

Threat hunting report

ID	Nam e	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali	192.168.84.135	Wazuh v4.12.0	siem-VMware- Virtual-Platform	Kali GNU/Linux 2025.3	Sep 9, 2025 @ 15:07:31.000	Oct 6, 2025 @ 19:03:25.000

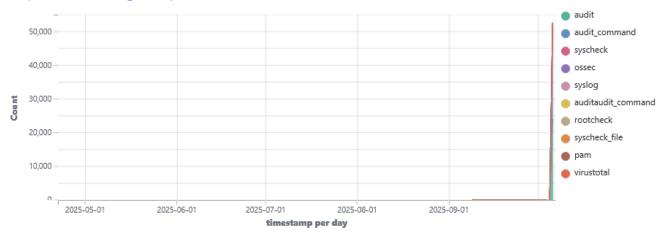
Group: default

Browse through your security alerts, identifying issues and threats in your environment.

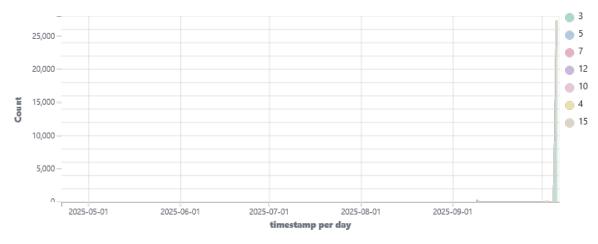
② 2025-04-21T19:03:29 to 2025-10-06T19:03:29

Q manager.name: siem-VMware-Virtual-Platform AND agent.id: 001

Top 10 Alert groups evolution

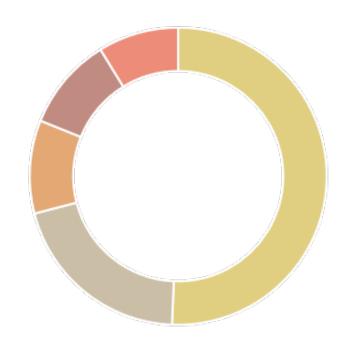


Alerts



wazuh.

Top 5 alerts



Audit: Command: /usr/k

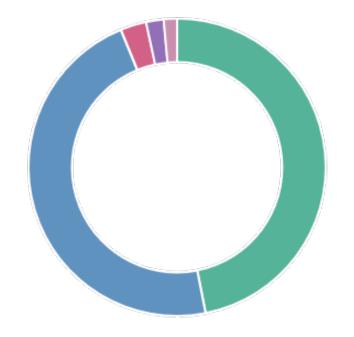
Audit: Command: /usr/k

Audit: Command: /usr/k

Audit: Command: /usr/k

Audit: Command: /usr/t

Top 5 rule groups



audit

audit_command

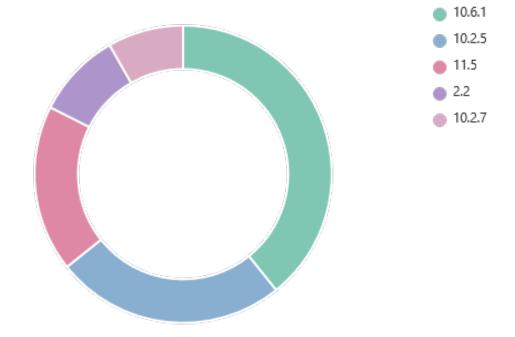
syscheck

ossec

syslog

wazuh.

Top 5 PCI DSS Requirements



28,030

558

11 - Authentication failure -

185
- Authentication success -



Alerts summary

80792 Audit: Command: /usr/bin/ipc. 3 11015 80797 Audit: Command: /usr/bin/ipc. 3 4408 80797 Audit: Command: /usr/bin/ipc. 3 2204 80792 Audit: Command: /usr/bin/dash. 3 1904 100200 File modified in /home directory. 5 921 100200 File modified in /home directory. 5 921 80792 Audit: Command: /usr/bin/dash. 7 503 80792 Audit: Command: /usr/bin/dash. 12 476 80793 Audit: Command: /usr/bin/dash. 12 476 80793 Audit: Command: /usr/bin/sed. 3 842 80793 Audit: Command: /usr/bin/sed. 3 943 80793 Audit: Command: /usr/bin/sed. 3 249 80793 Audit: Command: /usr/bin/sed. 3 185 80793 Audit: Command: /usr/bin/spl. 3 185 80793 Audit: Command: /usr/bin/spl. 3 185 80793 Audit: Command: /usr/bin/spl. 3 186 80793 Audit: Command: /usr/bin/spl. 3 186 80793 Audit: Command: /usr/bin/spl. 3 176 80793 A	Rule ID	Description	Level	Count
80792 Audit: Command: Ausribin/Next. 3 2204 80792 Audit: Command: Ausribin/Mash. 3 1904 80792 Audit: Command: Ausribin/Mash. 3 1904 100300 Flee modified in Anome directory. 5 931 510 Host-based anomaly detection event (rootcheck). 7 503 80792 Audit: Command: Ausribin/Se6_64. 3 426 100210 Audit: Elighty Suspicious Command executed: Ausribin/dash 12 426 80792 Audit: Command: Ausribin/red. 3 88 80793 Audit: Command: Ausribin/red. 3 249 80792 Audit: Command: Ausribin/red. 3 185 80793 Audit: Command: Ausribin/red. 3 185 80794 Audit: Command: Ausribin/red. 3 182 80795 Audit: Command: Ausribin/red. 3 148 80792 Audit: Command: Ausribin/red. 3 148 80793 Audit: Command: Ausribin/red. 3 125 80794 Audit:	80792	Audit: Command: /usr/bin/gnome.	3	11015
80792 Audit: Command: /usr/bin/head. 3 2204 80792 Audit: Command: /usr/bin/dash. 3 1904 100300 File modified in /home directory. 5 931 510 Host-based anomaly detection event (rootcheck). 7 503 80792 Audit: Command: /usr/bin/s6_64. 3 4/6 100210 Audit: Highly Suspicious Command executed. /usr/bin/dash 12 426 80792 Audit: Command: /usr/bin/sed. 3 384 87103 Virusfoati. Alert - No records in Virusfotal database 3 281 80792 Audit: Command: /usr/bin/rm. 3 289 80793 Audit: Command: /usr/bin/rm. 3 289 5501 PAM: Login session obsed. 3 182 80792 Audit: Command: /usr/bin/dplkg. 3 182 5501 PAM: Login session obsed. 3 183 80792 Audit: Command: /usr/bin/dplkg. 3 184 5501 Past (Login Sector obsector obsec	80792	Audit: Command: /usr/bin/ip.	3	4408
80792 Audit: Command: /usr/bin/dash. 3 1904 100300 File modified in /home directory. 5 931 510 Host-based anomaly detection event (rootcheck). 7 503 80792 Audit: Command: /usr/bin/x86_64. 3 426 80792 Audit: Command: /usr/bin/sed. 3 384 80792 Audit: Command: /usr/bin/sed. 3 384 87103 VrusTotal: Alert: No records in VirusTotal database 3 281 80792 Audit: Command: /usr/bin/rm. 3 289 80792 Audit: Command: /usr/bin/dryfulp 3 185 80792 Audit: Command: /usr/bin/dpkg. 3 189 80792 Audit: Command: /usr/bin/dpkg. 3 148 80792 Audit: Command: /usr/bin/cat. 7 143 80792 Audit: Command: /usr/bin/cat. 3 126 80792 Audit: Command: /usr/bin/cat. 3 126 80792 Audit: Command: /usr/bin/cat. 3 107 80792 Audit: Comman	80792	Audit: Command: /usr/bin/cut.	3	2204
100300 File modified in /home directory. 5 931 510 Host-based anomaly detection event (rootcheck). 7 503 80792 Audit: Command: Just/bin/886, 6-4. 3 426 100710 Audit: Highly Suspicious Command executed: /usr/bin/dash 12 476 80792 Audit: Command: Just/bin/sed. 3 384 87103 Virus/Total: Alert: No records in Virus/Total database 3 281 80792 Audit: Command: /usr/bin/rm. 3 249 5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 185 80792 Audit: Command: /usr/bin/dpkg. 3 189 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 5501 Integrity checksum changed. 7 116 5502 Integrity checksum changed. 7 116 5503 File added to the system. 5 116 80792 Audit: Command: /usr/bin/perl. 3 <t< td=""><td>80792</td><td>Audit: Command: /usr/bin/head.</td><td>3</td><td>2204</td></t<>	80792	Audit: Command: /usr/bin/head.	3	2204
510 Host-based anomaly detection event (rootcheck). 7 503 80792 Audit: Command: /usr/bin/x86_64. 3 426 100210 Audit: Highly Suspicious Command executed: /usr/bin/dash 12 426 80792 Audit: Command: /usr/bin/rsed. 3 281 80792 Audit: Command: /usr/bin/rm. 3 229 5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 182 80792 Audit: Command: /usr/bin/dpkg. 3 189 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 80792 Audit: Command: /usr/bin/ret. 5 116 80792 Audit: Command: /usr/bin/pen. 5 84 2904 Dekg (Debian Package) half configured.	80792	Audit: Command: /usr/bin/dash.	3	1904
80792 Audit: Command: /usr/bin/x86, 64. 3 426 100210 Audit: Lighly Suspicious Command executed: /usr/bin/dash 12 426 80792 Audit: Command: /usr/bin/sed. 3 384 87103 VirusTotal: Alert - No records in VirusTotal database 3 281 80792 Audit: Command: /usr/bin/rm. 3 249 5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 182 80792 Audit: Command: /usr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 554 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 80792 Audit: Command: /usr/bin/cat. 3 107 40704 Systemd: Service exited due to a failure. 5 84 80792 Audit: Command: /usr/bin/	100300	File modified in /home directory.	5	931
100210 Audit: Highly Suspicious Command: Ausr/bin/sed. 3 384 80792 Audit: Command: Ausr/bin/sed. 3 384 87103 VirusTotal: Alert - No records in VirusTotal database 3 281 80792 Audit: Command: Ausr/bin/rm. 3 249 80792 Audit: Command: Ausr/bin/rm. 3 185 5501 PAM: Login session obsed. 3 182 80792 Audit: Command: Ausr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: Ausr/bin/cac/gcc/x86_64. 3 107 40704 Systemd: Service exted due to a failure. 5 84 80792 Audit: Command: Ausr/bin/pacly half configured. 7 81 80792 New dokg (Deb	510	Host-based anomaly detection event (rootcheck).	7	503
80792 Audit: Command: /usr/bin/sed. 3 384 87103 VirusTotal: Alert - No records in VirusTotal database 3 281 80792 Audit: Command: /usr/bin/m. 3 249 5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 148 5503 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 80792 Audit: Command: /usr/bin/cat. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dybg (Debian Package) haif configured. 7 8	80792	Audit: Command: /usr/bin/x86_64.	3	426
87103 VirusTotal: Alert - No records in VirusTotal database 3 281 80792 Audit: Command: /usr/bin/rm. 3 249 5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 182 80792 Audit: Command: /usr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 5503 File deleted. 7 143 100301 File added to rhome directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 551 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dykg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/rperl. 3 78 80792 Audit: Command: /usr/bin/rperl.	100210	Audit: Highly Suspicious Command executed: /usr/bin/dash	12	426
80792 Audit: Command: /usr/bin/rm. 3 249 5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 182 80792 Audit: Command: /usr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/fbin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/fbin/exet. 5 84 2904 Dykg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 80792 Audit: Command: /usr/bin/perl. 3 65 80792 Audit: Lighly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/make. 3	80792	Audit: Command: /usr/bin/sed.	3	384
5501 PAM: Login session opened. 3 185 5502 PAM: Login session closed. 3 182 80792 Audit: Command: /usr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /nome directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a fallure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2901 New dpkg (Debian Package) installed. 7 73 80792 Audit: Command: /usr/bin/pasename. 3 52 80793 Audit: Command: /usr/bin/make. 3	87103	VirusTotal: Alert - No records in VirusTotal database	3	281
5502 PAM: Login session closed. 3 182 80792 Audit: Command: /usr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dykg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dykg (Debian Package) installed. 7 73 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dykg (Debian Package) requested to install.	80792	Audit: Command: /usr/bin/rm.	3	249
80792 Audit: Command: /usr/bin/dpkg. 3 159 5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 80792 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/pasename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/basename. 3 3 46 80792 Audit: Command: /usr/bin/make. 3 3 4 <tr< td=""><td>5501</td><td>PAM: Login session opened.</td><td>3</td><td>185</td></tr<>	5501	PAM: Login session opened.	3	185
5402 Successful sudo to ROOT executed. 3 148 553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 46 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: C	5502	PAM: Login session closed.	3	182
553 File deleted. 7 143 100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/bibexec/gc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/pasename. 3 52 80792 Audit: Command: /usr/bin/basename. 3 47 80792 Audit: Command: /usr/bin/make. 3 47 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/b	80792	Audit: Command: /usr/bin/dpkg.	3	159
100301 File added to /home directory. 5 135 80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/bin/make. 3 34 80792	5402	Successful sudo to ROOT executed.	3	148
80792 Audit: Command: /usr/bin/cat. 3 126 550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/make. 3 46 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/rest. 3 29 100210<	553	File deleted.	7	143
550 Integrity checksum changed. 7 116 554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/test. 3 32 80792 Audit: Command: /usr/bin/test. 3 39 80792	100301	File added to /home directory.	5	135
554 File added to the system. 5 116 80792 Audit: Command: /usr/libexec/gc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/test. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210	80792	Audit: Command: /usr/bin/cat.	3	126
80792 Audit: Command: /usr/libexec/gcc/x86_64. 3 107 40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 34 80792 Audit: Command: /usr/bin/make. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/loin/tyara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nsudo 12 7	550	Integrity checksum changed.	7	116
40704 Systemd: Service exited due to a failure. 5 84 2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/test. 3 32 80792 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 7 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bi	554	File added to the system.	5	116
2904 Dpkg (Debian Package) half configured. 7 81 80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/test. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	80792	Audit: Command: /usr/libexec/gcc/x86_64.	3	107
80792 Audit: Command: /usr/bin/perl. 3 78 2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/sbin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	40704	Systemd: Service exited due to a failure.	5	84
2902 New dpkg (Debian Package) installed. 7 73 100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	2904	Dpkg (Debian Package) half configured.	7	81
100210 Audit: Highly Suspicious Command executed: /usr/bin/bash 12 70 80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 34 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/bin/make. 3 32 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	80792	Audit: Command: /usr/bin/perl.	3	78
80792 Audit: Command: /usr/bin/grep. 3 65 80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 34 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	2902	New dpkg (Debian Package) installed.	7	73
80792 Audit: Command: /usr/bin/basename. 3 52 2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	100210	Audit: Highly Suspicious Command executed: /usr/bin/bash	12	70
2901 New dpkg (Debian Package) requested to install. 3 47 80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	80792	Audit: Command: /usr/bin/grep.	3	65
80792 Audit: Command: /usr/bin/m4. 3 46 80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	80792	Audit: Command: /usr/bin/basename.	3	52
80792 Audit: Command: /usr/sbin/unix_chkpwd. 3 44 80792 Audit: Command: /usr/bin/make. 3 34 80792 Audit: Command: /usr/lib/apt/methods/http. 3 32 80792 Audit: Command: /usr/bin/test. 3 29 100210 Audit: Highly Suspicious Command executed: /usr/bin/sudo 12 29 80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	2901	New dpkg (Debian Package) requested to install.	3	47
80792Audit: Command: /usr/bin/make.33480792Audit: Command: /usr/lib/apt/methods/http.33280792Audit: Command: /usr/bin/test.329100210Audit: Highly Suspicious Command executed: /usr/bin/sudo122980792Audit: Command: /usr/local/bin/yara.328100210Audit: Highly Suspicious Command executed: /usr/bin/nc127	80792	Audit: Command: /usr/bin/m4.	3	46
80792Audit: Command: /usr/lib/apt/methods/http.33280792Audit: Command: /usr/bin/test.329100210Audit: Highly Suspicious Command executed: /usr/bin/sudo122980792Audit: Command: /usr/local/bin/yara.328100210Audit: Highly Suspicious Command executed: /usr/bin/nc127	80792	Audit: Command: /usr/sbin/unix_chkpwd.	3	44
80792Audit: Command: /usr/bin/test.329100210Audit: Highly Suspicious Command executed: /usr/bin/sudo122980792Audit: Command: /usr/local/bin/yara.328100210Audit: Highly Suspicious Command executed: /usr/bin/nc127	80792	Audit: Command: /usr/bin/make.	3	34
100210Audit: Highly Suspicious Command executed: /usr/bin/sudo122980792Audit: Command: /usr/local/bin/yara.328100210Audit: Highly Suspicious Command executed: /usr/bin/nc127	80792	Audit: Command: /usr/lib/apt/methods/http.	3	32
80792 Audit: Command: /usr/local/bin/yara. 3 28 100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	80792	Audit: Command: /usr/bin/test.	3	29
100210 Audit: Highly Suspicious Command executed: /usr/bin/nc 12 7	100210	Audit: Highly Suspicious Command executed: /usr/bin/sudo	12	29
	80792	Audit: Command: /usr/local/bin/yara.	3	28
100210 Audit: Highly Suspicious Command executed: /usr/bin/chmod 12 4	100210	Audit: Highly Suspicious Command executed: /usr/bin/nc	12	7
	100210	Audit: Highly Suspicious Command executed: /usr/bin/chmod	12	4



87104 VirusTratak Alert - Anomerkalik local/share/nautilus/tags/metaudb-shm - No positives found 3 4 87104 VirusTostak Alert - Anomerkalik local/share/nautilus/tags/metaudb-val - No positives found 3 4 87104 VirusTostak Alert - Anomerkalik (ache/mozilla/firefox/cs2l/vm8z default-esr/satmup-incomplete - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (ache/mozilla/firefox/cs2l/vm8z default-esr/sock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/cs2l/vm8z default-esr/sock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/cs2l/vm8z default-esr/fock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/cs2l/vm8z default-esr/fock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/cs2l/vm8z default-esr/fock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/cs2l/vm8z default-esr/fock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/cs2l/vm8z default-esr/fock - No positives found 3 2 87104 VirusTostak Alert - Anomerkalik (mozilla/firefox/	Rule ID	Description	Level	Count
100110 Audit: Highly Suspicious Command executed: Austr/bin/su 12 2 2 37104 Virus Total: Alert - Anome/hall/cache/mozilla/firefox/cs2lwm82.default-esr/sacrup-incomplete - No positives found 3 2 87104 Virus Total: Alert - Anome/hall/cache/mozilla/firefox/cs2lwm82.default-esr/sacre2/ce T151c2VyQ29udGV4dEkPTUs 3 2 No positives found 3 3 2 87104 Virus Total: Alert - Anome/hall/cache/mozilla/firefox/cs2lwm82.default-esr/sacre. No positives found 3 2 87104 Virus Total: Alert - Anome/hall/Desktop/Diamorphine/.git/brooks/update.csmple - No positives found 3 2 87104 Virus Total: Alert - Anome/hall/Desktop/Diamorphine/.git/brooks/update.csmple - No positives found 3 2 87104 Virus Total: Alert - Anome/hall/Desktop/Diamorphine/.git/brooks/update.csmple - No positives found 3 2 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	87104	VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-shm - No positives found	3	4
87104 VirusTotal Alert - Mome/kalif.cache/mozilia/firefox/cs2/km82 default-esr/startup-incomplete - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif.cache/mozilia/firefox/cs2/km82 default-esr/scache/rce_T151c7VyQ29budSVtdFikPTUs - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/mozilia/firefox/cs2/km82 default-esr/fock - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/mozilia/firefox/cs2/km82 default-esr/fock - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/mozilia/firefox/cs2/km82 default-esr/fock - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/moxilia/gydomada2.tx - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/malware/gydomada2.tx - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/malware/gydomada2.tx - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/malware/gydomada2.tx - No positives found 3 2 87104 VirusTotal Alert - Mome/kalif/malware/gydomada2.tx - No positives found 3 2 87107 CIS Distribution Independent Linux Benchmark v. 2.0.0. Ensure Bitchmositive processority is configured. 7 1	87104	VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-wal - No positives found	3	4
Virus Total: Alert - //homer/All/ / Zacher/mozilla/fire/fox/cs/bwm8z.default-esr/tache2/ce_T151c2VyQJ9udGVVdETIRPTUs - 3 2 No positives found	100210	Audit: Highly Suspicious Command executed: /usr/bin/su	12	2
No positives found 87104 VirusTotal Alert - /home/kali/moxilla/firefox/cs2lwm8z.default-esr/lock - No positives found 3 2 87104 VirusTotal Alert - /home/kali/Desktop/Damorphine/,gi/hooks/pusht-ocheskout.sample - No positives found 3 2 87104 VirusTotal Alert - /home/kali/Desktop/Damorphine/,gi/hooks/fupdate.sample - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87104 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87105 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87106 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 2 87107 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 1 87107 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No positives found 3 1 87108 VirusTotal Alert - /home/kali/malware/Jomda2.bit - No	87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/.startup-incomplete - No positives found	3	2
87104 VirusTotal: Alert - /home/kall/Desktop/Diamorphine/_git/hooks/pubate_sample - No positives found 3 2 87104 VirusTotal: Alert - /home/kall/Desktop/Diamorphine/_git/hooks/update_sample - No positives found 3 2 87104 VirusTotal: Alert - /home/kall/makware/3 and 2 2 87104 Audit: Highly Suspicious Command executed: /host/bir/curl 1 2 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure /etc/hosts.deny is configured. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure little is installed. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure PICP is disabled. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure little is installed. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPV6 loopback traffic is configured. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPV6 loopback traffic is configured. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure PICP6 router advertisements are not accepted. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure PICP6 router advertisements are not accepted. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure RDS is disabled. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure Set Ir is disabled. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure Set Ir is disabled. 7 1 19007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure Set Ir is set to 4 or less. 7 1 19007 CIS Distribution independent Linux	87104		3	2
87104 VirusTotal: Alert - /home/kali/Desktop/Diamorphine/ git/hooks/update.sample - No positives found 3 2 87104 VirusTotal: Alert - /home/kali/malware/3omda2.bt No positives found 3 2 87104 VirusTotal: Alert - /home/kali/malware/3omda2.bt No positives found 3 2 87104 VirusTotal: Alert - /home/kali/malware/3omda2.bt No positives found 1 2 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure /etc/hosts deny is configured. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure /etc/hosts deny is configured. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure AIDE is installed. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure AIDE is installed. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure ENd Forefried and the cacepted. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPM default deny firewall policy. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPM default deny firewall policy. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPM default deny firewall policy. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPM default deny firewall policy. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPM forophark traffic is configured. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure IPM forophark traffic is configured. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure Robe is disabled. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure Robe is disabled. 7 1 871007 CIS Distribution independent Linux Benchmark v2.0.0: Ensure Still all still report in the policy of the po	87104	VirusTotal: Alert - /home/kali/.mozilla/firefox/cs2lwm8z.default-esr/lock - No positives found	3	2
ST104 VirusTotal: Alert - Anome-Alail/mailwarer/3 omda 2.txt - No positives found 3 2	87104	VirusTotal: Alert - /home/kali/Desktop/Diamorphine/.git/hooks/push-to-checkout.sample - No positives found	3	2
100710 Audit: Highly Suspicious Command executed: /usr/bin/curl 12 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Disable USB Storage. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure AIDE is installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure AIDE is installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure AIDE is installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Navhi Server is not enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG fedicabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG fedicated fraffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG footback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG footback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IVPG router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Sis disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Sis disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Sis disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Sis Holmore Tipo Sis disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Sis Holmore Tipo Sis disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Sis Holmore Tipo Sis Distribution Independent Linux Benchmark v2.0.0: Ensure Sis Holmore Tipo Sis	87104	VirusTotal: Alert - /home/kali/Desktop/Diamorphine/.git/hooks/update.sample - No positives found	3	2
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Petchosts deny is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDF is Installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDF is Installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AVAID Server is not enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 in opback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 incure advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 incure advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 incure advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure EDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSTH Millor Tepforwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH dile Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAusthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAusthTries is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAusthTries is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensu	87104	VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found	3	2
19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure /etc/hosts.deny is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure AIDE is installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Mahi Server is not enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure DCCP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure ICMP redirects are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPV6 footback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPV6 footback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPV6 independent Linux Benchmark v2.0.0: Ensure BDF is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure REV6 is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure BCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH Independent Linux Independent Linux Benchmark v2.0.0: Ensure SSH Max-Startups is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH Max-Startups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH Max-Startu	100210	Audit: Highly Suspicious Command executed: /usr/bin/curl	12	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is Installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Avahi Server is not enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCH Allows Forwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCH Allows Forwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCH LoginGrace Time is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCH MaxAuthTries is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCH MaxStartups is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Avahi Server is not enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 independent series are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 independent series are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Royal Ensure Service Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Service Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELInux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH AllowTopForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SEH MaxSessions i	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTrp6rowarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DSH MaxSessions is set to 4 or less. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FSH MaxSessions is set to 4 or less. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DSH CPS is not enabled. 9 1 19008	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure ICMP redirects are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SECTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxAuthTries is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure DSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure DSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure DSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure DSH CIS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchm	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Avahi Server is not enabled.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 default deny firewall policy. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH ldler Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH Light Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH Alaxantifries is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SEH MaxSessions is set to 4 or less. 7	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 loopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxStartups is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure CIPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure CIPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure CIPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure FTP Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 router advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure VIMp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure PIMp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Se	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure StLinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Old Signature is set to 4 or less. 7 1 19008 CIS Di	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 loopback traffic is configured.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSestions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BTP Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 router advertisements are not accepted.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed.	7	1
CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled. 7 1 79007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 79007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 7 1 7 1 7 1 7 1 1 7 1 1 1 1 1 1 1 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure Reverse Path Filtering is enabled.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled.	7	1
CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure / tmp is configured. 8 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 9 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Server is not enabled.	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux is not disabled in bootloader configuration.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CSH MaxSessions is set to 4 or less. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DSH True True True True True True True True	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH AllowTcpForwarding is disabled.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH Idle Timeout Interval is configured.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH LoginGraceTime is set to one minute or less.	7	1
19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured. 7 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxAuthTries is set to 4 or less.	7	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxSessions is set to 4 or less.	7	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1	19007	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH MaxStartups is configured.	7	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Disable Automounting.	3	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /tmp is configured.	3	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled. 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled. 3 1 19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled. 3 1	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure CUPS is not enabled.	3	1
19008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.31	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DHCP Server is not enabled.	3	1
19008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.31	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DNS Server is not enabled.	3	1
19008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.31	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure FTP Server is not enabled.	3	1
19008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.3119008CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.31	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure GDM login banner is configured.	3	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled. 3 1	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP Proxy Server is not enabled.	3	1
	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure HTTP server is not enabled.	3	1
19008 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IP forwarding is disabled. 3 1	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IMAP and POP3 server is not enabled.	3	1
	19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IP forwarding is disabled.	3	1



Rule ID	Description	Level	Count
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NFS and RPC are not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NIS Client is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure NIS Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux or AppArmor are installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SETroubleshoot is not installed.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SNMP Server is not enabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH HostbasedAuthentication is disabled.	3	1
19008	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SSH IgnoreRhosts is enabled.	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mesa_shader_cache_db/marker - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/activity-stream.weather_feed.json - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/cache2/ ce_T151c2VyQ29udGV4dElkPTUsYSw= - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/safebrowsing/ads-track-digest256.vlpset - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/safebrowsing/social-tracking-protection-twitter-digest256.vlpset - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-wal - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-wal - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.mozilla/firefox/cs2lwm8z.default-esr/.parentlock - No positives found	3	1



Groups summary

Groups	Count
audit	24066
audit_command	24047
syscheck	1447
ossec	985
syslog	741
auditaudit_command	539
rootcheck	503
syscheck_file	375
pam	372
virustotal	333
dpkg	201
sca	196
authentication_success	185
config_changed	154
sudo	150
syscheck_entry_deleted	143
syscheck_entry_added	116
syscheck_entry_modified	116
local	84
systemd	84
active_response	14
errors	12
audit_anom	11
authentication_failed	11
ids	9
suricata	9
audit_configuration	8
service_availability	6
attack	5
invalid_login	4
sshd	4
accesslog	3
web	3
access_control	2
process_monitor	2
sql_injection	1