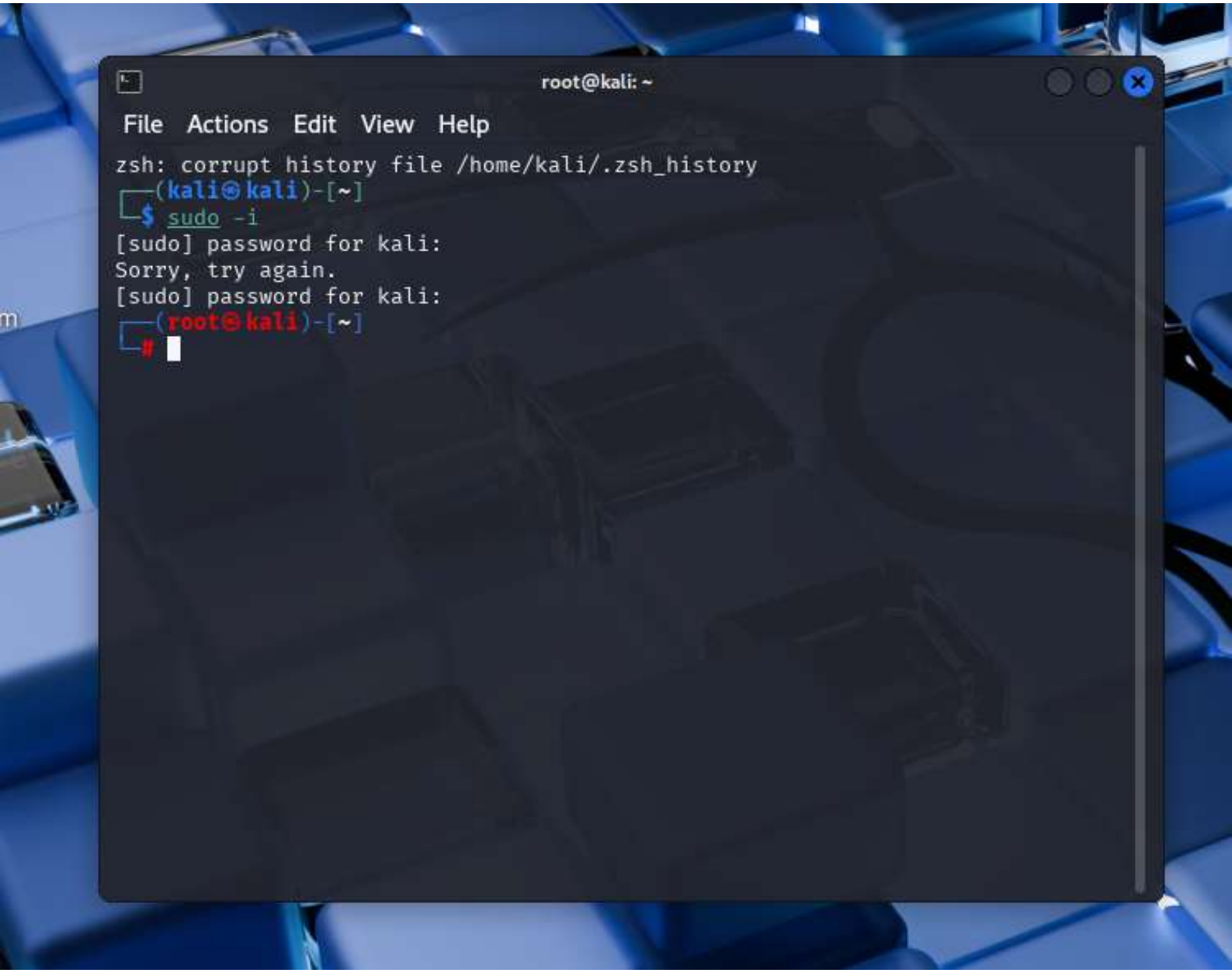
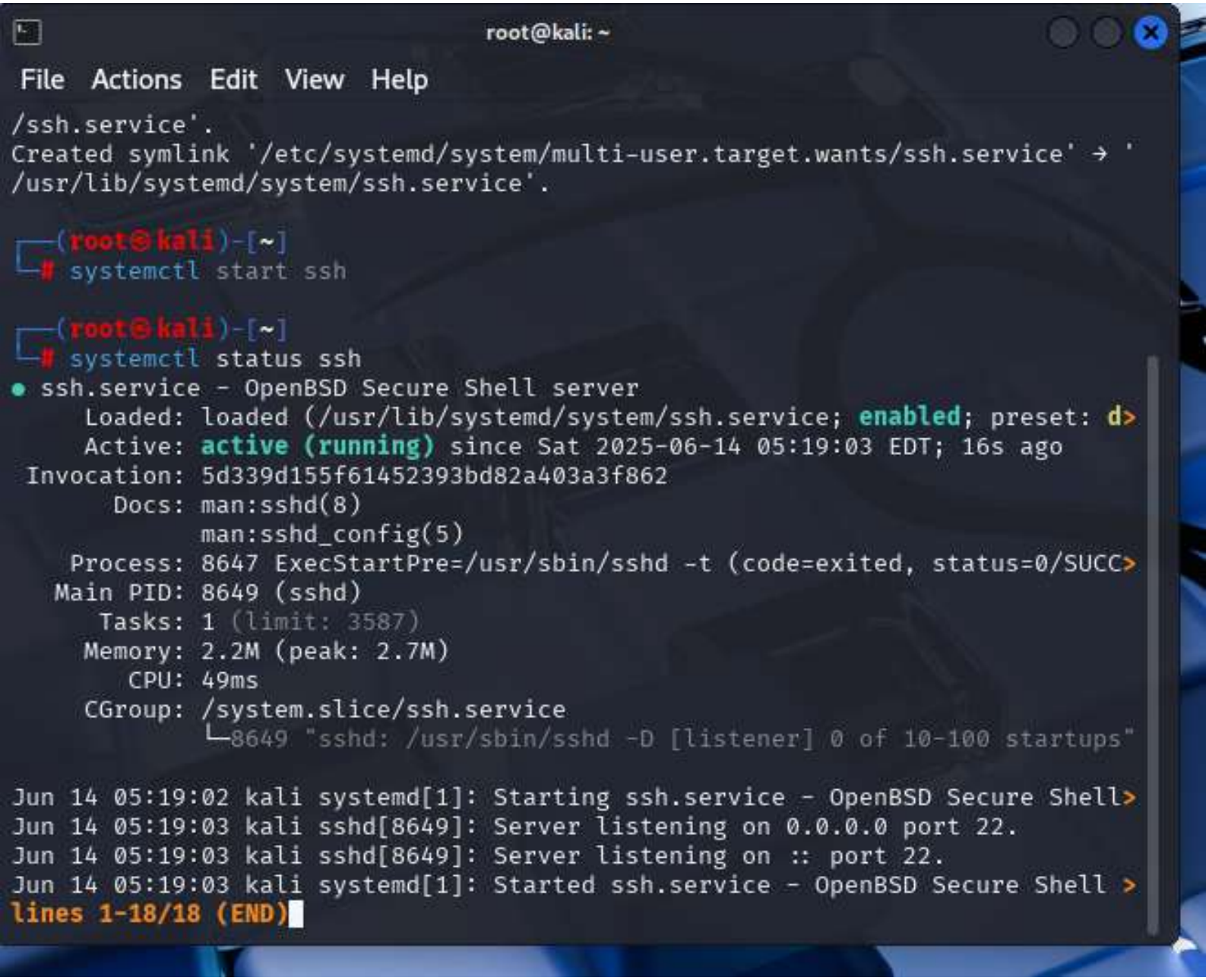
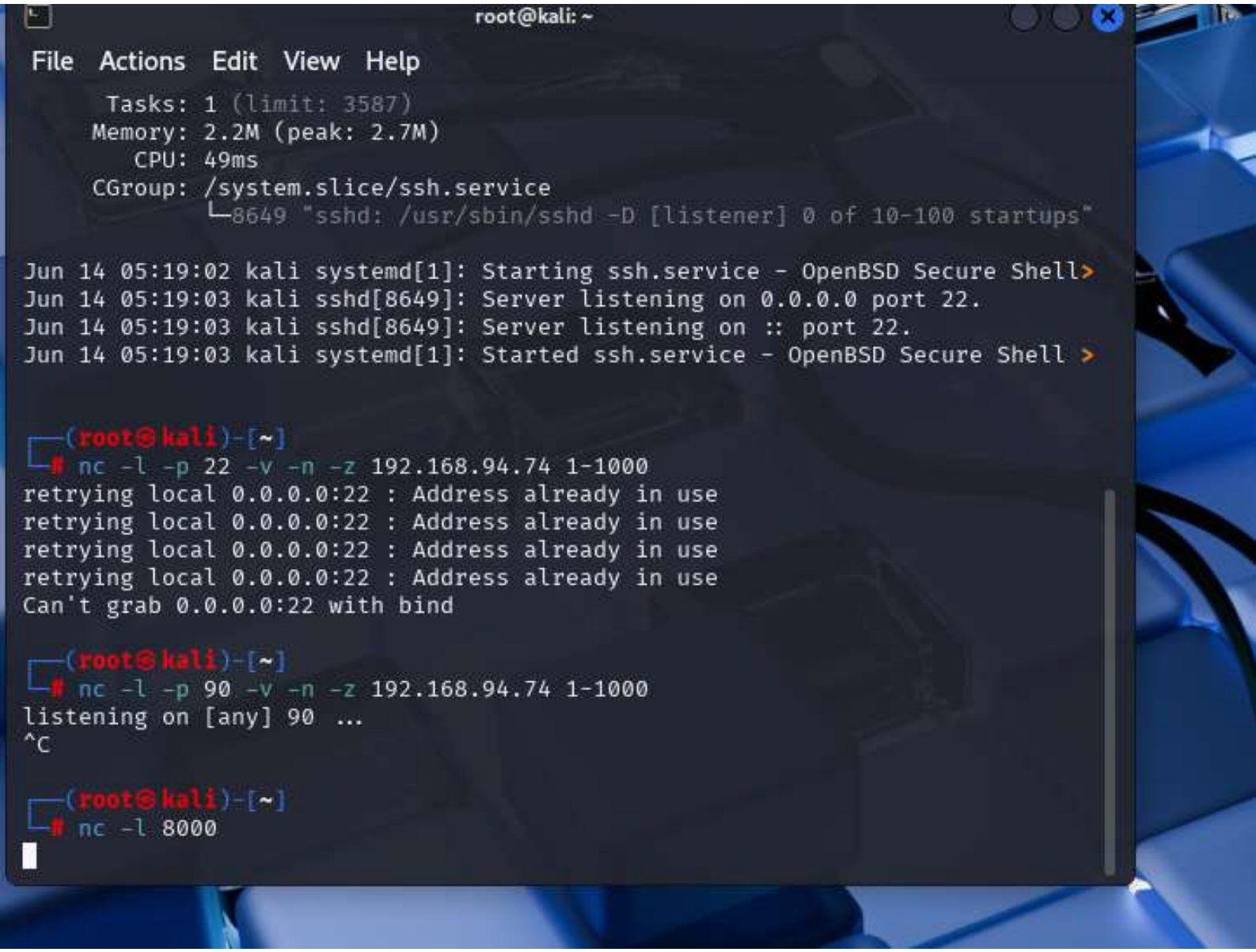
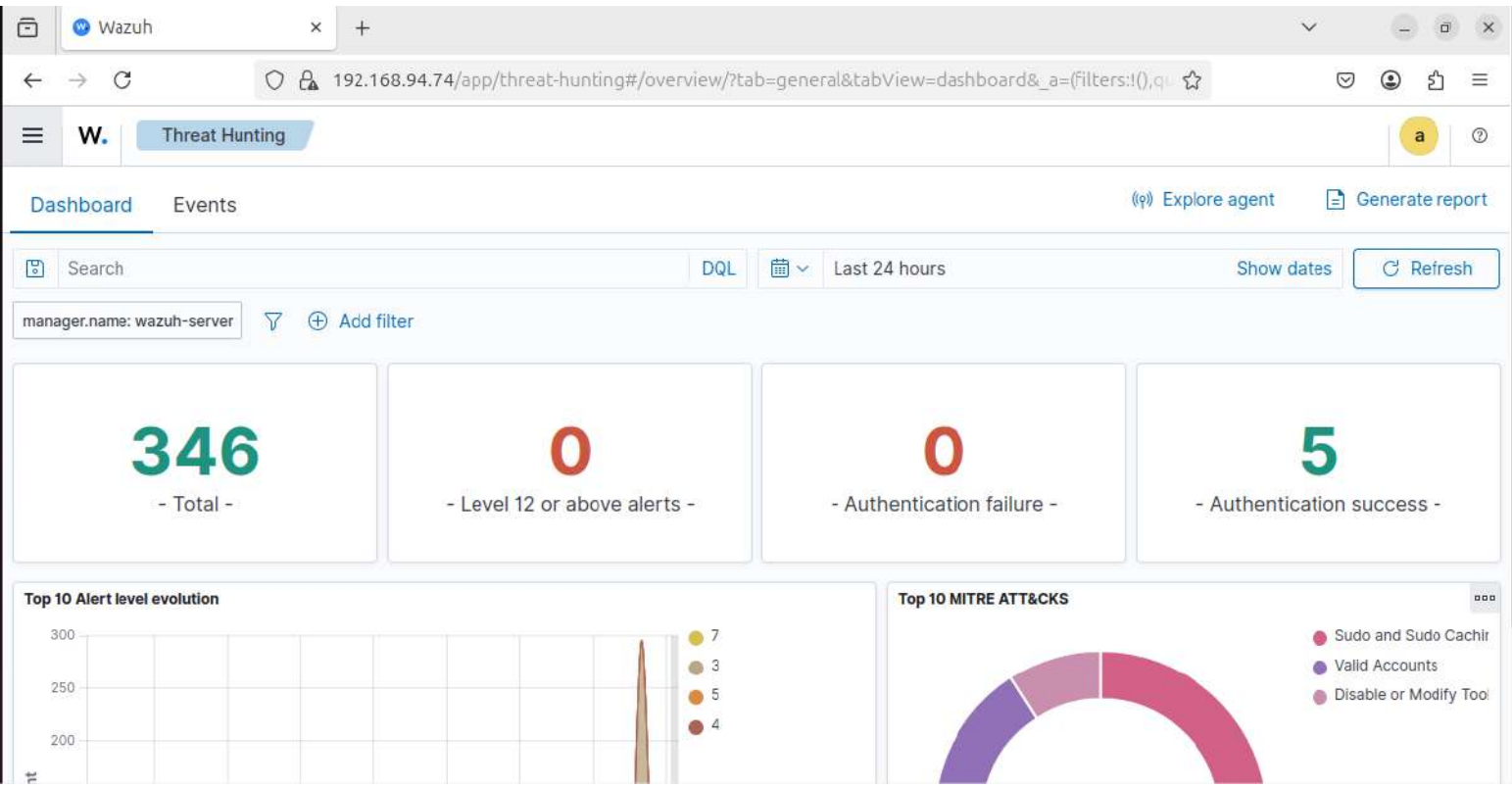
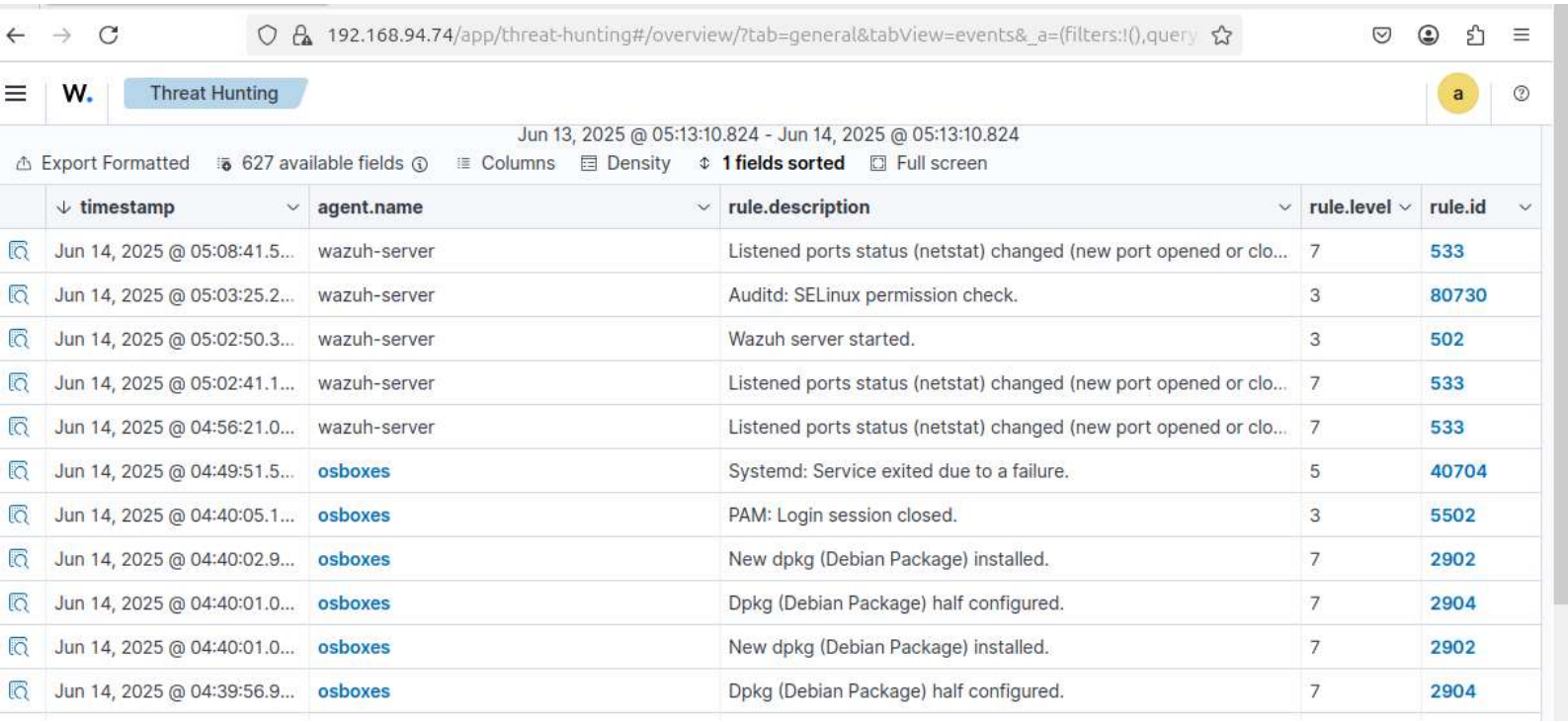

root@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ sudo -i
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
(root㉿kali)-[~]
#


root@kali: ~
File Actions Edit View Help
/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
┌──(root㉿kali)-[~]
└─# systemctl start ssh
┌──(root㉿kali)-[~]
└─# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: d>
Active: active (running) since Sat 2025-06-14 05:19:03 EDT; 16s ago
Invocation: 5d339d155f61452393bd82a403a3f862
Docs: man:sshd(8)
man:sshd_config(5)
Process: 8647 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCC>
Main PID: 8649 (sshd)
Tasks: 1 (limit: 3587)
Memory: 2.2M (peak: 2.7M)
CPU: 49ms
CGroup: /system.slice/ssh.service
└─8649 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Jun 14 05:19:02 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell>
Jun 14 05:19:03 kali sshd[8649]: Server listening on 0.0.0.0 port 22.
Jun 14 05:19:03 kali sshd[8649]: Server listening on :: port 22.
Jun 14 05:19:03 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell >
lines 1-18/18 (END)


root@kali: ~
File Actions Edit View Help
Tasks: 1 (limit: 3587)
Memory: 2.2M (peak: 2.7M)
CPU: 49ms
CGroup: /system.slice/ssh.service
└─8649 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Jun 14 05:19:02 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell>
Jun 14 05:19:03 kali sshd[8649]: Server listening on 0.0.0.0 port 22.
Jun 14 05:19:03 kali sshd[8649]: Server listening on :: port 22.
Jun 14 05:19:03 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell >
┌──(root㉿kali)-[~]
└─# nc -l -p 22 -v -n -z 192.168.94.74 1-1000
retrying local 0.0.0.0:22 : Address already in use
retrying local 0.0.0.0:22 : Address already in use
retrying local 0.0.0.0:22 : Address already in use
retrying local 0.0.0.0:22 : Address already in use
Can't grab 0.0.0.0:22 with bind
┌──(root㉿kali)-[~]
└─# nc -l -p 90 -v -n -z 192.168.94.74 1-1000
listening on [any] 90 ...
^C
┌──(root㉿kali)-[~]
└─# nc -l 8000


Wazuh
192.168.94.74/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_a=(filters:!(),qu
W.
Threat Hunting
a
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
Add filter
346
- Total -
0
- Level 12 or above alerts -
0
- Authentication failure -
5
- Authentication success -
Top 10 Alert level evolution
300
250
200
7
3
5
4
Top 10 MITRE ATT&CKS
Sudo and Sudo Cachir
Valid Accounts
Disable or Modify Tool


192.168.94.74/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query
W.
Threat Hunting
a
Jun 13, 2025 @ 05:13:10.824 - Jun 14, 2025 @ 05:13:10.824
Export Formatted
627 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Jun 14, 2025 @ 05:08:41.5... wazuh-server Listened ports status (netstat) changed (new port opened or clo... 7 533
Jun 14, 2025 @ 05:03:25.2... wazuh-server Auditd: SELinux permission check. 3 80730
Jun 14, 2025 @ 05:02:50.3... wazuh-server Wazuh server started. 3 502
Jun 14, 2025 @ 05:02:41.1... wazuh-server Listened ports status (netstat) changed (new port opened or clo... 7 533
Jun 14, 2025 @ 04:56:21.0... wazuh-server Listened ports status (netstat) changed (new port opened or clo... 7 533
Jun 14, 2025 @ 04:49:51.5... osboxes Systemd: Service exited due to a failure. 5 40704
Jun 14, 2025 @ 04:40:05.1... osboxes PAM: Login session closed. 3 5502
Jun 14, 2025 @ 04:40:02.9... osboxes New dpkg (Debian Package) installed. 7 2902
Jun 14, 2025 @ 04:40:01.0... osboxes Dpkg (Debian Package) half configured. 7 2904
Jun 14, 2025 @ 04:40:01.0... osboxes New dpkg (Debian Package) installed. 7 2902
Jun 14, 2025 @ 04:39:56.9... osboxes Dpkg (Debian Package) half configured. 7 2904

Document Details

View surrounding documents

View single document

Table JSON

t _index	wazuh-alerts-4.x-2025.06.14
t agent.id	000
t agent.name	wazuh-server
t decoder.name	ossec
t full_log	ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* /usr tcp6 :::22 :::* /usr udp 192.168.94.74:68 0.0.0.0:* 2173/systemd-networ udp 127.0.0.1:323 0.0.0.0:* 1638/chronyd udp6 ::1:323 :::* 1638/chronyd
t id	1749892121.1211285
t input.type	log
t location	netstat listening ports
t manager.name	wazuh-server
t previous_log	ossec: output: 'netstat listening p tcp 0.0.0.0:22 0.0.0.0:* /usr tcp6 :::22 :::* /usr udp 192.168.94.74:68 0.0.0.0:* 2173/systemd-networ udp 127.0.0.1:323 0.0.0.0:* 1638/chronyd

Document Details

View surrounding documents | View single document

t	previous_output	Previous output: ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* /usr tcp6 :::22 :::* /usr udp 192.168.94.74:68 0.0.0.0:* 2173/systemd-networ udp 127.0.0.1:323 0.0.0.0:* 1638/chronyd
t	rule.description	Listened ports status (netstat) changed (new port opened or closed).
#	rule.firedtimes	2
t	rule.gdpr	IV_35.7.d
t	rule.gpg13	10.1
t	rule.groups	ossec
t	rule.hipaa	164.312.b
t	rule.id	533
#	rule.level	7
◕	rule.mail	false
t	rule.nist_800_53	AU.14, AU.6
t	rule.pci_dss	10.2.7, 10.6.1
t	rule.tsc	CC6.8, CC7.2, CC7.3
🗓	timestamp	Jun 14, 2025 @ 05:08:41.543

349 hits

Jun 13, 2025 @ 05:23:02.798 - Jun 14, 2025 @ 05:23:02.798

Export Formatted | 627 available fields | Columns | Density | **1 fields sorted** | Full screen

	timestamp	agent.name	rule.description	rule.level	rule.id
	Jun 14, 2025 @ 05:19:11.9...	osboxes	Apparmor DENIED	3	52002
	Jun 14, 2025 @ 05:19:11.9...	osboxes	Apparmor DENIED	3	52002
	Jun 14, 2025 @ 05:19:11.9...	osboxes	Apparmor messages grouped.	3	52000
	Jun 14, 2025 @ 05:08:41.5...	wazuh-server	Listened ports status (netstat) changed (new port opened or clo...	7	533
	Jun 14, 2025 @ 05:03:25.2...	wazuh-server	Auditd: SELinux permission check.	3	80730
	Jun 14, 2025 @ 05:02:50.3...	wazuh-server	Wazuh server started.	3	502
	Jun 14, 2025 @ 05:02:41.1...	wazuh-server	Listened ports status (netstat) changed (new port opened or clo...	7	533
	Jun 14, 2025 @ 04:56:21.0...	wazuh-server	Listened ports status (netstat) changed (new port opened or clo...	7	533
	Jun 14, 2025 @ 04:49:51.5...	osboxes	Systemd: Service exited due to a failure.	5	40704

Document Details

View surrounding documents

View single document

Table | JSON

t	_index	wazuh-alerts-4.x-2025.06.14
t	agent.id	001
t	agent.ip	192.168.94.59
t	agent.name	osboxes
t	decoder.name	ossec
t	full_log	ossec: output: 'process list': PID USER COMMAND 1 root /sbin/init splash 2 root [kthreadd] 3 root [pool_workqueue_release] 4 root [kworker/R-rcu_g] 5 root [kworker/R-rcu_p]
t	id	1749895376.1218542
t	input.type	log
t	location	process list
t	manager.name	wazuh-server
t	rule.description	netcat listening for incoming connection.
#	rule.firedtimes	1
t	rule.groups	ossec, process_monitor

Document Details

View surrounding documents

View single document

t	decoder.name	ossec
t	full_log	ossec: output: 'process list': PID USER COMMAND 1 root /sbin/init splash 2 root [kthreadd] 3 root [pool_workqueue_release] 4 root [kworker/R-rcu_g] 5 root [kworker/R-rcu_p]
t	id	1749895376.1218542
t	input.type	log
t	location	process list
t	manager.name	wazuh-server
t	rule.description	netcat listening for incoming connection.
#	rule.firedtimes	1
t	rule.groups	ossec, process_monitor
t	rule.id	100051
#	rule.level	7
◕	rule.mail	false
📅	timestamp	Jun 14, 2025 @ 06:02:56.054

Document Details

View surrounding documents

View single document

Table JSON

t	_index	wazuh-alerts-4.x-2025.06.14
t	agent.id	000
t	agent.name	wazuh-server
t	decoder.name	ossec
t	full_log	ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* /usr tcp6 :::22 :::* /usr udp 192.168.94.74:68 0.0.0.0:* 2173/systemd-networ udp 127.0.0.1:323 0.0.0.0:* 1638/chronyd udp6 ::1:323 :::* 1638/chronyd
t	id	1749895728.1236414
t	input.type	log
t	location	netstat listening ports
t	manager.name	wazuh-server
t	previous_log	ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* /usr tcp6 :::22 :::* /usr