

Threat hunting report

Warning. Agent is disconnected

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 3, 2025 @ 17:50:49.000

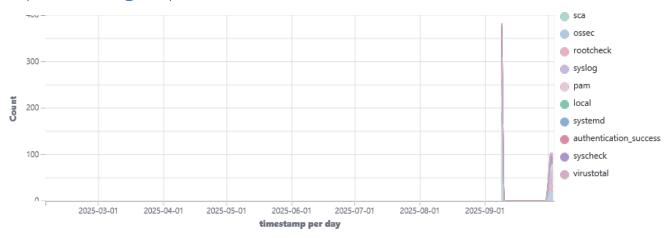
Group: default

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

© 2025-02-03T17:55:34 to 2025-10-03T17:47:03

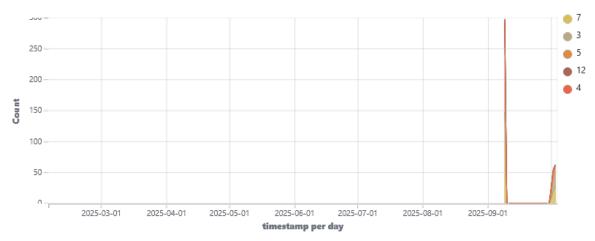
Q manager.name: siem-VMware-Virtual-Platform AND agent.id: 001

Top 10 Alert groups evolution

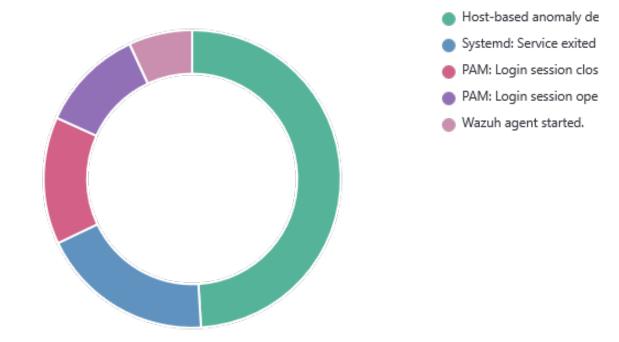




Alerts

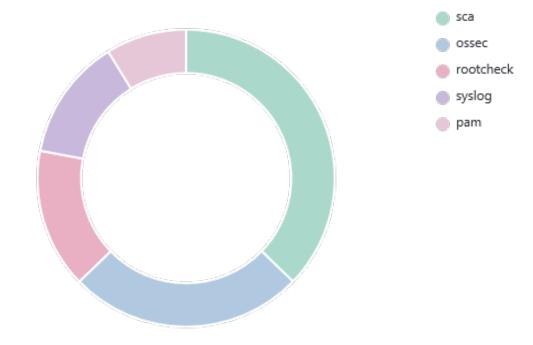


Top 5 alerts

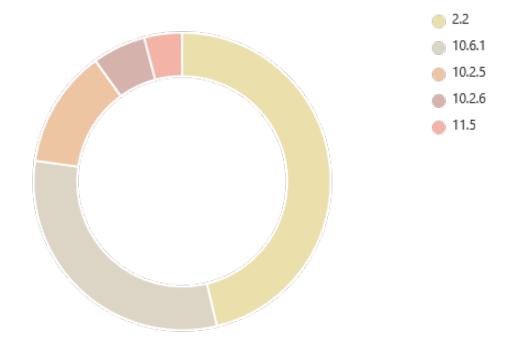




Top 5 rule groups



Top 5 PCI DSS Requirements





438

- Level 12 or above alerts -

2 - Authentication failure -

20
- Authentication success -



Alerts summary

510 Host based anomally detection event (rootcheck). 7 78 40704 Systemic Service exited due to a failure. 5 30 5502 PAM: Login session closed. 3 23 5501 PAM: Login session opened. 3 20 503 Wazuh agent started. 3 12 506 Wazuh agent started. 3 12 507 Wazuh agent started. 3 12 508 Wazuh agent started. 3 12 509 Successful sudo to ROOT executed. 3 8 552 Flie deleted. 7 8 657 Active response; active response/bin/remove-threats.h - add 3 8 554 Flie deleted. 5 7 8 6570 Active response; active response/bin/remove-threats.h - add 3 8 5540 Flie deleted. 5 7 8 65710 Virus Total; Alert - Anome/all/malware/decir - 65 engines detected this file 12 6 87105 Virus Total; Alert	Rule ID	Description	Level	Count
5502 PAM: Login session closed. 3 23 5501 PAM: Login session opened. 3 20 503 Wazuh agent started. 3 12 506 Wazuh agent storpped. 3 12 5402 Successful sudo to ROOT executed. 3 8 553 File deleted. 7 8 657 Active response: active-response/bin/remove-threatish - add 3 8 554 File added to the system. 5 7 87105 VirusTotal: Alert - Americalizmalware/ecir - 66 engines detected this file 12 6 87103 VirusTotal: Alert - No records in VirusTotal database 3 6 8704 Dig (Debian Package) installed. 7 4 2904 Dykig (Debian Package) interstall changed (new port opened or closee). 7 4 33 Listed ports status (restat) changed (new port opened or closee). 7 4 40 Syslogd exiting (logging stopped). 5 3 87105 VirusTotal: Alert - Americalirmalware 7 2	510	Host-based anomaly detection event (rootcheck).	7	78
5501 PAM: Login session opened. 3 20 503 Wazuh agent started. 3 12 506 Wazuh agent startepped. 3 12 5402 Successful suld to ROOT executed. 3 8 553 File deleted. 7 8 657 Active response: active-response/bin/remove-threat.sh - add 3 8 554 File added to the system. 5 7 87105 VirusTotal: Alert - No records in VirusTotal database 3 6 87105 VirusTotal: Alert - No records in VirusTotal database 3 6 87007 VirusTotal: Alert - No records in VirusTotal database 3 6 87105 VirusTotal: Alert - No records in VirusTotal database 3 6 87105 VirusTotal: Alert - No records in VirusTotal database 3 6 87105 VirusTotal: Alert - No records in VirusTotal database 3 6 87104 Ustened ports status (nestatal) changed (new port opened or closed). 7 4 933 Ustened ports status (nestatal) changed (new port open	40704	Systemd: Service exited due to a failure.	5	30
503 Wazuh agent started. 3 12 506 Wazuh agent storpped. 3 12 5402 Successful sudo to ROOT executed. 3 8 553 File deleted. 7 8 657 Active response: active-response/bin/remove-threat.sh - add 3 8 554 File added to the system. 5 7 87103 VirusTotal. Alert - No records in VirusTotal database 5 7 87103 VirusTotal. Alert - No records in VirusTotal database 3 6 87104 Dpkg (Debian Package) installed. 7 4 2902 New dpkg (Debian Package) installed. 7 4 2904 Dpkg (Debian Package) and configured. 7 4 533 Listened ports status (nestal) changed (new port opened or closed). 7 4 540 Syslogd exiting (logging stopped). 5 3 87105 VirusTotal. Alert - /home/kail/malware/cir - 65 engines detected this file 12 2 10001 File added to /home/kail/malware/cir - 65 engines detected this file <td< td=""><td>5502</td><td>PAM: Login session closed.</td><td>3</td><td>23</td></td<>	5502	PAM: Login session closed.	3	23
506 Wazuh agent stopped. 3 12 5402 Successful sudo to ROOT executed. 3 8 553 File deleted. 7 8 657 Active response: active-response/bin/remove-threat.sh - add 3 8 554 File added to the system. 5 7 87105 VirusTotal: Alert - /home/kall/malware/ecir - 66 engines detected this file 12 6 87103 VirusTotal: Alert - No records in VirusTotal database 3 6 2902 New dpkg (Deblan Package) half configured. 7 4 2904 Dpkg (Deblan Package) half configured. 7 4 33 Listened ports status (netstat) changed (new port opened or closed). 7 4 34 Sysingd exiting (logging stopped). 5 3 37 VirusTotal: Alert - /home/kall/malware/cir - 65 engines detected this file 12 2 10001 File added to 7 home/kall/malware/cir - 65 engines detected this file 12 2 10002 File added to 7 home/kall/malware/cir - 65 engines detected this file 12 2	5501	PAM: Login session opened.	3	20
5402 Successful sudo to ROOT executed. 3 8 553 File deleted. 7 8 657 Active response active-response/bin/remove-threat.sh - add 3 8 554 File added to the system. 5 7 87105 VirusTotal: Alert - No records in VirusTotal Idatabase 12 6 87103 VirusTotal: Alert - No records in VirusTotal Idatabase 3 6 2902 New dpkg (Debian Package) haif configured. 7 4 2904 Dpkg (Debian Package) haif configured. 7 4 533 Listened ports status (nestat) changed (new port opened or closed). 7 4 5404 Syslogd exiting (logging stopped). 5 3 87105 VirusTotal: Alert - Nome/kall/malware/cir - 65 engines detected this file 12 2 100201 File added to /home/kall/malware/cir - 65 engines detected this file 12 2 100201 File added to /home/kall/malware/cir - 65 engines detected this file 12 2 100201 File added to /home/kall/malware/cir - 65 engines detected this file 12 <t< td=""><td>503</td><td>Wazuh agent started.</td><td>3</td><td>12</td></t<>	503	Wazuh agent started.	3	12
553 File deleted. 7 8 657 Active response: active-response/bin/remove-threat.sh - add 3 8 554 File added to the system. 5 7 87105 VirusTotal: Alert - /homer/kall/malware/cdir - 66 engines detected this file 12 6 87103 VirusTotal: Alert - No records in VirusTotal database 3 6 2902 New dpkg (Debian Package) Installed. 7 4 2904 Dpkg (Debian Package) Installed. 7 4 2904 Dpkg (Debian Package) Installed. 7 4 533 Listened ports status (netstat) changed (new port opened or closed). 7 4 534 VirusTotal: Alert - /homer/kall/malware 7 4 5000 NirusTotal: Alert - /homer/kall/malware 7 2 2901 New dpkg (Debian Package) requested to install. 3 2 2902 New dpkg (Debian Package) requested to install. 3 2 2901 New dpkg (Debian Package) requested to install. 3 2 2902 New dpkg (Debian Package) reques	506	Wazuh agent stopped.	3	12
Active responser active-response/bin/remove-threat.sh - add File added to the system. 5 7 87105 VirusTotal: Alert - / home/kali/malware/ecir - 66 engines detected this file 12 6 87103 VirusTotal: Alert - / home/kali/malware/ecir - 66 engines detected this file 3 6 87105 VirusTotal: Alert - / home/kali/malware/ecir - 66 engines detected this file 3 7 4 9 902 New dpkg (Debian Package) installed. 7 4 2904 Dpkg (Debian Package) half configured. 7 4 1004 Syslogd exiting (logging stopped). 7 4 1004 Syslogd exiting (logging stopped). 87105 VirusTotal: Alert - / home/kali/malware/ecir - 65 engines detected this file 12 2 100201 File added to /home/kali/malware/ecir - 65 engines detected this file 12 2 100201 File added to /home/kali/malware/ecir - 65 engines detected this file 12 2 100201 File added to /home/kali/malware/acir - 65 engines detected this file 12 2 100201 File added to /home/kali/malware/acir - 65 engines detected this file 12 2 100201 File added to /home/kali/malware/acir - 65 engines detected this file 13 2 14 2 15 2 16 3 3 2 17 4 4 18 3 2 18 7 6 7 7 7 2 18 7 7 8 9 18 7 8 9 18 7 9 7 1 1 19 7 1 1	5402	Successful sudo to ROOT executed.	3	8
File added to the system. 5 7 87105 Virus Total: Alert - /homer/kal/malware/ecir - 66 engines detected this file 12 6 87103 Virus Total: Alert - No records in Virus Total database 3 6 2902 New dpkg (Debian Package) installed. 7 4 2904 Dpkg (Debian Package) half configured. 7 4 2904 Dpkg (Debian Package) half configured. 7 4 1004 Syslogd exiting (logging stopped). 7 4 1005 Virus Total: Alert - /homer/kal/malware/ecir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/ecir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/ecir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/ecir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/acir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/acir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/acir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/acir - 65 engines detected this file 12 2 100201 File added to /homer/kal/malware/3omda2.txt - No positives found 3 2 100307 Cis Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure AlDE is installed. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 idefault deny firewall policy. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 idefault deny firewall policy. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 idefault deny firewall policy. 7 1 10007 Cis Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 idefault deny firewall policy. 7 1 10007 Cis Distr	553	File deleted.	7	8
87105 VirusTotal: Alert - /homer/kali/malware/ecir - 66 engines detected this file 12 6 87103 VirusTotal: Alert - No records in VirusTotal database 3 6 2902 New dpkg (Debian Package) Installed. 7 4 2904 Dpkg (Debian Package) half configured. 7 4 533 Listened ports status (netstat) changed (new port opened or closed). 7 4 1004 Syslogd exiting (logging stopped). 5 3 87105 VirusTotal: Alert - /homer/kali/malware/ecir - 65 engines detected this file 12 2 100201 File added to /homer/kali/malware 65 engines detected this file 12 2 2901 New dpkg (Debian Package) requested to install. 3 2 2901 New dpkg (Debian Package) requested to install. 3 2 4002 Sistinution Independent Linux Benchmark v2.0.0.: Disable USB Storage. 7 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 AlDE is installed. 7 1 19007 CIS Distribution Independent Linux B	657	Active response: active-response/bin/remove-threat.sh - add	3	8
87103VirusTotal: Alert - No records in VirusTotal database362902New dpkg (Debian Package) installed.742904Dpkg (Debian Package) half configured.74533Listened ports status (netstat) changed (new port opened or closed).741004Syslogd exiting (logging stopped).5387105VirusTotal: Alert - /homer/kali/malware percir - 65 engines detected this file122100201File added to /homer/kali/malware percir - 65 engines detected this file1222901New dpkg (Debian Package) requested to install.325403First time user executed sudo.4287104VirusTotal: Alert - /homer/kali/malware/3omda2.txt - No positives found3219007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure BIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 loopback traffic is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 loopback traffic is configured.7119007CIS Distribution Ind	554	File added to the system.	5	7
2902New dpkg (Debian Package) installed.742904Dpkg (Debian Package) half configured.74533Listened ports status (netstat) changed (new port opened or closed).741004Syslogd exiting (logging stopped).5387105VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file122100201File added to /home/kali/malware portional package) requested to install.322901New dpkg (Debian Package) requested to install.325403First time user executed sudo.4287104VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found3219007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AlDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AlDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure PCP is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 Godpalut deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 Godpalut deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPV6 Godpalut deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure PV6 Godpalut deny firewall policy.	87105	VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file	12	6
2904Dykg (Debian Package) half configured.74533Listened ports status (netstat) changed (new port opened or closed).741004Syslogd exiting (logging stopped).5387105VirusTotal: Alert - /home/kall/malware/ecir - 65 engines detected this file122100201File added to /home/kall/malware722901New dpkg (Debian Package) requested to install.325403First time user executed sudo.4287104VirusTotal: Alert - /home/kall/malware/3omda2.txt - No positives found3219007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AlbE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 footbeak traffic is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled.7<	87103	VirusTotal: Alert - No records in VirusTotal database	3	6
533Listened ports status (netstat) changed (new port opened or closed).741004Syslogd exiting (logging stopped).5387105VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file122100201File added to /home/kali/malware722901New dpkg (Debian Package) requested to install.325403First time user executed sudo.4287104VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found3219007CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AlDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AlDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICCP is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 inopback traffic is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 inopback traffic is configured.7119007CIS Distribution Independent Linux Benchmark v2.	2902	New dpkg (Debian Package) installed.	7	4
Syslogd exiting (logging stopped). 5 3	2904	Dpkg (Debian Package) half configured.	7	4
87105VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file122100201File added to /home/kali/malware722901New dpkg (Debian Package) requested to install.325403First time user executed sudo.4287104VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found3219007CIS Distribution Independent Linux Benchmark v2.0.0: Disable USB Storage.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure /etc/hosts.deny is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure AIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure AIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure DCCP is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure ICMP redirects are not accepted.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 default deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 forouter advertisements are not accepted.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure LDAP client is not installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure RDS is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SCTP is disabled.7119007	533	Listened ports status (netstat) changed (new port opened or closed).	7	4
100201File added to /home/kali/malware722901New dpkg (Debian Package) requested to install.325403First time user executed sudo.4287104VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found3219007CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure /etc/hosts.deny is configured.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AIDE is installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AVAIDE Server is not enabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure DCCP is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure ICMP redirects are not accepted.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 forouter advertisements are not accepted.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure LDAP client is not installed.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure RDS is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SCTP is disabled.7119007CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SST AllowTcpForwarding is disabled.7	1004	Syslogd exiting (logging stopped).	5	3
New dpkg (Debian Package) requested to install. First time user executed sudo. 4 2 87104 VirusTotal: Alert - /home/kall/malware/3omda2.txt - No positives found 3 2 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage: 7 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 AlDE is installed. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AlDE 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 Hoopback traffic is configured. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 Prouter advertisements are not accepted. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure IPv6 Prouter 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 RDS 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 SELInux is not disabled in bootloader configuration. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH AllowTcpForvarding is disabled. 7 1 19007 CIS Distribution Independent Linux Benchmark v2.0.0: Ensure SSH LoginGraceTime is set to one minute or less. 7 1	87105	VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file	12	2
First time user executed sudo. First part time server is not enabled. First time user executed sudo. First part exerver is not enabled. First	100201	File added to /home/kali/malware	7	2
87104 VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found 3 2 19007 CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage. 7 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 AlDE 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 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 IPv6 router advertisements 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 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 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 LoginGraceTime is set to one minute or less. 7 1	2901	New dpkg (Debian Package) requested to install.	3	2
CIS Distribution Independent Linux Benchmark v2.0.0.: Disable USB Storage. 7 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 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 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 IPv6 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 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 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 LoginGraceTime is set to one minute or less. 7 1	5403	First time user executed sudo.	4	2
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 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 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 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 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	87104	VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found	3	2
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 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 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.: 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 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 SCTP is 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 Hole 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 /etc/hosts.deny is configured.	7	1
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 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 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 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 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 Avahi Server is not enabled.	7	1
CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure IPv6 default deny firewall policy. 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 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 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 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 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 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 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 LDAP client is not installed.	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 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 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 SCTP 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 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 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 MaxAuthTries is set to 4 or less. 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



Rule ID	Description	Level	Count
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 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 IP forwarding is disabled.	3	1
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
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AppArmor is not disabled in bootloader configuration.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux policy is configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password creation requirements are configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password hashing algorithm is SHA-512.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password reuse is limited.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the SELinux state is enforcing.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the audit configuration is immutable.	3	1
19004	SCA summary: CIS Distribution Independent Linux Benchmark v2.0.0.: Score less than 50% (45)	7	1
501	New wazuh agent connected.	3	1
5503	PAM: User login failed.	5	1
5557	unix_chkpwd: Password check failed.	5	1
591	Log file rotated.	3	1



Groups summary

Groups	Count
sca	191
ossec	131
rootcheck	78
syslog	68
pam	45
local	30
systemd	30
authentication_success	20
syscheck	17
virustotal	16
syscheck_file	15
dpkg	10
sudo	10
active_response	8
	8
config_changed	
syscheck_entry_deleted	
syscheck_entry_added	7
errors	3
authentication_failed	2