
 [[ $epoch_change_date -le $now ]]; then output="${output} - Pass"; else output="${output} - Fail";
 ((failures++)); fi; echo "${output}"; done; echo "Number of failures: ${failures}"' returned :

Username, Current Days, Last Password Change Days
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
root, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
daemon, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
bin, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
sys, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
sync, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
games, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
man, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
lp, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
mail, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
news, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
uucp, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
```

```
proxy, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
www-data, 19849, Never - Fail
sh: 1: [[: not found
sh: 1: [[: not found
sh: 1: failures++: not found
backup, 19849, Neve [...]
```

5.5.2 Ensure system accounts are secured

Info

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell.

Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the nologin shell. This prevents the account from potentially being used to run any commands.

Solution

Set the shell for any accounts returned by the audit to nologin:

usermod -s $(which nologin) <user>

Lock any non root accounts returned by the audit:

usermod -L <user>

The following command will set all system accounts to a non login shell:

awk -F: '$1!~/(root|sync|shutdown|halt|^+)/ && $3<''$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)'' && $7!~/((/usr)?/sbin/nologin)/ && $7!~/(/bin)?/false/ {print $1}' /etc/passwd | while read -r user; do usermod -s '$(which nologin)' '$user'; done

The following command will automatically lock not root system accounts:

awk -F: '($1!~/(root|^+)/ && $3<''$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)'') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!~/LK?/) {print $1}' | while read -r user; do usermod -L '$user'; done

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /bin/egrep -v "^+" /etc/passwd | /usr/bin/awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $3<1000 && $7!="/usr/sbin/nologin" && $7!="/bin/false")' | /usr/bin/awk '{ print } END { if (NR==0) print "none" }'

expect: none system: Linux

Hosts

192.168.111.1

```
The command '/bin/egrep -v "^+" /etc/passwd | /usr/bin/awk -F: '($1!="root" && $1!="sync" && $1!
="shutdown" && $1!="halt" && $3<1000 && $7!="/usr/sbin/nologin" && $7!="/bin/false")' | /usr/bin/awk
 '{ print } END { if (NR==0) print "none" }'' returned :

none
```

5.5.3 Ensure default group for the root account is GID 0

Info

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Rationale:

Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.

Solution

Run the following command to set the root user default group to GID 0 :

usermod -g 0 root

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: ^root:x:0:0:

file: /etc/passwd regex: ^root:

system: Linux

Hosts

192.168.111.1

```
Compliant file(s):
      /etc/passwd - regex '^root:' found - expect '^root:x:0:0:' found in the following lines:
          1: root:x:0:0::/root:/bin/bash
```

5.23 Ensure that docker exec commands are not used with the privileged option

Info

You should not use docker exec with the --privileged option.

Rationale:

Using the --privileged option in docker exec commands gives extended Linux capabilities to the command. This could potentially be an insecure practice, particularly when you are running containers with reduced capabilities or with enhanced restrictions.

Impact:

If you need enhanced capabilities within a container, then run it with all the permissions it requires. These should be specified individually.

Solution

You should not use the --privileged option in docker exec commands.

Default Value:

By default, the docker exec command runs without the --privileged option.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3

ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: ausearch -k docker | grep exec | grep privileged | awk '{ print } END { if (NR==0) print "none" }'

expect: none

Hosts

192.168.111.1

```
The command 'ausearch -k docker | grep exec | grep privileged | awk '{ print } END { if (NR==0)
 print "none" }'' returned :

sh: 1: ausearch: not found
none
```

5.24 Ensure that docker exec commands are not used with the user=root option

Info

You should not use docker exec with the --user=root option.

Rationale:

Using the --user=root option in a docker exec command, executes it within the container as the root user. This could potentially be insecure, particularly when you are running containers with reduced capabilities or enhanced restrictions.

For example, if your container is running as a tomcat user (or any other non-root user), it would be possible to run a command through docker exec as root with the --user=root option. This could potentially be dangerous.

Impact:

None.

Solution

You should not use the --user=root option in docker exec commands.

Default Value:

By default, the docker exec command runs without the --user option.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

cmd: ausearch -k docker | grep exec | grep user | awk '{ print } END { if (NR==0) print "none" }'
expect: none

Hosts

192.168.111.1

```
The command 'ausearch -k docker | grep exec | grep user | awk '{ print } END { if (NR==0) print
 "none" }'' returned :

sh: 1: ausearch: not found
none
```

6.1.1 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.

Rationale:

It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following command to set permissions on /etc/passwd:

chown root:root /etc/passwd # chmod u-x,go-wx /etc/passwd

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/passwd group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/passwd with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd
```

6.1.2 Ensure permissions on /etc/passwd- are configured

Info

The /etc/passwd- file contains backup user account information.

Rationale:

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following command to set permissions on /etc/passwd- :

chown root:root /etc/passwd-

chmod u-x,go-wx /etc/passwd-

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/passwd- group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/passwd- with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd-
```

6.1.3 Ensure permissions on /etc/group are configured

Info

The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Solution

Run the following command to set permissions on /etc/group :

chown root:root /etc/group

chmod u-x,go-wx /etc/group

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/group group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/group with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven permissions :
 FALSE is compliant with the policy value

/etc/group
```

6.1.4 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.

Rationale:

It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following command to set permissions on /etc/group- :

chown root:root /etc/group-

chmod u-x,go-wx /etc/group-

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/group- group: root mask: 133 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/group- with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/group-
```

6.1.5 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.

Rationale:

If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.

Solution

Run one of the following commands to set ownership of /etc/shadow to root and group to either root or shadow:

chown root:root /etc/shadow # chown root:shadow /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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/shadow group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/shadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow
```

6.1.6 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.

Rationale:

It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run one of the following commands to set ownership of /etc/shadow- to root and group to either root or shadow:

chown root:root /etc/shadow- # chown root:shadow /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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/shadow- group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/shadow- with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow-
```

6.1.7 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.

Rationale:

If attackers can gain read access to the /etc/gshadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/gshadow file (such as group administrators) could also be useful to subvert the group.

Solution

Run one of the following commands to set ownership of /etc/gshadow to root and group to either root or shadow:

chown root:root /etc/gshadow # chown root:shadow /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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/gshadow group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/gshadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow
```

6.1.8 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.

Rationale:

It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run one of the following commands to set ownership of /etc/gshadow- to root and group to either root or shadow:

chown root:root /etc/gshadow- # chown root:shadow /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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: /etc/gshadow- group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.111.1

```
The file /etc/gshadow- with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow-
```

6.2.1 Ensure accounts in /etc/passwd use shadowed passwords

Info

Local accounts can uses shadowed passwords. With shadowed passwords, The passwords are saved in 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.

Rationale:

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:

sed -e 's/^([a-zA-Z0-9_]*):[^:]*:/1:x:/' -i /etc/passwd

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/files/4068

References

800-171	3.5.2
800-171	3.13.16
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
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)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/awk -F: '($2 != "x") { print $1 " is not set to shadowed passwords "}' /etc/passwd | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'

expect: none system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}' /etc/
passwd | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'' returned :

none
```

6.2.2 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.

Rationale:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

Solution

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

passwd -l <username>

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/awk -F : '($2 == "") { print $1 " does not have a password."}' /etc/shadow | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'

expect: none system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/awk -F : '($2 == "") { print $1 " does not have a password."}' /etc/shadow | /
usr/bin/awk '{print} END {if (NR == 0) print "none"}'' returned :

none
```

6.2.3 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 .

Rationale:

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

Solution

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1222, T1222.002

TA0003

M1027

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.1
800-53	AC-2c.
800-53R5	AC-2c.
CN-L3	7.1.3.2(d)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2c.

LEVEL	1A
NESA	T5.2.1
NESA	T5.2.2
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
PCI-DSSV3.2.1	1.1.5
PCI-DSSV3.2.1	7.1.1
PCI-DSSV3.2.1	7.1.3
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: passwd_invalid_gid system: Linux

Hosts

192.168.111.1

```
No issues found.
```

6.2.4 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.

Rationale:

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

Solution

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/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/awk -F: 'FILENAME == "/etc/group" && $1 == "shadow" { gid=$3; if ($4!="") { print "secondary "$4; f=1 } } FILENAME == "/etc/passwd" && $4 == gid { print "primary "$1; f=1 } END { if (!f) print "shadow group empty" }' /etc/group /etc/passwd expect: ^shadow group empty$ system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/awk -F: 'FILENAME == "/etc/group" && $1 == "shadow" { gid=$3; if ($4!="")
 { print "secondary "$4; f=1 } } FILENAME == "/etc/passwd" && $4 == gid { print "primary "$1; f=1 }
 END { if (!f) print "shadow group empty" }' /etc/group /etc/passwd' returned :

shadow group empty
```

6.2.5 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.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Solution

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1078, T1078.001, T1078.003

TA0005

M1027

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: passwd_duplicate_uid system: Linux

Hosts

192.168.111.1

```
No duplicate User IDs detected
```

6.2.6 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.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Solution

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Additional Information:

You can also use the grpck command to check for other inconsistencies in the /etc/group file.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1078, T1078.001, T1078.003

TA0005

M1027

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)

ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: group_duplicate_gid system: Linux

Hosts

192.168.111.1

```
No duplicate Group IDs detected
```

6.2.7 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.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd . For example, if 'test4' has a UID of 1000 and a subsequent 'test4' entry has a UID of 2000, logging in as 'test4' will use UID 1000. Effectively, the UID is shared, which is a security problem.

Solution

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1078, T1078.001, T1078.003

TA0004

M1027

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: passwd_duplicate_username system: Linux

Hosts

192.168.111.1

```
No issues found.
```

6.2.8 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.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group . Effectively, the GID is shared, which is a security problem.

Solution

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1078, T1078.001, T1078.003

TA0004

M1027

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: group_duplicate_name system: Linux

Hosts

192.168.111.1

```
No issues found.
```

6.2.10 Ensure root is the only UID 0 account

Info

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

Solution

Remove any users other than root with UID 0 or assign them a new UID if appropriate.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1548, T1548.000

TA0001

M1026

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.1.5
800-53	AC-6(5)
800-53R5	AC-6(5)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: passwd_zero_uid system: Linux

Hosts

192.168.111.1

```
No issues found.
```

6.2.11 Ensure local interactive user home directories exist

Info

Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in '/' and will not be able to write any files or have local environment variables set.

Solution

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

The following script will create a home directory for users with an interactive shell whose home directory doesn't exist:

#!/usr/bin/env bash

{ valid_shells='^($(sed -rn '/^//{s,/,\\/,g;p}' /etc/shells | paste -s -d '|' -))$'

awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | while read -r user home; do if [! -d '$home']; then echo -e '

- User '$user' home directory '$home' doesn't exist

- creating home directory '$home'

'

mkdir '$home'

chmod g-w,o-wrx '$home'

chown '$user' '$home'

fi done }

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

name: active_accounts_without_home_dir system: Linux

Hosts

192.168.111.1

```
No issues found.
```

6.2.12 Ensure local interactive users own their home directories

Info

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Solution

Change the ownership of any home directories that are not owned by the defined user to the correct user.

The following script will update local interactive user home directories to be own by the user:

#!/usr/bin/env bash

{ output=''

valid_shells='^($(sed -rn '/^//{s,/,\\/,g;p}' /etc/shells | paste -s -d '|' -))$'

awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | while read -r user home; do owner='$(stat -L -c '%U' '$home')'

if ['$owner' != '$user']; then echo -e '

- User '$user' home directory '$home' is owned by user '$owner'

- changing ownership to '$user'

'

chown '$user' '$home'

fi done }

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

mask: 0000 name: accounts_bad_home_permissions system: Linux use_valid_shells: YES

Hosts

192.168.111.1

```
No issues found.
```

6.2.14 Ensure no local interactive user has .netrc files

Info

The .netrc file contains data for logging into a remote host for file transfers via FTP.

While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.

Rationale:

The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.

If a .netrc file is required, and follows local site policy, it should have permissions of 600 or more restrictive.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc file permissions and determine the action to be taken in accordance with local site policy.

The following script will remove .netrc files from interactive users' home directories

#!/usr/bin/env bash

{ perm_mask='0177'

valid_shells='^($(sed -rn '/^//{s,/,\\/,g;p}' /etc/shells | paste -s -d '|' -))$'

awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | while read -r user home; do if [-f '$home/.netrc']; then echo -e '

- User '$user' file: '$home/.netrc' exists

- removing file: '$home/.netrc'

'

rm -f '$home/.netrc'

fi done }

See Also

https://workbench.cisecurity.org/files/4068

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

800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: ~/.netrc system: Linux

Hosts

192.168.111.1

6.2.15 Ensure no local interactive user has .forward files

Info

The .forward file specifies an email address to forward the user's mail to.

Rationale:

Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

The following script will remove .forward files from interactive users' home directories

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

{ output=''
fname='.forward'
valid_shells='^($( sed -rn '/^//{s,/,\\V,g;p}' /etc/shells | paste -s -d '|' - ))$'
awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | (while read -r user home; do if [ -f '$home/$fname' ]; then echo -e '$output
- User '$user' file: '$home/$fname' exists
- removing file: '$home/$fname'
'
rm -r '$home/$fname'
fi done ) }
```

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: ~/.forward system: Linux

Hosts

192.168.111.1

6.2.16 Ensure no local interactive user has .rhosts files

Info

While no .rhosts files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf . Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .rhosts files and determine the action to be taken in accordance with site policy.

The following script will remove .rhosts files from interactive users' home directories

#!/usr/bin/env bash

{ perm_mask='0177'

valid_shells='^($(sed -rn '/^//{s,/,\\/,g;p}' /etc/shells | paste -s -d '|' -))$'

awk -v pat='$valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd | while read -r user home; do if [-f '$home/.rhosts']; then echo -e '

- User '$user' file: '$home/.rhosts' exists

- removing file: '$home/.rhosts'

'

rm -f '$home/.rhosts'

fi done }

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

file: ~/.rhosts system: Linux

Hosts

192.168.111.1

7.5 Ensure Docker's secret management commands are used for managing secrets in a Swarm cluster

Info

Use Docker's in-built secret management command.

Rationale:

Docker has various commands for managing secrets in a Swarm cluster. This is the foundation for future secret support in Docker with potential improvements such as Windows support, different backing stores, etc.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Follow docker secret documentation and use it to manage secrets effectively.

Impact:

None Default Value:

Not Applicable

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSCV6	18
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	2M
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: docker secret ls expect: .*

Hosts

192.168.111.1

```
The command 'docker secret ls' returned :

Error response from daemon: This node is not a swarm manager. Use "docker swarm init" or "docker
 swarm join" to connect this node to swarm and try again.
```

7.8 Ensure node certificates are rotated as appropriate

Info

Rotate swarm node certificates as appropriate.

Rationale:

Docker Swarm uses mutual TLS for clustering operations amongst its nodes. Certificate rotation ensures that in an event such as compromised node or key, it is difficult to impersonate a node. By default, node certificates are rotated every 90 days. You should rotate it more often or as appropriate in your environment.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the below command to set the desired expiry time.

For example, docker swarm update --cert-expiry 48h Impact:

None Default Value:

By default, node certificates are rotated automatically every 90 days.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.13.10
800-53	SC-12
800-53R5	SC-12
CSCV6	14.2
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.10.1.2
ITSG-33	SC-12
ITSG-33	SC-12a.
LEVEL	2M
NESA	T7.4.1
NESA	T7.4.2
NIAV2	CY2
NIAV2	CY8
NIAV2	CY9
QCSC-V1	5.2.2
QCSC-V1	6.2

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: docker info | grep -i 'Expiry Duration'

expect: .*

Hosts

192.168.111.1

```
The command 'docker info | grep -i 'Expiry Duration'' returned :

WARNING: bridge-nf-call-iptables is disabled
WARNING: bridge-nf-call-ip6tables is disabled
```

7.9 Ensure CA certificates are rotated as appropriate

Info

Rotate root CA certificates as appropriate.

Rationale:

Docker Swarm uses mutual TLS for clustering operations amongst its nodes. Certificate rotation ensures that in an event such as compromised node or key, it is difficult to impersonate a node. Node certificates depend upon root CA certificates. For operational security, it is important to rotate these frequently. Currently, root CA certificates are not rotated automatically. You should thus establish a process to rotate it at the desired frequency.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the below command to rotate the certificate.

docker swarm ca --rotate Impact:

None Default Value:

By default, root CA certificates are not rotated.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.5.2
800-53	IA-5(2)
800-53R5	IA-5(2)
CSCV6	14.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(2)
LEVEL	2M
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: ls -l /etc/docker/certs.d/CA_CERT expect: .*

Hosts

192.168.111.1

```
The command 'ls -l /etc/docker/certs.d/CA_CERT' returned :

ls: cannot access '/etc/docker/certs.d/CA_CERT': No such file or directory
```

7.10 Ensure management plane traffic has been separated from data plane traffic

Info

Separate management plane traffic from data plane traffic.

Rationale:

Separating the management plane traffic from data plane traffic ensures that these traffics are on their respective paths. These paths could then be individually monitored and could be tied to different traffic control policies and monitoring. It also ensures that management plane is always reachable despite the huge volume of data flow.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Initialize Swarm with dedicated interfaces for management and data planes respectively.

For example, docker swarm init --advertise-addr=192.168.0.1 --data-path-addr=17.1.0.3 Impact:

You would require 2 network interface cards per node.

Default Value:

By default, the data plane traffic is not separated from management plane traffic.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.13.2
800-171	3.13.5
800-53	SC-7(13)
800-53R5	SC-7(13)
CN-L3	8.1.10.6(h)
CSCV6	18
CSF	PR.AC-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(13)
LEVEL	2M
NESA	T4.5.4
NIAV2	GS7d
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	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	3.1
TBA-FIISB	43.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: docker node inspect --format '{{ .Status.Addr }}' self expect: .*

Hosts

192.168.111.1

```
The command 'docker node inspect  --format '{{ .Status.Addr }}' self' returned :

Status: Error response from daemon: This node is not a swarm manager. Use "docker swarm init" or
 "docker swarm join" to connect this node to swarm and try again., Code: 1
```

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.4.1
800-53	CM-8a.1.
800-53R5	CM-8a.1.
CN-L3	8.1.10.2(a)
CN-L3	8.1.10.2(b)
CSF	DE.CM-7
CSF	ID.AM-1
CSF	ID.AM-2
CSF	PR.DS-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.8.1.1
ITSG-33	CM-8a.
NESA	T1.2.1
NESA	T1.2.2
NIAV2	NS35
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

PASSED

Hosts

192.168.111.1

CIS_Docker_v1.6.0_L2_Docker_Linux.audit from CIS Docker Benchmark v1.6.0

See Also

https://workbench.cisecurity.org/benchmarks/11818

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

PASSED

Hosts

192.168.111.1

CIS_Ubuntu_22.04_LTS_Server_v1.0.0_L1.audit from CIS Ubuntu Linux 22.04 LTS Benchmark

See Also

https://workbench.cisecurity.org/files/4068

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

PASSED

Hosts

192.168.111.1

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

1.2.1 Ensure package manager repositories are configured

Info

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

Rationale:

If a system's package repositories are misconfigured important patches may not be identified or a rogue repository could introduce compromised software.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure your package manager repositories according to site policy.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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
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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/apt-cache policy expect: system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/apt-cache policy' returned :
```

```
Package files:
 100 /var/lib/dpkg/status
     release a=now
Pinned packages:
```

1.2.1 Ensure the container host has been Hardened

Info

A container host is able to run one or more containers. It is of utmost importance to harden the host to mitigate host security misconfiguration.

Rationale:

You should follow infrastructure security best practices and harden your host OS. Keeping the host system hardened will ensure that host vulnerabilities are mitigated. Not hardening the host system could lead to security exposures and breaches.

Impact:

None.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

You may consider various CIS Security Benchmarks for your container host. If you have other security guidelines or regulatory requirements to adhere to, please follow them as suitable in your environment.

Default Value:

By default, the host has factory setting and is not hardened.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	5
CSCV8	16.7
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7

LEVEL	1M
LEVEL	2M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

WARNING

Hosts

192.168.111.1

1.2.2 Ensure GPG keys are configured

Info

Most packages managers implement GPG key signing to verify package integrity during installation.

Rationale:

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Update your package manager GPG keys in accordance with site policy.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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
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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

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

Hosts

192.168.111.1

```
The command 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>
```

2.4 Ensure nonessential services are removed or masked

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.

Rationale:

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 command to remove the package containing the service:

apt purge <package_name>

OR If required packages have a dependency:

Run the following command to stop and mask the service:

systemctl --now mask <service_name>

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: /usr/bin/lsof -i -P -n | /bin/grep -v "(ESTABLISHED)"

expect: Manual Review Required system: Linux

Hosts

192.168.111.1

```
The command '/usr/bin/lsof -i -P -n | /bin/grep -v "(ESTABLISHED)"' returned :

COMMAND       PID            USER   FD   TYPE   DEVICE SIZE/OFF NODE NAME
systemd-r  503671 systemd-resolve   13u  IPv4 44979759      0t0  UDP 127.0.0.53:53
systemd-r  503671 systemd-resolve   14u  IPv4 44979760      0t0  TCP 127.0.0.53:53 (LISTEN)
caddy      505313           caddy    3u  IPv4 51174461      0t0  TCP 127.0.0.1:443 (LISTEN)
caddy      505313           caddy    8u  IPv4 44974009      0t0  UDP 127.0.0.1:443
caddy      505313           caddy   10u  IPv4 44974011      0t0  UDP 192.168.111.1:443
caddy      505313           caddy   12u  IPv4 44974013      0t0  UDP 198.18.30.2:443
caddy      505313           caddy   19u  IPv4 51172709      0t0  TCP 127.0.0.1:48050 (LISTEN)
caddy      505313           caddy   20u  IPv4 51174462      0t0  TCP 192.168.111.1:443 (LISTEN)
caddy      505313           caddy   22u  IPv4 51174463      0t0  TCP 198.18.30.2:443 (LISTEN)
caddy      505313           caddy   23u  IPv6 51174464      0t0  TCP *:80 (LISTEN)
caddy      505313           caddy   30u  IPv6 51174465      0t0  TCP *:42001 (LISTEN)
caddy      505313           caddy   31u  IPv4 51174466      0t0  TCP 192.168.111.1:80 (LISTEN)
caddy      505313           caddy   32u  IPv4 51174467      0t0  TCP 198.18.30.2:80 (LISTEN)
sshd       506056            root    3u  IPv4 44986736      0t0  TCP *:22 (LISTEN)
sshd       506056            root    4u  IPv6 44986738      0t0  TCP *:22 (LISTEN)
appliance  528952            root    7u  IPv4 45003128      0t0  TCP 127.0.0.1:48001 (LISTEN)
appliance  528952            root    9u  IPv4 45006335      0t0  TCP 127.0.0.1:48000 (LISTEN)
scion-all  553473            root   11u  IPv4 45022009      0t0  TCP 127.0.0.1:41200 (LISTEN)
scion-all  553473            root   12u  IPv4 45024767      0t0  TCP 127.0.0.1:41201 (LISTEN)
appliance  553563           scion    7u  IPv4 45019786      0t0  TCP 127.0.0.1:48030 (LISTEN)
appliance  553563           scion    9u  IPv4 45025702      0t0  TCP 127.0.0.1:48031 (LISTE [...]
```

2.10 Ensure base device size is not changed until needed

Info

In certain circumstances, you might need containers bigger than 10G in size. In these cases, carefully choose the base device size.

Rationale:

The base device size can be increased at daemon restart. Increasing the base device size allows all future images and containers to be of the new base device size. A user can use this option to expand the base device size however shrinking is not permitted. This value affects the system-wide base empty filesystem that may already be initialized and inherited by pulled images.

Though the file system does not allot the increased size if it is empty, it will use more space for the empty case depending upon the device size. This may cause a denial of service by ending up in file system being over-allocated or full.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Do not set --storage-opt dm.basesize until needed.

Impact:

None.

Default Value:

The default base device size is 10G.

See Also

https://workbench.cisecurity.org/files/1726

References

CSCV6	18
LEVEL	2A

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

WARNING

Hosts

192.168.111.1

2.16 Ensure daemon-wide custom seccomp profile is applied, if needed

Info

You can choose to apply your custom seccomp profile at the daemon-wide level if needed and override Docker's default seccomp profile.

Rationale:

A large number of system calls are exposed to every userland process with many of them going unused for the entire lifetime of the process. Most of the applications do not need all the system calls and thus benefit by having a reduced set of available system calls. The reduced set of system calls reduces the total kernel surface exposed to the application and thus improvises application security.

You could apply your own custom seccomp profile instead of Docker's default seccomp profile. Alternatively, if Docker's default profile is good for your environment, you can choose to ignore this recommendation.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

By default, Docker's default seccomp profile is applied. If this is good for your environment, no action is necessary. Alternatively, if you choose to apply your own seccomp profile, use the --seccomp-profile flag at daemon start or put it in the daemon runtime parameters file.

dockerd --seccomp-profile </path/to/seccomp/profile>

Impact:

A misconfigured seccomp profile could possibly interrupt your container environment. Docker-default blocked calls have been carefully scrutinized. These address some critical vulnerabilities/issues within container environments (for example, kernel key ring calls). So, you should be very careful while overriding the defaults.

Default Value:

By default, Docker applies a seccomp profile.

See Also

https://workbench.cisecurity.org/files/1726

References

800-53	SC-39
800-53R5	SC-39
CSCV6	18
GDPR	32.1.b
HIPAA	164.306(a)(1)
LEVEL	2M
QCSC-V1	5.2.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: docker info --format '{{ .SecurityOptions }}'
expect:

Hosts

192.168.111.1

```
The command 'docker info --format '{{ .SecurityOptions }}'' returned :

[name=apparmor name=seccomp,profile=builtin name=cgroupns]
```

3.1.1 Ensure system is checked to determine if IPv6 is enabled

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 trillion3 addresses.

Features of IPv6

Hierarchical addressing and routing infrastructure

Stateful and Stateless configuration

Support for quality of service (QoS)

An ideal protocol for neighboring node interaction

Rationale:

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.

Impact:

IETF RFC 4038 recommends that applications are built with an assumption of dual stack. Disabling IPv6 on the system may cause some applications to fail or have unexpected behavior.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations. If IPv6 is to be disabled, use one of the two following methods to disable IPv6 on the system:

To disable IPv6 through the GRUB2 config, run the following command to add ipv6.disable=1 to the GRUB_CMDLINE_LINUX parameters:

Edit /etc/default/grub and add ipv6.disable=1 to the GRUB_CMDLINE_LINUX parameters:

Example:

GRUB_CMDLINE_LINUX='ipv6.disable=1'

Run the following command to update the grub2 configuration:

update-grub

OR To disable IPv6 through sysctl settings, set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

Example:

printf '

net.ipv6.conf.all.disable_ipv6 = 1 net.ipv6.conf.default.disable_ipv6 = 1 ' >> /etc/sysctl.d/60-disable_ipv6.conf

Run the following command to set the active kernel parameters:

{ sysctl -w net.ipv6.conf.all.disable_ipv6=1 sysctl -w net.ipv6.conf.default.disable_ipv6=1 sysctl -w net.ipv6.route.flush=1 }

Default Value:

IPv6 is enabled

Additional Information:

Having more addresses has grown in importance with the expansion of smart devices and connectivity. IPv6 provides more than enough globally unique IP addresses for every networked device currently on the planet, helping ensure providers can keep pace with the expected proliferation of IP-based devices.

NIST SP 800-53 Rev. 5:

CM-7

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Manual Review Required$ system: Linux timeout: 7200

Hosts

192.168.111.1

```
The command script with multiple lines returned :

IPv6 is enabled on the system
```

4.2.1.6 Ensure journald log rotation is configured per site policy

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/journald.conf is the configuration file used to specify how logs generated by Journald should be rotated.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Review /etc/systemd/journald.conf and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.

The specific parameters for log rotation are:

SystemMaxUse= SystemKeepFree= RuntimeMaxUse= RuntimeKeepFree= MaxFileSec=

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

expect: Manual Review Required file: /etc/systemd/journald.conf /etc/systemd/journald.conf.d/* min_occurrences: 1 regex: ^[\s]*(SystemMaxUse|SystemKeepFree|RuntimeMaxUse|RuntimeKeepFree|MaxFileSec)[\s]*= required: NO system: Linux

Hosts

192.168.111.1

```
No matching files were found
Less than 1 matches of regex found
```

4.2.1.7 Ensure journald default file permissions 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.

Rationale:

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

NOTE: Nessus has not performed this check. Please review 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. Requirements is either 0640 or site policy if that is less restrictive.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

WARNING

Hosts

192.168.111.1

4.8 Ensure setuid and setgid permissions are removed

Info

Removing setuid and setgid permissions in the images can prevent privilege escalation attacks within containers.

Rationale:

setuid and setgid permissions can be used for privilege escalation. Whilst these permissions can on occasion be legitimately needed, you should consider removing them from packages which do not need them. This should be reviewed for each image.

Impact:

The above command would break all executables that depend on setuid or setgid permissions including legitimate ones. You should therefore be careful to modify the command to suit your requirements so that it does not reduce the permissions of legitimate programs excessively. Because of this, you should exercise a degree of caution and examine all processes carefully before making this type of modification in order to avoid outages.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

You should allow setuid and setgid permissions only on executables which require them. You could remove these permissions at build time by adding the following command in your Dockerfile, preferably towards the end of the Dockerfile:

RUN find / -perm /6000 -type f -exec chmod a-s {} ; || true

Default Value:

Not Applicable

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.1.5
800-171	3.1.6
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
CSCV8	5.4
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	2M
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_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

WARNING

Hosts

192.168.111.1

4.8 Ensure setuid and setgid permissions are removed in the images

Info

Removing setuid and setgid permissions in the images would prevent privilege escalation attacks in the containers.

Rationale:

setuid and setgid permissions could be used for elevating privileges. While these permissions are at times legitimately needed, these could potentially be used in privilege escalation attacks. Thus, you should consider dropping these permissions for the packages which do not need them within the images.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Allow setuid and setgid permissions only on executables which need them. You could remove these permissions during build time by adding the following command in your Dockerfile, preferably towards the end of the Dockerfile:

RUN find / -perm +6000 -type f -exec chmod a-s {} ; || true Impact:

Above command breaks all the executables that depend on setuid or setgid permissions including the legitimate ones. Hence, be careful to modify the command to suit your requirements so that it does not drop the permissions of legitimate programs. This requires a careful examination of each executable and fine tuning the permissions.

Default Value:

Not Applicable

See Also

https://workbench.cisecurity.org/files/1726

References

CSCV6	5.1
LEVEL	2M

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

WARNING

Hosts

192.168.111.1

4.11 Ensure only verified packages are installed

Info

You should verify the authenticity of packages before installing them into images.

Rationale:

Verifying authenticity of software packages is essential for building a secure container image. Packages with no known provenance could potentially be malicious or have vulnerabilities that could be exploited.

Impact:

None

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

You should use a secure package distribution mechanism of your choice to ensure the authenticity of software packages.

Default Value:

Not Applicable

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-53	SA-22
800-53R5	SA-22
CSCV7	18.3
CSCV8	2.2
GDPR	32.1.b
HIPAA	164.306(a)(1)
LEVEL	2M

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

WARNING

Hosts

192.168.111.1

4.11 Ensure verified packages are only Installed

Info

Verify authenticity of the packages before installing them in the image.

Rationale:

Verifying authenticity of the packages is essential for building a secure container image. Tampered packages could potentially be malicious or have some known vulnerabilities that could be exploited.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Use GPG keys for downloading and verifying packages or any other secure package distribution mechanism of your choice.

Impact:

None Default Value:

Not Applicable

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.4.6
800-171	3.4.7
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)
CSCV6	18.1
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
LEVEL	2M
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_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: for image in $(docker images|awk {'print $3'}); do docker history $image;done expect:

Hosts

192.168.111.1

```
The command 'for image in $(docker images|awk {'print $3'}); do docker history $image;done'
 returned :

Error response from daemon: invalid reference format: repository name (library/IMAGE) must be
 lowercase
IMAGE          CREATED       CREATED BY        SIZE      COMMENT
2713bb13f7dd   N/A           bazel build ...   0B
<missing>      N/A           bazel build ...   5.83MB
<missing>      N/A           bazel build ...   376MB
<missing>      8 weeks ago   bazel build ...   17.9MB
<missing>      8 weeks ago   bazel build ...   2.36MB
IMAGE          CREATED       CREATED BY        SIZE      COMMENT
dfa060592f3f   N/A           bazel build ...   0B
<missing>      N/A           bazel build ...   43MB
<missing>      8 weeks ago   bazel build ...   1.17MB
<missing>      8 weeks ago   bazel build ...   0B
<missing>      8 weeks ago   bazel build ...   17.9MB
<missing>      8 weeks ago   bazel build ...   2.36MB
IMAGE          CREATED       CREATED BY        SIZE      COMMENT
ec842bc66d0f   N/A           bazel build ...   0B
<missing>      N/A           bazel build ...   11.4MB
<missing>      8 weeks ago   bazel build ...   1.17MB
<missing>      8 weeks ago   bazel build ...   0B
<missing>      8 weeks ago   bazel build ...   17.9MB
<missing>      8 weeks ago   bazel build ...   2.36MB
IMAGE          CREATED        CREATED BY                                      SIZE      COMMENT
bb0d0d8b3897   5 months ago   EXPOSE map[4317/tcp:{} 55678/tcp:{} 55679/tc…   0B
 buildkit.dockerfile.v0
<missing>      5 months ago   CMD ["--config" "/etc/otelcol-contrib/config…   0B
 buildkit.dockerfile.v0
<missing>      5 months ago   ENTRYPOINT ["/otelcol-contrib"]                 0B
 buildkit.dockerfile.v0
<missing>      5 months ago   COPY configs/otelcol-contrib.yaml /etc/otelc…   0B
 buildkit.dockerfile.v0
<missing>      5 months ago   COPY otelcol-contrib /otelcol-contrib # buil…   1.38kB
 buildkit.dockerfile.v0
 [...]
```

5.2 Ensure SELinux security options are set, if applicable

Info

SELinux is an effective and easy-to-use Linux application security system. It is available on quite a few Linux distributions by default such as Red Hat and Fedora.

Rationale:

SELinux provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. You can thus add an extra layer of safety by enabling SELinux on your Linux host, if applicable.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

If SELinux is applicable for your Linux OS, use it. You may have to follow below set of steps:

1. Set the SELinux State.

2. Set the SELinux Policy.

3. Create or import a SELinux policy template for Docker containers.

4. Start Docker in daemon mode with SELinux enabled. For example, docker daemon --selinux-enabled 5. Start your Docker container using the security options. For example, docker run --interactive --tty --security-opt label=level:TopSecret centos /bin/bash Impact:

The container (process) would have set of restrictions as defined in SELinux policy. If your SELinux policy is mis-configured, then the container may not entirely work as expected.

Default Value:

By default, no SELinux security options are applied on containers.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.1.1
800-171	3.1.2
800-53	AC-3(3)
800-53R5	AC-3(3)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	14.4
CSF	PR.AC-4

CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(3)
LEVEL	2A
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
PCI-DSSV3.2.1	7.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: /usr/bin/docker ps -q | xargs /usr/bin/docker inspect --format '{{ .Id }}: SecurityOpt={{json .HostConfig.SecurityOpt }}'

expect:

Hosts

192.168.111.1

```
The command '/usr/bin/docker ps -q | xargs /usr/bin/docker inspect --format '{{ .Id }}:
 SecurityOpt={{json .HostConfig.SecurityOpt }}'' returned :

dea9d413aa4e6c81cc50bc0a2abf83136224ba98f3c7b340aa3d582d1c726a49: SecurityOpt=["label=disable"]
467c702d266a24f7161dde71be5bd7ac23fcd74f757f308f99da46c9b50f9601: SecurityOpt=["label=disable"]
59307a95ce1ad9c488f6e3251d1ea27dc4899fcaecac3fff7da743889de3d7a4: SecurityOpt=null
55c0c98a006f9fbc64dd01749f51cfb4bc953ee4292ccd480145ac7fd8def28f: SecurityOpt=["label=disable"]
aecec6366a92cad27e3a0575c38855dbf3d5b6a27c6e816ec4197eca0afa08f6: SecurityOpt=["label=disable"]
9e9bcdda183bdb00d257d0406ae9d6709c281e3b9efff8aa66209643a44311ce: SecurityOpt=null
1d776cbdd0d463dd04f1a9d93d43ebc7daab59cbaaa9adc1c362b4f4b853c9fe: SecurityOpt=null
e2cc5042a66ba3dfd375ca872c8c5fcc42a69e6a189937737df0d867bbb3704e: SecurityOpt=null
26617ac9f29bc37ef6aab11cd2bd6bca652b084eb3c185c6903e974ae561f1eb: SecurityOpt=["label=disable"]
66387d931de837fd56c2f7dbba0a620de1474743eb45239a0e3963e8bb78cfac: SecurityOpt=["label=disable"]
3a339e36fe870fb2de2ca39ca4951443698d7579023a7063769d8af50f60e428: SecurityOpt=null
```

5.4.5 Ensure all current passwords uses the configured hashing algorithm

Info

Currently used passwords with out of date hashing algorithms may pose a security risk to the system.

Rationale:

In use passwords should always match the configured hashing algorithm for the system.

Impact:

If the administrator forces a password change, this could cause a large spike in CPU usage if a large number of users change their password during the same time.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

If the administrator wish to force an immediate change on all users as per the output of the audit, execute:

#!/usr/bin/env bash

{ UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs) awk -F: -v UID_MIN='${UID_MIN}' '($3 >= UID_MIN && $1 != 'nfsnobody') { print $1 }' /etc/passwd | xargs -n 1 chage -d 0 }

NOTE: This could cause significant temporary CPU load on the system if a large number of users reset their passwords at the same time.

See Also

https://workbench.cisecurity.org/files/4068

References

800-171	3.5.2
800-171	3.13.16
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
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)
ITSG-33	IA-5(1)
ITSG-33	SC-28
ITSG-33	SC-28a.
ITSG-33	SC-28(1)
LEVEL	1M
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ManualReviewRequired system: Linux

Hosts

192.168.111.1

```
The command script with multiple lines did not return any result
```

5.22 Ensure docker exec commands are not used with privileged option

Info

Do not docker exec with --privileged option.

Rationale:

Using --privileged option in docker exec gives extended Linux capabilities to the command. This could potentially be insecure and unsafe to do especially when you are running containers with dropped capabilities or with enhanced restrictions.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Do not use --privileged option in docker exec command.

Impact:

None. If you need enhanced capabilities within the container, then run the container with the needed capabilities.

Default Value:

By default, docker exec command runs without --privileged option.

See Also

https://workbench.cisecurity.org/files/1726

References

CSCV6	5.1
LEVEL	2A

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

WARNING

Hosts

192.168.111.1

5.23 Ensure docker exec commands are not used with user option

Info

Do not docker exec with --user option.

Rationale:

Using --user option in docker exec executes the command within the container as that user. This could potentially be insecure and unsafe to do especially when you are running containers with dropped capabilities or with enhanced restrictions.

For example, suppose your container is running as tomcat user (or any other non-root user), it would be possible to run a command through docker exec as rootwith --user=root option. This could potentially be dangerous.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Do not use --user option in docker exec command.

Impact:

None.

Default Value:

By default, docker exec command runs without --user option.

See Also

https://workbench.cisecurity.org/files/1726

References

CSCV6	5
LEVEL	2A

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

WARNING

Hosts

192.168.111.1

5.29 Ensure Docker's default bridge docker0 is not used

Info

Do not use Docker's default bridge docker0. Use docker's user-defined networks for container networking.

Rationale:

Docker connects virtual interfaces created in the bridge mode to a common bridge called docker0. This default networking model is vulnerable to ARP spoofing and MAC flooding attacks since there is no filtering applied.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Follow Docker documentation and setup a user-defined network. Run all the containers in the defined network.

Impact:

You have to manage the user-defined networks.

Default Value:

By default, docker runs containers on its docker0 bridge.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.4.6
800-171	3.4.7
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)
CSCV6	9
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
LEVEL	2M
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_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

cmd: for net_id in $(docker network ls|awk {'print $1'}); do docker network inspect $net_id;done expect:

Hosts

192.168.111.1

```
The command 'for net_id in $(docker network ls|awk {'print $1'}); do docker network inspect
 $net_id;done' returned :

Error response from daemon: network NETWORK not found
[]
[
    {
        "Name": "bridge",
        "Id": "0bc78531b21e90eb1dc3fa5369422f4bd46726e203861d2f0fd8cdca0b9f0182",
        "Created": "2024-03-18T12:52:40.461588514Z",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": [
                {
                    "Subnet": "172.17.0.0/16",
                    "Gateway": "172.17.0.1"
                }
            ]
        },
        "Internal": false,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {},
        "Options": {
            "com.docker.network.bridge.default_bridge": "true",
            "com.docker.network.bridge.enable_icc": "true",
            "com.docker.network.bridge.enable_ip_masquerade": "false",
            "com.docker.network.bridge.host_binding_ipv4": "0.0.0.0",
            "com.docker.network.bridge.name": "docker0",
            "com.docker.network.driver.mtu": "1500"
        },
        "Labels": {}
    }
]
[
    {
        "Name": "host",
```

```
        "Id": "3c779ec41f0d47aaa5e30a62e81e14efd26b964126f2a9149de78748b158169a",
        "Created": "2022-02-24T23:16:30.981796884Z",
        "Scope": "local",
        "Driver": "host",
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": null
        },
        "Internal": false,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {
            "1d776cbdd0d463dd04f1a9d93d43ebc7daab59cbaaa9adc1c362b4f4b853c9fe": {
                "Name": "telemetry",
                "EndpointID": "cfc4d71d2fe896ed354a [...]
```

5.30 Ensure that Docker's default bridge 'docker0' is not used

Info

You should not use Docker's default bridge docker0. Instead you should use Docker's user-defined networks for container networking.

Rationale:

Docker connects virtual interfaces created in bridge mode to a common bridge called docker0. This default networking model is vulnerable to ARP spoofing and MAC flooding attacks as there is no filtering applied to it.

Impact:

User-defined networks need to be configured and managed in line with organizational security policy.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

You should follow the Docker documentation and set up a user-defined network. All the containers should be run in this network.

Default Value:

By default, Docker runs containers within the default docker0 bridge.

See Also

https://workbench.cisecurity.org/benchmarks/11818

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	2M

NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

WARNING

Hosts

192.168.111.1

6.1.12 Audit SUID executables

Info

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

find_option: suid name: find_suid_sgid_files system: Linux timeout: 7200

Hosts

192.168.111.1

```
The following 26 files are SUID:

  /usr/lib/dbus-1.0/dbus-daemon-launch-helper
     owner: root, group: messagebus, permissions: 4754

  /usr/lib/openssh/ssh-keysign
     owner: root, group: root, permissions: 4755

  /usr/bin/umount
     owner: root, group: root, permissions: 4755

  /usr/bin/chsh
     owner: root, group: root, permissions: 4755

  /usr/bin/mount
     owner: root, group: root, permissions: 4755

  /usr/bin/gpasswd
     owner: root, group: root, permissions: 4755

  /usr/bin/newgrp
     owner: root, group: root, permissions: 4755

  /usr/bin/chfn
     owner: root, group: root, permissions: 4755

  /usr/bin/su
     owner: root, group: root, permissions: 4755

  /usr/bin/passwd
     owner: root, group: root, permissions: 4755

  /usr/bin/sudo
     owner: root, group: root, permissions: 4755

  /usr/libexec/polkit-agent-helper-1
     owner: root, group: root, permissions: 4755
```

```
  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
bin/umount
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
bin/mount
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
bin/su
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/chsh
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/gpasswd
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/newgrp
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/chfn
     owner: root, group: root, permissions: 4755

  /var/lib/docker/overlay2/3c [...]
```

6.1.13 Audit SGID executables

Info

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Ensure that no rogue SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

See Also

https://workbench.cisecurity.org/files/4068

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

find_option: sgid name: find_suid_sgid_files system: Linux timeout: 7200

Hosts

192.168.111.1

```
The following 14 files are SGID:

  /usr/lib/x86_64-linux-gnu/utempter/utempter
     owner: root, group: utmp, permissions: 2755

  /usr/bin/wall
     owner: root, group: tty, permissions: 2755

  /usr/bin/chage
     owner: root, group: shadow, permissions: 2755

  /usr/bin/expiry
     owner: root, group: shadow, permissions: 2755

  /usr/bin/write.ul
     owner: root, group: tty, permissions: 2755

  /usr/bin/ssh-agent
     owner: root, group: _ssh, permissions: 2755

  /usr/bin/crontab
     owner: root, group: crontab, permissions: 2755

  /usr/sbin/pam_extrausers_chkpwd
     owner: root, group: shadow, permissions: 2755

  /usr/sbin/unix_chkpwd
     owner: root, group: shadow, permissions: 2755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/wall
     owner: root, group: tty, permissions: 2755
```

```
  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/chage
     owner: root, group: shadow, permissions: 2755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
usr/bin/expiry
     owner: root, group: shadow, permissions: 2755

  /var/lib/docker/overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/
sbin/unix_chkpwd
     owner: root, group: shadow, permissions: 2755

  /var/lib/docker/overlay2/6c1ab951b684fdcdac5ab437e00d2722b802d752147c5f4b7de36931e6e56f56/diff/
sbin/unix_chkpwd
     owner: root, group: shadow, permissions: 2755
```

CIS Docker Community Edition v1.1.0 L2 Docker

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://workbench.cisecurity.org/files/1726

References

800-171	3.4.1
800-53	CM-8a.1.
800-53R5	CM-8a.1.
CN-L3	8.1.10.2(a)
CN-L3	8.1.10.2(b)
CSF	DE.CM-7
CSF	ID.AM-1
CSF	ID.AM-2
CSF	PR.DS-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.8.1.1
ITSG-33	CM-8a.
NESA	T1.2.1
NESA	T1.2.2
NIAV2	NS35
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1

Audit File

CIS_Docker_Community_Edition_L2_Docker_v1.1.0.audit

Policy Value

WARNING

Hosts

appliance-cron.docker.container

control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

CIS_Docker_v1.6.0_L2_Docker_Linux.audit from CIS Docker Benchmark v1.6.0

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://workbench.cisecurity.org/benchmarks/11818

Audit File

CIS_Docker_v1.6.0_L2_Docker_Linux.audit

Policy Value

WARNING

Hosts

appliance-cron.docker.container
control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

CIS_Ubuntu_22.04_LTS_Server_v1.0.0_L1.audit from CIS Ubuntu Linux 22.04 LTS Benchmark

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://workbench.cisecurity.org/files/4068

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L1.audit

Policy Value

WARNING

Hosts

appliance-cron.docker.container
control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

CIS_Ubuntu_22.04_LTS_Workstation_v1.0.0_L1.audit from CIS Ubuntu Linux 22.04 LTS Benchmark

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://workbench.cisecurity.org/files/4068

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Workstation_L1.audit

Policy Value

WARNING

Hosts

192.168.111.1
appliance-cron.docker.container
control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

CIS_Ubuntu_22.04_LTS_v.1.0.0_Server_L2.audit from CIS Ubuntu Linux 22.04 LTS Benchmark

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://workbench.cisecurity.org/files/4068

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Server_L2.audit

Policy Value

WARNING

Hosts

192.168.111.1
appliance-cron.docker.container
control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

CIS_Ubuntu_22.04_LTS_v.1.0.0_Workstation_L2.audit from CIS Ubuntu Linux 22.04 LTS Benchmark

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://workbench.cisecurity.org/files/4068

Audit File

CIS_Ubuntu_22.04_LTS_v1.0.0_Workstation_L2.audit

Policy Value

WARNING

Hosts

192.168.111.1
appliance-cron.docker.container
control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

DISA_STIG_Docker_Enterprise_2.x_Linux_Unix_v2r1.audit from DISA Docker Enterprise 2.x Linux/UNIX v2r1 STIG

Info

NOTE: Nessus has not identified that the chosen audit applies to the target device.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_Docker_Enterprise_2-x_Linux-UNIX_V2R1_STIG.zip

Audit File

DISA_STIG_Docker_Enterprise_2.x_Linux_Unix_v2r1.audit

Policy Value

WARNING

Hosts

192.168.111.1
appliance-cron.docker.container
control-64-2_0_2b.docker.container
daemon-64-2_0_2b.docker.container
dataplane-control.docker.container
dataplane.docker.container
dispatcher.docker.container
gateway.docker.container
node-exporter.docker.container
promtail.docker.container
router.docker.container
telemetry.docker.container

Remediations

Suggested Remediations