wazuh.

info@wazuh.com
https://wazuh.com

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	debian	192.168.101.10	Wazuh v4.9.0	wazuh-server	Debian GNU/Linux 12	Oct 3, 2024 @ 03:36:38.000	Oct 3, 2024 @ 17:38:22.000

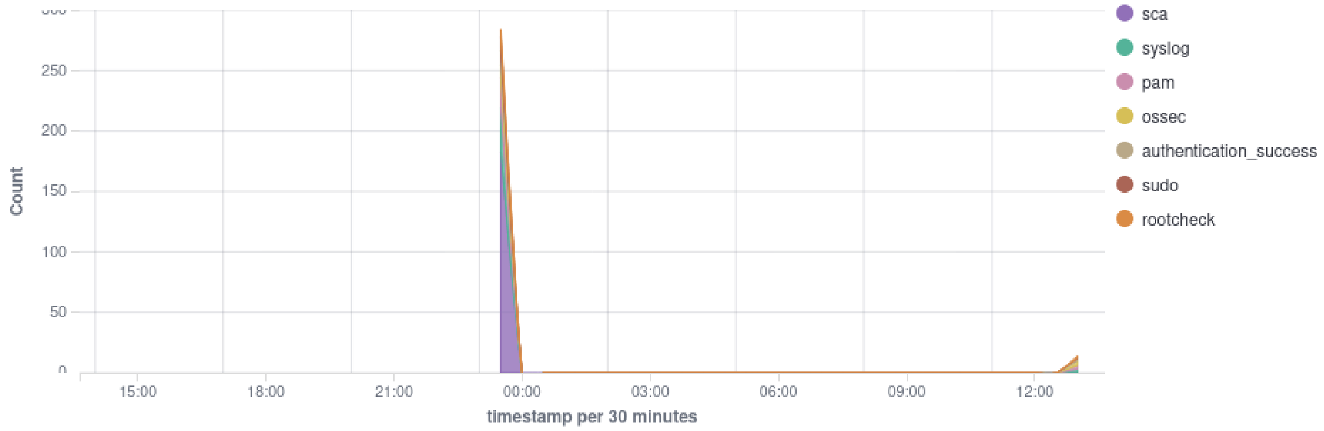
Group: default

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

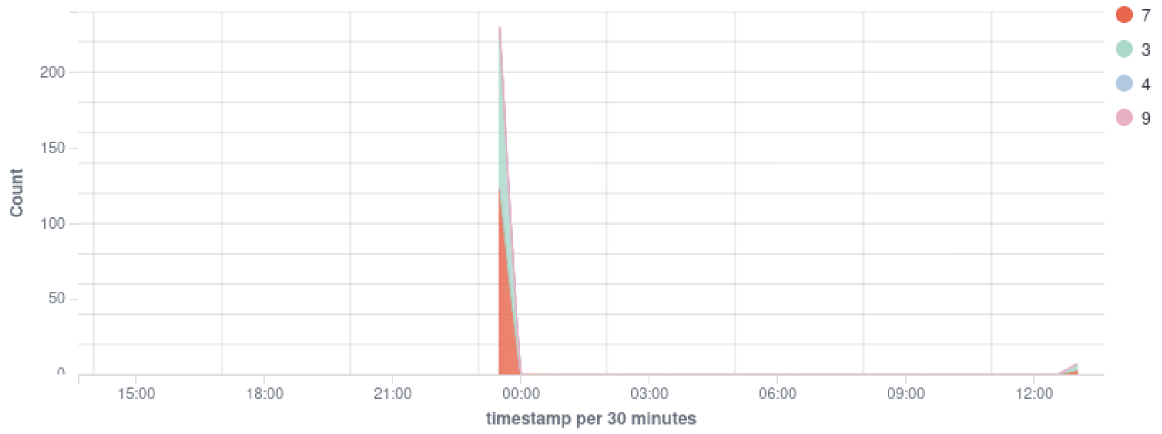
2024-10-02T13:38:21 to 2024-10-03T13:38:21

manager.name: wazuh-server AND agent.id: 002

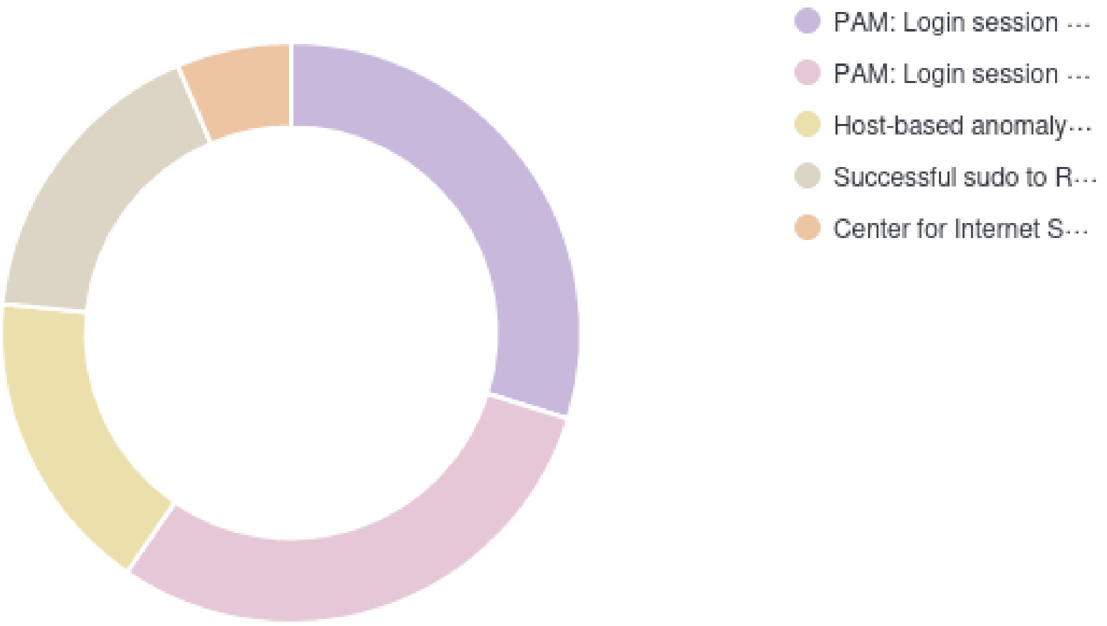
Top 10 Alert groups evolution



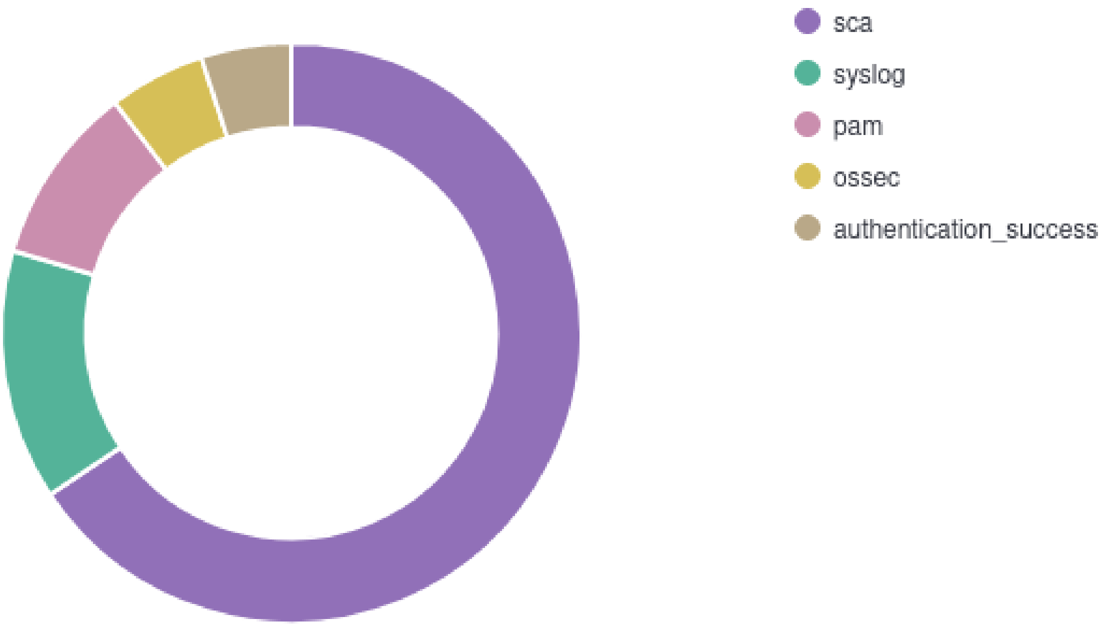
Alerts



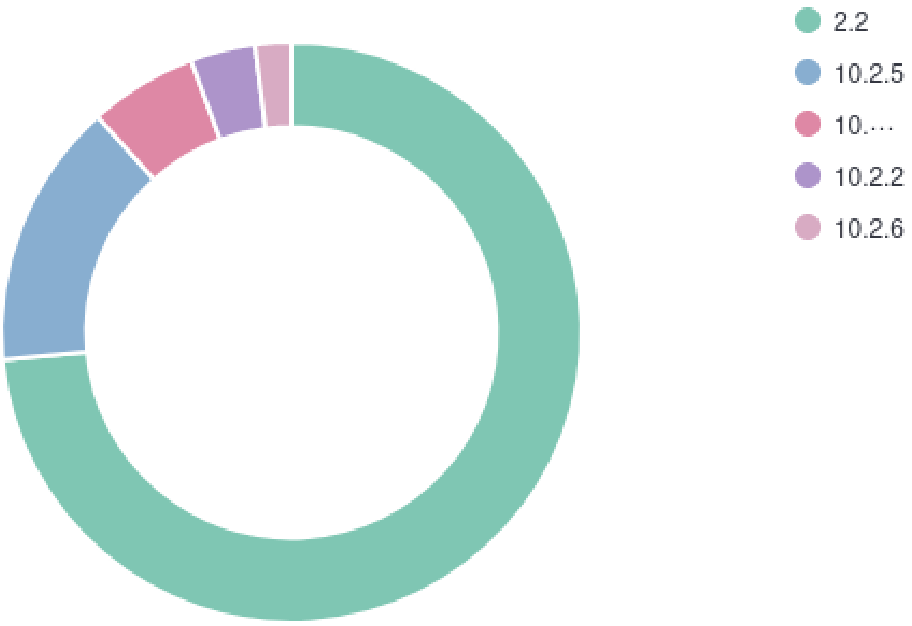
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



237
- Total -

0
- Level 12 or above alerts -

0
- Authentication failure -

14
- Authentication success -

Alerts summary

Rule ID	Description	Level	Count
5501	PAM: Login session opened.	3	14
5502	PAM: Login session closed.	3	14
5402	Successful sudo to ROOT executed.	3	9
510	Host-based anomaly detection event (rootcheck).	7	8
503	Wazuh agent started.	3	3
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NIS Server is not installed.	7	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	7	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure loopback traffic is configured.	7	2
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is not installed or disabled.	3	2
19005	SCA summary: Center for Internet Security Debian Family Linux Benchmark v1.0.0: Score less than 30% (28)	9	2
506	Wazuh agent stopped.	3	2
5403	First time user executed sudo.	4	2
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable Automounting.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable USB Storage.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure /tmp is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AIDE is installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is enabled in the bootloader configuration.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Avahi Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure CUPS is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DCCP is disabled.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DHCP Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DNS Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure FTP Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure GDM is removed or login is configured.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP Proxy Server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP server is not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IMAP and POP3 server are not installed.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 default deny firewall policy.	7	1
19007	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 loopback traffic is configured.	7	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH HostbasedAuthentication is disabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH IgnoreRhosts is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH LogLevel is appropriate.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxSessions is limited.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PAM is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitEmptyPasswords is disabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitUserEnvironment is disabled.	3	1

Rule ID	Description	Level	Count
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TCP SYN Cookies is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure X Window System is not installed.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure XD/NX support is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure address space layout randomization (ASLR) is enabled.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure all AppArmor Profiles are in enforce or complain mode.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure authentication required for single user mode.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure bogus ICMP responses are ignored.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure broadcast ICMP requests are ignored.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure cron daemon is enabled and running.	3	1
19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (sudoers) is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's Mandatory Access Controls are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable.	3	1
19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	3	1
501	New wazuh agent connected.	3	1

Rule ID	Description	Level	Count
533	Listened ports status (netstat) changed (new port opened or closed).	7	1

Groups summary

Groups	Count
sca	183
syslog	39
pam	28
ossec	15
authentication_success	14
sudo	11
rootcheck	8

timestamp	agent.name	rule.description	rule.level	rule.id
Oct 3, 2024 @ 13:48:19.133	debian	PAM: Login session opened.	3	5501
Oct 3, 2024 @ 13:48:19.121	debian	PAM: Login session opened.	3	5501
Oct 3, 2024 @ 13:48:19.119	debian	PAM: Login session closed.	3	5502
Oct 3, 2024 @ 13:48:09.075	debian	PAM: User login failed.	5	5503
Oct 3, 2024 @ 13:47:28.951	debian	PAM: User login failed.	5	5503
Oct 3, 2024 @ 13:47:24.937	debian	PAM: User login failed.	5	5503
Oct 3, 2024 @ 13:46:42.850	debian	Listened ports status (netstat) changed (new port opened or closed).	7	533
Oct 3, 2024 @ 13:46:40.102	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 3, 2024 @ 13:46:40.086	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 3, 2024 @ 13:46:38.687	debian	Wazuh agent started.	3	503
Oct 3, 2024 @ 13:25:08.460	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 3, 2024 @ 13:25:08.441	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 3, 2024 @ 13:25:05.305	debian	PAM: Login session opened.	3	5501
Oct 3, 2024 @ 13:25:05.288	debian	PAM: Login session opened.	3	5501
Oct 3, 2024 @ 13:25:05.286	debian	PAM: Login session closed.	3	5502
Oct 3, 2024 @ 13:25:05.246	debian	Listened ports status (netstat) changed (new port opened or closed).	7	533
Oct 3, 2024 @ 13:25:02.543	debian	Wazuh agent started.	3	503
Oct 2, 2024 @ 23:50:15.175	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:49:19.109	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:49:19.065	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:48:27.049	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:48:27.007	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:47:30.901	debian	PAM: Login session closed.	3	5502

Oct 2, 2024 @ 23:47:28.940	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:47:28.899	debian	First time user executed sudo.	4	5403
Oct 2, 2024 @ 23:47:04.942	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:47:04.942	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:47:04.872	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:47:00.859	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:46:52.892	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:46:52.851	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:44:08.598	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:44:02.588	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:44:02.588	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:43:58.573	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:43:52.569	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:43:52.568	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:43:44.555	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:43:40.564	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:43:40.564	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:40:28.516	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:40:22.545	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @ 23:40:22.533	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @ 23:40:21.183	debian	Wazuh agent started.	3	503
Oct 2, 2024 @ 23:40:19.851	debian	Wazuh agent stopped.	3	506
Oct 2, 2024 @ 23:40:10.923	debian	PAM: Login session closed.	3	5502

Oct 2, 2024 @ 23:39:08.847	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:39:08.837	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:37:56.610	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:37:54.629	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:37:54.610	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:37:38.599	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:37:38.598	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:37:38.594	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @ 23:37:38.590	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:37:38.589	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @ 23:37:38.585	debian	First time user executed sudo.	4	5403
Oct 2, 2024 @ 23:37:35.099	debian	SCA summary: Center for Internet Security Debian Family Linux Benchmark v1.0.0: Score less than 30% (28)	9	19005
Oct 2, 2024 @ 23:37:23.997	debian	SCA summary: Center for Internet Security Debian Family Linux Benchmark v1.0.0: Score less than 30% (28)	9	19005
Oct 2, 2024 @ 23:37:17.366	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure password fields are not empty.	3	19008
Oct 2, 2024 @ 23:37:17.366	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure root is the only UID 0 account.	3	19008
Oct 2, 2024 @ 23:37:17.362	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure accounts in /etc/passwd use shadowed passwords.	7	19007
Oct 2, 2024 @ 23:37:17.291	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/gshadow- are configured.	7	19007
Oct 2, 2024 @ 23:37:17.289	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/gshadow are configured.	7	19007
Oct 2, 2024 @ 23:37:17.258	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/group- are configured.	7	19007
Oct 2, 2024 @ 23:37:17.258	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/shadow- are configured.	7	19007
Oct 2, 2024 @ 23:37:17.257	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/shadow are configured.	7	19007
Oct 2, 2024 @ 23:37:17.255	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/passwd- are configured.	7	19007
Oct 2, 2024 @ 23:37:17.255	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/group are configured.	7	19007

Oct 2, 2024 @ 23:37:17.254	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/passwd are configured.	7	19007
Oct 2, 2024 @ 23:37:17.253	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure access to the su command is restricted.	7	19007
Oct 2, 2024 @ 23:37:17.240	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default group for the root account is GID 0.	3	19008
Oct 2, 2024 @ 23:37:17.239	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure inactive password lock is 30 days or less.	7	19007
Oct 2, 2024 @ 23:37:17.229	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure minimum days between password changes is configured.	7	19007
Oct 2, 2024 @ 23:37:17.229	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure password expiration warning days is 7 or more.	7	19007
Oct 2, 2024 @ 23:37:17.228	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure password hashing algorithm is SHA-512.	7	19007
Oct 2, 2024 @ 23:37:17.228	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure password expiration is 365 days or less.	7	19007
Oct 2, 2024 @ 23:37:17.205	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure password reuse is limited.	3	19008
Oct 2, 2024 @ 23:37:17.203	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure lockout for failed password attempts is configured.	7	19007
Oct 2, 2024 @ 23:37:17.200	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH LoginGraceTime is set to one minute or less.	7	19007
Oct 2, 2024 @ 23:37:17.197	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure password creation requirements are configured.	7	19007
Oct 2, 2024 @ 23:37:17.124	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxStartups is configured.	7	19007
Oct 2, 2024 @ 23:37:17.124	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxSessions is limited.	3	19008
Oct 2, 2024 @ 23:37:17.121	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH AllowTcpForwarding is disabled.	7	19007
Oct 2, 2024 @ 23:37:16.991	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH Idle Timeout Interval is configured.	7	19007
Oct 2, 2024 @ 23:37:16.980	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PAM is enabled.	3	19008
Oct 2, 2024 @ 23:37:16.978	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH access is limited.	7	19007
Oct 2, 2024 @ 23:37:16.978	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH warning banner is configured.	7	19007
Oct 2, 2024 @ 23:37:16.969	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure only strong Key Exchange algorithms are used.	3	19008
Oct 2, 2024 @ 23:37:16.969	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure only strong MAC algorithms are used.	7	19007
Oct 2, 2024 @ 23:37:16.968	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure only strong Ciphers are used.	3	19008
Oct 2, 2024 @ 23:37:16.966	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitUserEnvironment is disabled.	3	19008

Oct 2, 2024 @ 23:37:16.964	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH PermitEmptyPasswords is disabled.	3	19008
Oct 2, 2024 @ 23:37:16.949	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH root login is disabled.	7	19007
Oct 2, 2024 @ 23:37:16.927	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH HostbasedAuthentication is disabled.	3	19008
Oct 2, 2024 @ 23:37:16.926	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH IgnoreRhosts is enabled.	3	19008
Oct 2, 2024 @ 23:37:16.905	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH MaxAuthTries is set to 4 or less.	7	19007
Oct 2, 2024 @ 23:37:16.843	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH X11 forwarding is disabled.	7	19007
Oct 2, 2024 @ 23:37:16.837	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SSH LogLevel is appropriate.	3	19008
Oct 2, 2024 @ 23:37:16.819	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on SSH public host key files are configured.	3	19008
Oct 2, 2024 @ 23:37:16.816	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on SSH private host key files are configured.	3	19008
Oct 2, 2024 @ 23:37:16.766	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/ssh/sshd_config are configured.	7	19007
Oct 2, 2024 @ 23:37:16.765	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure cron is restricted to authorized users.	7	19007
Oct 2, 2024 @ 23:37:16.765	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure at is restricted to authorized users.	7	19007
Oct 2, 2024 @ 23:37:16.763	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/cron.d are configured.	7	19007
Oct 2, 2024 @ 23:37:16.761	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable.	3	19009
Oct 2, 2024 @ 23:37:16.759	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/cron.monthly are configured.	7	19007
Oct 2, 2024 @ 23:37:16.758	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/cron.weekly are configured.	7	19007
Oct 2, 2024 @ 23:37:16.756	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/cron.daily are configured.	7	19007
Oct 2, 2024 @ 23:37:16.755	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/cron.hourly are configured.	7	19007
Oct 2, 2024 @ 23:37:16.754	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure journald is configured to send logs to rsyslog.	3	19008
Oct 2, 2024 @ 23:37:16.751	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/crontab are configured.	7	19007
Oct 2, 2024 @ 23:37:16.751	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure cron daemon is enabled and running.	3	19008
Oct 2, 2024 @ 23:37:16.750	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure logrotate assigns appropriate permissions.	7	19007
Oct 2, 2024 @ 23:37:16.731	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure journald is configured to write logfiles to persistent disk.	7	19007

Oct 2, 2024 @ 23:37:16.715	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure journald is configured to compress large log files.	3	19008
Oct 2, 2024 @ 23:37:16.714	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured.	3	19009
Oct 2, 2024 @ 23:37:16.708	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog Service is enabled.	7	19007
Oct 2, 2024 @ 23:37:16.701	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog is installed.	7	19007
Oct 2, 2024 @ 23:37:16.701	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected.	3	19009
Oct 2, 2024 @ 23:37:16.501	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected.	3	19009
Oct 2, 2024 @ 23:37:16.499	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (sudoers) is collected.	3	19009
Oct 2, 2024 @ 23:37:16.481	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected.	3	19009
Oct 2, 2024 @ 23:37:16.462	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected.	3	19009
Oct 2, 2024 @ 23:37:16.462	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	3	19009
Oct 2, 2024 @ 23:37:16.435	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected.	3	19009
Oct 2, 2024 @ 23:37:16.429	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected.	3	19009
Oct 2, 2024 @ 23:37:16.411	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected.	3	19009
Oct 2, 2024 @ 23:37:16.410	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's Mandatory Access Controls are collected.	3	19009
Oct 2, 2024 @ 23:37:16.409	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected.	3	19009
Oct 2, 2024 @ 23:37:16.407	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected.	3	19009
Oct 2, 2024 @ 23:37:16.406	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected.	3	19009
Oct 2, 2024 @ 23:37:16.386	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full.	3	19009
Oct 2, 2024 @ 23:37:16.385	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted.	3	19009
Oct 2, 2024 @ 23:37:16.378	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit_backlog_limit is sufficient.	7	19007
Oct 2, 2024 @ 23:37:16.378	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured.	3	19009
Oct 2, 2024 @ 23:37:16.377	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure auditing for processes that start prior to auditd is enabled.	7	19007
Oct 2, 2024 @ 23:37:16.249	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure auditd service is enabled.	7	19007

Oct 2, 2024 @ 23:37:16.248	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure auditd is installed.	7	19007
Oct 2, 2024 @ 23:37:16.247	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 loopback traffic is configured.	7	19007
Oct 2, 2024 @ 23:37:16.247	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IPv6 default deny firewall policy.	7	19007
Oct 2, 2024 @ 23:37:16.245	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure loopback traffic is configured.	7	19007
Oct 2, 2024 @ 23:37:16.219	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	7	19007
Oct 2, 2024 @ 23:37:16.219	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is not installed or disabled.	3	19008
Oct 2, 2024 @ 23:37:16.210	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nftables is not installed.	7	19007
Oct 2, 2024 @ 23:37:16.185	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure iptables packages are installed.	7	19007
Oct 2, 2024 @ 23:37:16.180	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nftables service is enabled.	7	19007
Oct 2, 2024 @ 23:37:16.174	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	3	19008
Oct 2, 2024 @ 23:37:16.154	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure loopback traffic is configured.	7	19007
Oct 2, 2024 @ 23:37:16.147	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure base chains exist.	7	19007
Oct 2, 2024 @ 23:37:16.147	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure iptables are flushed.	7	19007
Oct 2, 2024 @ 23:37:16.147	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure a table exists.	7	19007
Oct 2, 2024 @ 23:37:16.136	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is not installed or disabled.	3	19008
Oct 2, 2024 @ 23:37:16.135	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	7	19007
Oct 2, 2024 @ 23:37:16.135	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nftables is installed.	3	19008
Oct 2, 2024 @ 23:37:16.130	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure ufw service is enabled.	7	19007
Oct 2, 2024 @ 23:37:16.130	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure iptables-persistent is not installed.	7	19007
Oct 2, 2024 @ 23:37:16.127	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TIPC is disabled.	7	19007
Oct 2, 2024 @ 23:37:16.127	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Uncomplicated Firewall is installed.	3	19008
Oct 2, 2024 @ 23:37:15.957	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure RDS is disabled.	7	19007
Oct 2, 2024 @ 23:37:15.948	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SCTP is disabled.	7	19007

Oct 2, 2024 @ 23:37:15.947	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DCCP is disabled.	7	19007
Oct 2, 2024 @ 23:37:15.946	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure bogus ICMP responses are ignored.	3	19008
Oct 2, 2024 @ 23:37:15.936	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TCP SYN Cookies is enabled.	3	19008
Oct 2, 2024 @ 23:37:15.934	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure broadcast ICMP requests are ignored.	3	19008
Oct 2, 2024 @ 23:37:15.934	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure LDAP client is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.932	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure RPC is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.916	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure telnet client is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.904	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure talk client is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.897	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsh client is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.885	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NIS Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.882	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NIS Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.878	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mail transfer agent is configured for local-only mode.	3	19008
Oct 2, 2024 @ 23:37:15.878	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsync service is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.836	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure SNMP Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.778	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure IMAP and POP3 server are not installed.	7	19007
Oct 2, 2024 @ 23:37:15.778	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Samba is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.778	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP Proxy Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.777	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure NFS is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.777	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure HTTP server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.772	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure FTP Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.772	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DNS Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.771	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure LDAP server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.766	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DHCP Server is not installed.	7	19007

Oct 2, 2024 @ 23:37:15.764	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure CUPS is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.760	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure Avahi Server is not installed.	7	19007
Oct 2, 2024 @ 23:37:15.759	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure X Window System is not installed.	3	19008
Oct 2, 2024 @ 23:37:15.757	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure ntp is configured.	7	19007
Oct 2, 2024 @ 23:37:15.756	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure chrony is configured.	7	19007
Oct 2, 2024 @ 23:37:15.753	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure systemd-timesyncd is configured.	7	19007
Oct 2, 2024 @ 23:37:15.751	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure time synchronization is in use.	3	19008
Oct 2, 2024 @ 23:37:15.692	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure updates, patches, and additional security software are installed.	3	19008
Oct 2, 2024 @ 23:37:15.564	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure GDM is removed or login is configured.	7	19007
Oct 2, 2024 @ 23:37:15.458	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure local login warning banner is configured properly.	7	19007
Oct 2, 2024 @ 23:37:15.424	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/motd are configured.	7	19007
Oct 2, 2024 @ 23:37:15.423	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure remote login warning banner is configured properly.	7	19007
Oct 2, 2024 @ 23:37:15.421	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/issue are configured.	7	19007
Oct 2, 2024 @ 23:37:15.419	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on /etc/issue.net are configured.	7	19007
Oct 2, 2024 @ 23:37:15.418	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure message of the day is configured properly.	7	19007
Oct 2, 2024 @ 23:37:15.418	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure all AppArmor Profiles are enforcing.	7	19007
Oct 2, 2024 @ 23:37:15.417	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is enabled in the bootloader configuration.	7	19007
Oct 2, 2024 @ 23:37:15.417	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure all AppArmor Profiles are in enforce or complain mode.	3	19008
Oct 2, 2024 @ 23:37:15.414	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AppArmor is installed.	3	19008
Oct 2, 2024 @ 23:37:15.400	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure prelink is disabled.	3	19008
Oct 2, 2024 @ 23:37:15.396	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure prelink is disabled.	7	19007
Oct 2, 2024 @ 23:37:15.395	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure address space layout randomization (ASLR) is enabled.	3	19008
Oct 2, 2024 @ 23:37:15.386	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure XD/NX support is enabled.	3	19008

Oct 2, 2024 @ 23:37:15.384	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure authentication required for single user mode.	3	19008
Oct 2, 2024 @ 23:37:15.383	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure bootloader password is set.	7	19007
Oct 2, 2024 @ 23:37:15.375	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure permissions on bootloader config are configured.	7	19007
Oct 2, 2024 @ 23:37:15.374	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure filesystem integrity is regularly checked.	7	19007
Oct 2, 2024 @ 23:37:15.330	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure AIDE is installed.	7	19007
Oct 2, 2024 @ 23:37:15.328	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure sudo log file exists.	7	19007
Oct 2, 2024 @ 23:37:15.323	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure sudo commands use pty.	3	19008
Oct 2, 2024 @ 23:37:15.315	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure sudo is installed.	3	19008
Oct 2, 2024 @ 23:37:15.195	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure noexec option set on /dev/shm partition.	7	19007
Oct 2, 2024 @ 23:37:15.195	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable USB Storage.	7	19007
Oct 2, 2024 @ 23:37:15.195	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable Automounting.	7	19007
Oct 2, 2024 @ 23:37:15.194	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nodev option set on /dev/shm partition.	3	19008
Oct 2, 2024 @ 23:37:15.144	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nosuid option set on /dev/shm partition.	3	19008
Oct 2, 2024 @ 23:37:15.120	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nodev option set on /home partition.	3	19008
Oct 2, 2024 @ 23:37:15.120	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure separate partition exists for /home.	7	19007
Oct 2, 2024 @ 23:37:15.119	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure separate partition exists for /var/log/audit.	7	19007
Oct 2, 2024 @ 23:37:15.118	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure separate partition exists for /var/log.	7	19007
Oct 2, 2024 @ 23:37:15.117	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure noexec option set on /var/tmp partition.	3	19008
Oct 2, 2024 @ 23:37:15.115	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nodev option set on /var/tmp partition.	3	19008
Oct 2, 2024 @ 23:37:15.115	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nosuid option set on /var/tmp partition.	7	19007
Oct 2, 2024 @ 23:37:15.113	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure separate partition exists for /var/tmp.	7	19007
Oct 2, 2024 @ 23:37:15.112	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure separate partition exists for /var.	7	19007
Oct 2, 2024 @ 23:37:15.111	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure noexec option set on /tmp partition.	3	19008

Oct 2, 2024 @ 23:37:15.111	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nosuid option set on /tmp partition.	3	19008
Oct 2, 2024 @ 23:37:15.080	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure nodev option set on /tmp partition.	3	19008
Oct 2, 2024 @ 23:37:15.079	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure /tmp is configured.	7	19007
Oct 2, 2024 @ 23:37:15.076	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of udf filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:15.045	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of squashfs filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:15.044	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of hfsplus filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:14.950	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of jffs2 filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:14.949	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of hfs filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:14.947	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of freevxfs filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:14.947	debian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure mounting of cramfs filesystems is disabled.	7	19007
Oct 2, 2024 @ 23:37:05.786	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @ 23:37:05.776	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @ 23:37:04.415	debian	Wazuh agent started.	3	503
Oct 2, 2024 @ 23:37:02.135	debian	Wazuh agent stopped.	3	506
Oct 2, 2024 @ 23:37:00.266	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @ 23:37:00.209	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @ 23:36:58.433	debian	New wazuh agent connected.	3	501