

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

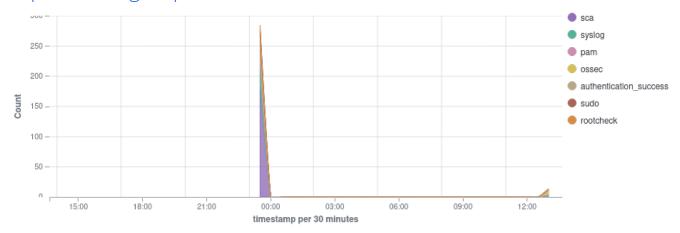
Group: default

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

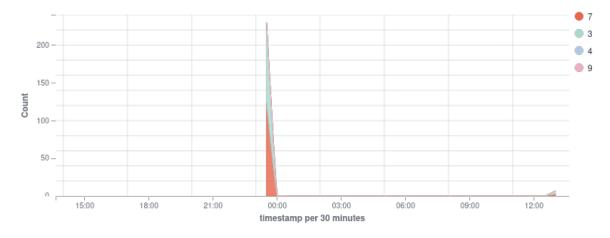
© 2024-10-02T13:38:21 to 2024-10-03T13:38:21

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

Top 10 Alert groups evolution

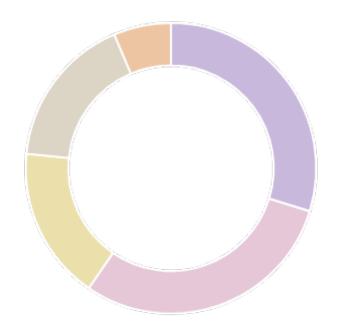


Alerts



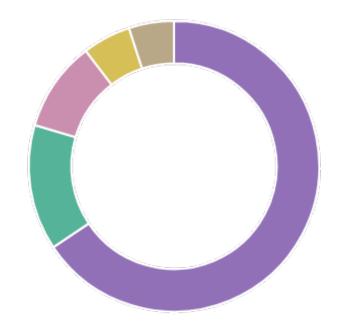
wazuh.

Top 5 alerts



- PAM: Login session ...
- PAM: Login session ...
- Host-based anomaly...
- Successful sudo to R...
- Center for Internet S...

Top 5 rule groups







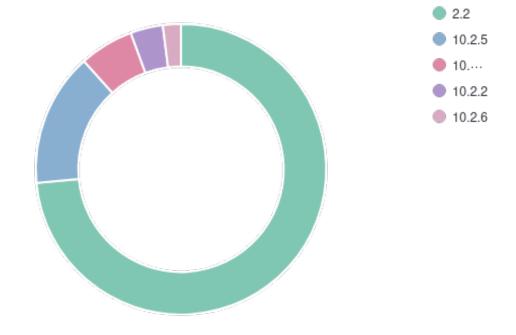




authentication_success



Top 5 PCI DSS Requirements



237

Level 12 or above alerts -

O - 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



Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TCP SYN Coolies is enabled. 3 1	Rule ID	Description	Level	Count
Senter for internet Security Debian Family Linux Benchmark v1.0.0: Ensure XWindow System is not installed. 3 1	19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure TCP SYN Cookies is enabled.	3	1
Secretar 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 Uncomplicated Firewall is installed.	3	1
1908 Certer for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure aldress space Jayout randomization (VSLR) is enabled.	19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure X Window System is not installed.	3	1
(ASI-R) is enabled	19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure XD/NX support is enabled.	3	1
complain mode. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure authentication required for single user mode. Senter for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure bogus ICMP responses are ignored. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure broadcast ICMP requests are ignored. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure condacast ICMP requests are ignored. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure acide to default deny firewall policy. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure acide to default deny firewall policy. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure acide to get storage size is configured. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure acide to get sorage size is configured. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission acide (audiers) is collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network information are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network acide environment are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network acide environment are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network acide environment are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network acideted. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network acideted. C	19008		3	1
mode. 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 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 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured. 3 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted. 3 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (3 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission (2 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission (2 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected. 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network (3 1 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network (3 1 1 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected. 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected. 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19000 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19000 Center for Internet Secur	19008		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 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure addit logs storage size is configured. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure addit logs are not automatically deleted. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure addit logs are not automatically deleted. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure dispression and internet Security Debian Family Linux Benchmark v1.0.0: Ensure dispression and internet Security Debian Family Linux Benchmark v1.0.0: Ensure dispression and internet Security Debian Family Linux Benchmark v1.0.0: Ensure dispression and 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 network environment 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 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group 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 system administrator command 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure syst	19008		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 logs storage size is configured. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission (sudders) is collected. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (sudders) is collected. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time (modification events are collected.) 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network (sandatory 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 (sandatory 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 (sandatory access) (sandatory access) (sandatory a	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 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 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 network and address countrols 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 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 the system's network environment are collected. 3 1	19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure broadcast ICMP requests are ignored.	3	1
19099Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured.3119099Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope and indication events are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network and environment are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected.3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure systog default file permissions3119090Center for Internet Security Debian Family Linux Benchmark v1.0.0: En	19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure cron daemon is enabled and running.	3	1
19099 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted. 3 1 19099 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (suddors) is collected. 3 1 19090 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected. 3 1 19090 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 network 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 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 login and logout events are collected. 3 1 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 3 1 <td>19008</td> <td>Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.</td> <td>3</td> <td>1</td>	19008	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure default deny firewall policy.	3	1
19009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure changes to system administration scope (sudoers) is collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network Mandatory Access Controls are collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network Admards or accollected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected.3119009Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected.3119009Cente	19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit log storage size is configured.	3	1
(sudoers) is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure discretionary access control permission modification events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's and mandatory Access Controls are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group and information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure lied deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure lied deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure syslog default file permissions configured. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable. 19	19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure audit logs are not automatically deleted.	3	1
modification events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify date and time information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's a landatory Access Controls are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable.	19009		3	1
Information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's Mandatory Access Controls are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system default file permissions orofigured. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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 the audit configuration is immutable. 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.	19009		3	1
Mandatory Access Controls are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify the system's network environment are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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 the audit configuration is immutable. 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 the audit configuration is immutable. 3 1	19009		3	1
environment are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure events that modify user/group information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	19009		3	1
information are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions configured. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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.	19009		3	1
19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure kernel module loading and unloading is collected. 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. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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.	19009		3	1
collected. 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. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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 3 1	19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure file deletion events by users are collected.	3	1
Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure rsyslog default file permissions Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	19009		3	1
configured. 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. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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 3 1	19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure login and logout events are collected.	3	1
Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure successful file system mounts are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	19009		3	1
collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system administrator command executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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.	19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure session initiation information is collected.	3	1
executions (sudo) are collected. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure system is disabled when audit logs are full. 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.	19009		3	1
full. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable. 19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access attempts are collected.	19009		3	1
19009 Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure unsuccessful unauthorized file access 3 1 attempts are collected.	19009		3	1
attempts are collected.	19009	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure the audit configuration is immutable.	3	1
501 New wazuh agent connected. 3 1	19009		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_succes	s 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 @	dala i a u	DAM: Heaviled in failed	_	5500
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 @	uebiaii	FAM. Oser login latteu.	3	3303
13:46:42.850	debian	Listened ports status (netstat) changed (new port opened or closed).	7	533
Oct 3, 2024 @	dobian	Electrica porte etatas (netetat) enangos (new port openios en eteces).	,	000
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 @	dalai au	DAM: Login accion anonad		FF04
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 @	debiaii	TAPI. LOGIII SESSIOII Closed.	3	3302
13:25:05.246	debian	Listened ports status (netstat) changed (new port opened or closed).	7	533
Oct 3, 2024 @				555
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 @	dobica	DAMi Login appaign algorid		5500
23:48:27.007	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @ 23:47:30.901	dehian	PAM· Login sassion closed	2	5500
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 @				5 400
23:43:52.568	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @	al a la taux	DAM: Login cooking along d	0	5500
23:43:44.555	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @	dobion	DAM: Login aggion ananod	2	EE01
23:43:40.564 Oct 2, 2024 @	debian	PAM: Login session opened.	3	5501
23:43:40.564	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @	черіан	Successful sudo to NOOT executed.	3	3402
23:40:28.516	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @	acbiaii	1711 1. LUBIN SUSSION CHOSEG.	3	3302
23:40:22.545	debian	Host-based anomaly detection event (rootcheck).	7	510
Oct 2, 2024 @	GODIGIT	Those successfully detection event (rectained).	,	310
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 @	acbian	TAIT. LOGIT 30331011 Opened.	0	3301
23:39:08.837	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @	aobian	Cuccocciations to 11001 choosing.	0	0402
23:37:56.610	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @	aobian	This is Edgin decoration decoration	0	0002
23:37:54.629	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @	aosian	This is 20gin occording policial.		
23:37:54.610	debian	Successful sudo to ROOT executed.	3	5402
Oct 2, 2024 @				0.02
23:37:38.599	debian	PAM: Login session closed.	3	5502
Oct 2, 2024 @	aosian	This is 205 in occording to cook.		
23:37:38.598	debian	PAM: Login session opened.	3	5501
Oct 2, 2024 @		7711 N 20811 000010 11 000110 11		
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 @		SCA summary: Center for Internet Security Debian Family Linux Benchmark		
23:37:35.099	debian	v1.0.0: Score less than 30% (28)	9	19005
Oct 2, 2024 @		SCA summary: Center for Internet Security Debian Family Linux Benchmark		
23:37:23.997	debian	v1.0.0: Score less than 30% (28)	9	19005
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.366	debian	password fields are not empty.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.366	debian	root is the only UID 0 account.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.362	debian	accounts in /etc/passwd use shadowed passwords.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.291	debian	permissions on /etc/gshadow- are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.289	debian	permissions on /etc/gshadow are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.258	debian	permissions on /etc/group- are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.258	debian	permissions on /etc/shadow- are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.257	debian	permissions on /etc/shadow are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.255	debian	permissions on /etc/passwd- are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.255	debian	permissions on /etc/group are configured.	7	19007

0-+0-0004-0		Ocatania de la tamanto Casanita Dabian Familia di mun Danadana adulto O. Faranna		
Oct 2, 2024 @	al a la i a sa	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
23:37:17.254	debian	permissions on /etc/passwd are configured.	7	19007
Oct 2, 2024 @	al a la t a sa	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:17.253	debian	access to the su command is restricted.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:17.240	debian	default group for the root account is GID 0.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:17.239	debian	inactive password lock is 30 days or less.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.229	debian	minimum days between password changes is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.229	debian	password expiration warning days is 7 or more.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.228	debian	password hashing algorithm is SHA-512.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.228	debian	password expiration is 365 days or less.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.205	debian	password reuse is limited.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.203	debian	lockout for failed password attempts is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.200	debian	SSH LoginGraceTime is set to one minute or less.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.197	debian	password creation requirements are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.124	debian	SSH MaxStartups is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.124	debian	SSH MaxSessions is limited.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:17.121	debian	SSH AllowTcpForwarding is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.991	debian	SSH Idle Timeout Interval is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.980	debian	SSH PAM is enabled.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.978	debian	SSH access is limited.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.978	debian	SSH warning banner is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.969	debian	only strong Key Exchange algorithms are used.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.969	debian	only strong MAC algorithms are used.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.968	debian	only strong Ciphers are used.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.966	debian	SSH PermitUserEnvironment is disabled.	3	19008

Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure 23:37:16.964 debian SSH PermitEmptyPasswords is disabled. Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure 23:37:16.949 debian SSH root login is disabled.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	3	190081
	7	10007
S S	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	0	10000
23:37:16.927 debian SSH HostbasedAuthentication is disabled.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	0	40000
23:37:16.926 debian SSH IgnoreRhosts is enabled.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:16.905 debian SSH MaxAuthTries is set to 4 or less.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:16.843 debian SSH X11 forwarding is disabled.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:16.837 debian SSH LogLevel is appropriate.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.819 debian permissions on SSH public host key files are configured.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.816 debian permissions on SSH private host key files are configured.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.766 debian permissions on /etc/ssh/sshd_config are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.765 debian cron is restricted to authorized users.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure at		
23:37:16.765 debian is restricted to authorized users.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.763 debian permissions on /etc/cron.d are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.761 debian the audit configuration is immutable.	3	19009
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.759 debian permissions on /etc/cron.monthly are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.758 debian permissions on /etc/cron.weekly are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.756 debian permissions on /etc/cron.daily are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.755 debian permissions on /etc/cron.hourly are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.754 debian journald is configured to send logs to rsyslog.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.751 debian permissions on /etc/crontab are configured.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.751 debian cron daemon is enabled and running.	3	19008
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.750 debian logrotate assigns appropriate permissions.	7	19007
Oct 2, 2024 @ Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.731 debian journald is configured to write logfiles to persistent disk.	7	19007

0 10 00010		0 . ()		
Oct 2, 2024 @	al a la i a sa	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	0	10000
23:37:16.715	debian	journald is configured to compress large log files.	3	19008
Oct 2, 2024 @	al a la taux	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	0	40000
23:37:16.714	debian	rsyslog default file permissions configured.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:16.708	debian	rsyslog Service is enabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:16.701	debian	rsyslog is installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:16.701	debian	kernel module loading and unloading is collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.501	debian	system administrator command executions (sudo) are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.499	debian	changes to system administration scope (sudoers) is collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.481	debian	file deletion events by users are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.462	debian	successful file system mounts are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.462	debian	unsuccessful unauthorized file access attempts are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.435	debian	discretionary access control permission modification events are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.429	debian	session initiation information is collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.411	debian	login and logout events are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.410	debian	events that modify the system's Mandatory Access Controls are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.409	debian	events that modify the system's network environment are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.407	debian	events that modify user/group information are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.406	debian	events that modify date and time information are collected.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.386	debian	system is disabled when audit logs are full.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.385	debian	audit logs are not automatically deleted.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.378	debian	audit_backlog_limit is sufficient.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.378	debian	audit log storage size is configured.	3	19009
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.377	debian	auditing for processes that start prior to auditd is enabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.249	debian	auditd service is enabled.	7	19007

0-+0-0004-0		Contaging International Consults Debian Family Linux Boneharanks 4 0 0s Family		
Oct 2, 2024 @	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
23:37:16.248	debian	auditd is installed.	7	19007
Oct 2, 2024 @ 23:37:16.247	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
	debian	IPv6 loopback traffic is configured.	7	19007
Oct 2, 2024 @	al a la la ca	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	-	40007
23:37:16.247	debian	IPv6 default deny firewall policy.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:16.245	debian	loopback traffic is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:16.219	debian	default deny firewall policy.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.219	debian	Uncomplicated Firewall is not installed or disabled.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:16.210	debian	nftables is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.185	debian	iptables packages are installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.180	debian	nftables service is enabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.174	debian	default deny firewall policy.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.154	debian	loopback traffic is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.147	debian	base chains exist.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.147	debian	iptables are flushed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure a		
23:37:16.147	debian	table exists.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.136	debian	Uncomplicated Firewall is not installed or disabled.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.135	debian	default deny firewall policy.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.135	debian	nftables is installed.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.130	debian	ufw service is enabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.130	debian	iptables-persistent is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.127	debian	TIPC is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:16.127	debian	Uncomplicated Firewall is installed.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.957	debian	RDS is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.948	debian	SCTP is disabled.	7	19007

0-+0-00040		O-stanfanlatamat O-smith D-bira Family Linux Banaharahad O O Family		
Oct 2, 2024 @	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure DCCP is disabled.	7	10007
23:37:15.947	debian		7	19007
Oct 2, 2024 @ 23:37:15.946	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	2	10000
	debian	bogus ICMP responses are ignored.	3	19008
Oct 2, 2024 @	al a la taux	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.936	debian	TCP SYN Cookies is enabled.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.934	debian	broadcast ICMP requests are ignored.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:15.934	debian	LDAP client is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:15.932	debian	RPC is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
23:37:15.916	debian	telnet client is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.904	debian	talk client is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.897	debian	rsh client is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.885	debian	NIS Server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.882	debian	NIS Server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.878	debian	mail transfer agent is configured for local-only mode.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.878	debian	rsync service is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.836	debian	SNMP Server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.778	debian	IMAP and POP3 server are not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.778	debian	Samba is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.778	debian	HTTP Proxy Server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.777	debian	NFS is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.777	debian	HTTP server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.772	debian	FTP Server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.772	debian	DNS Server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.771	debian	LDAP server is not installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.766	debian	DHCP Server is not installed.	7	19007

0-+0-00046		Contain for Internat Consults Debian Formily Linux Bonches and 1 0 0. Forms		
Oct 2, 2024 @	dahian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure CUPS is not installed.	7	10007
	debian		7	19007
Oct 2, 2024 @	dahian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
	debian	Avahi Server is not installed.	7	19007
Oct 2, 2024 @	-1 - 1- t	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure X	0	40000
	debian	Window System is not installed.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
	debian	ntp is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
	debian	chrony is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
	debian	systemd-timesyncd is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	
	debian	time synchronization is in use.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	updates, patches, and additional security software are installed.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	GDM is removed or login is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	local login warning banner is configured properly.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	permissions on /etc/motd are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	remote login warning banner is configured properly.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.421	debian	permissions on /etc/issue are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.419	debian	permissions on /etc/issue.net are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.418	debian	message of the day is configured properly.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	all AppArmor Profiles are enforcing.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
	debian	AppArmor is enabled in the bootloader configuration.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.417	debian	all AppArmor Profiles are in enforce or complain mode.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.414	debian	AppArmor is installed.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.400	debian	prelink is disabled.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.396	debian	prelink is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.395	debian	address space layout randomization (ASLR) is enabled.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.386	debian	XD/NX support is enabled.	3	19008

0 . 0 . 0 . 0 . 0				
Oct 2, 2024 @	al a la taux	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	0	40000
23:37:15.384	debian	authentication required for single user mode.	3	19008
Oct 2, 2024 @	al a la ta ca	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	-	40007
23:37:15.383	debian	bootloader password is set.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:15.375	debian	permissions on bootloader config are configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:15.374	debian	filesystem integrity is regularly checked.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	-	40007
23:37:15.330	debian	AIDE is installed.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:15.328	debian	sudo log file exists.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.323	debian	sudo commands use pty.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.315	debian	sudo is installed.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:15.195	debian	noexec option set on /dev/shm partition.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable	_	
23:37:15.195	debian	USB Storage.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Disable	_	40007
23:37:15.195	debian	Automounting.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.194	debian	nodev option set on /dev/shm partition.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.144	debian	nosuid option set on /dev/shm partition.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		40000
23:37:15.120	debian	nodev option set on /home partition.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	_	40007
23:37:15.120	debian	separate partition exists for /home.	7	19007
Oct 2, 2024 @	al a la ta ca	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	-	40007
23:37:15.119	debian	separate partition exists for /var/log/audit.	7	19007
Oct 2, 2024 @	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
23:37:15.118	debian	separate partition exists for /var/log.	7	19007
Oct 2, 2024 @	al a la i a sa	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	2	10000
23:37:15.117	debian	noexec option set on /var/tmp partition.	3	19008
Oct 2, 2024 @	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	2	10000
23:37:15.115	debian	nodev option set on /var/tmp partition.	3	19008
Oct 2, 2024 @	dobion	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
23:37:15.115	debian	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	7	19007
	uebiaii	separate partition exists for /var/tmp.	7	19007
Oct 2, 2024 @	dobian	Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	10007
23:37:15.112	debian	separate partition exists for /var. Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure	7	19007
Oct 2, 2024 @	dobian	· ·	2	10000
23:37:15.111	debian	noexec option set on /tmp partition.	3	19008

Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.111	debian	nosuid option set on /tmp partition.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.080	debian	nodev option set on /tmp partition.	3	19008
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.079	debian	/tmp is configured.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.076	debian	mounting of udf filesystems is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.045	debian	mounting of squashfs filesystems is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:15.044	debian	mounting of hfsplus filesystems is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:14.950	debian	mounting of jffs2 filesystems is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:14.949	debian	mounting of hfs filesystems is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:14.947	debian	mounting of freevxfs filesystems is disabled.	7	19007
Oct 2, 2024 @		Center for Internet Security Debian Family Linux Benchmark v1.0.0: Ensure		
23:37:14.947	debian	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