Matrixon Systems - Major Project Report

Title: Attack, Detection & Hardening of Enterprise Infrastructure Using SIEM
Student Name: Kaushal Jung Thapa
Semester: 5th
Course: Certified Ethical Hacking
Date: 25 Dec 2025

Table of Contents

---

1. Project Overview

Objective: Simulate real-world cyberattacks, detect security events using a SIEM solution, and apply system hardening measures.

Scope: - conducting red team attacks on internal and web servers, collecting and correlating logs through the Wazuh SIEM platform, and implementing system hardening measures such as SSH, Apache, and firewall configurations.

Infrastructure Diagram:

```
[VM2 - Web Server / Attacker]
          |
          | attacks
          v
[VM1 - Internal Server] & [VM2 - Self for Web logs]
          |
          | logs forwarded
          v
[VM3 - SIEM / Log Analyzer]
```

---

2. Environment Setup

VM	Role	IP (Example)	Purpose
VM1	Internal Server	10.0.1.4	Victim
VM2	Web Server	10.0.1.5	Attacker & Victim
VM3	SIEM Server	10.0.1.7	Log collection, analysis

Preparatory Steps: - Update all VMs: `sudo apt update && sudo apt upgrade -y` - Set hostnames: VM1 → `internal-server`, VM2 → `web-server`, VM3 → `siem`

---

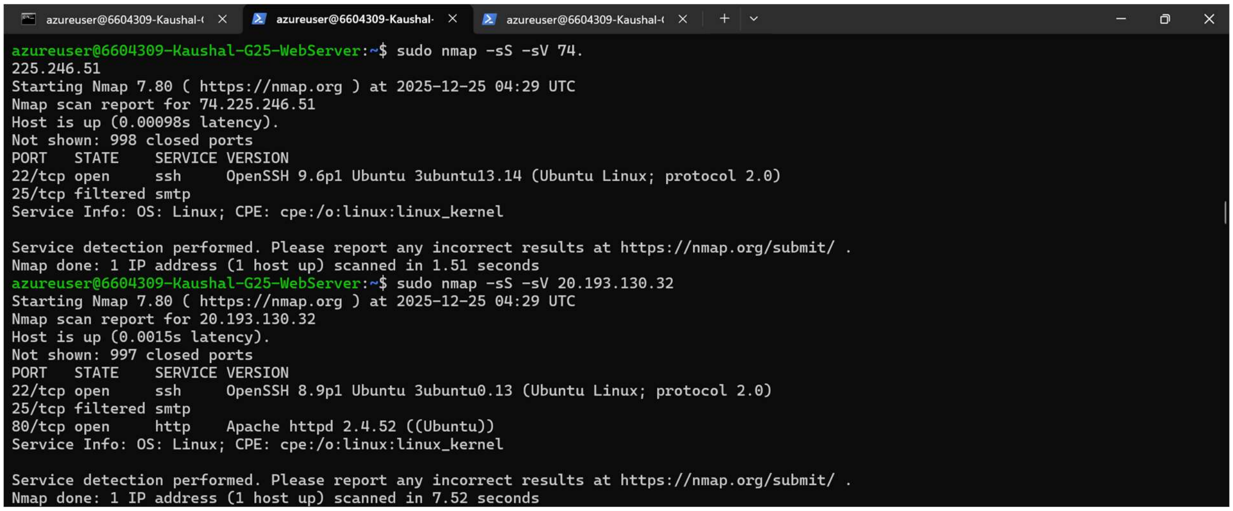
3. Red Team Simulation (Attacks)

3.1 Port Scanning

Command (VM2):

```
nmap -sS -sV VM_IP
nmap -sS -sV VM_IP
```

Purpose: Identify open ports and running services. **Logs:** `/var/log/syslog` (VM1 & VM2), Wazuh alerts (VM3)


azureuser@6604309-Kaushal-(
azureuser@6604309-Kaushal-
azureuser@6604309-Kaushal-(

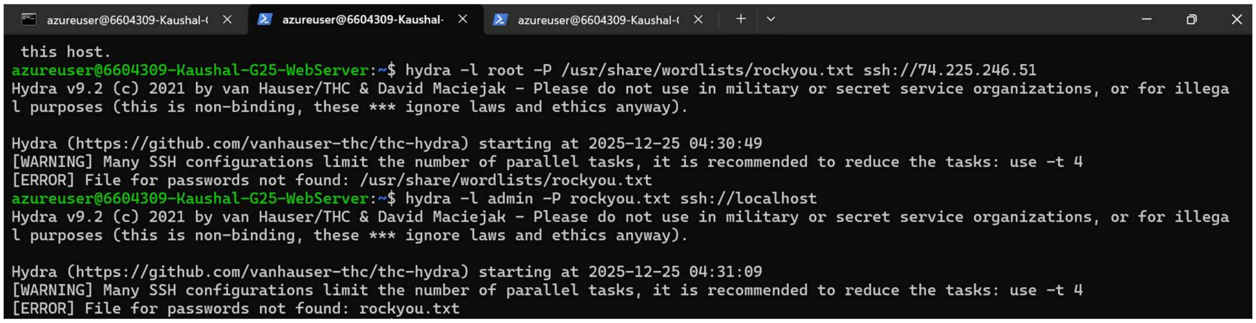
```
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nmap -sS -sV 74.
225.246.51
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 04:29 UTC
Nmap scan report for 74.225.246.51
Host is up (0.00098s latency).
Not shown: 998 closed ports
PORT    STATE    SERVICE VERSION
22/tcp open     ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
25/tcp filtered smtp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nmap -sS -sV 20.193.130.32
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 04:29 UTC
Nmap scan report for 20.193.130.32
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT    STATE    SERVICE VERSION
22/tcp open     ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
25/tcp filtered smtp
80/tcp open     http    Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

3.2 SSH Brute Force Attack

Command (VM2):

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://VM_IP
```

Logs: `/var/log/auth.log` (VM1), SIEM alerts (VM3)



azureuser@6604309-Kaushal-(
azureuser@6604309-Kaushal-
azureuser@6604309-Kaushal-(

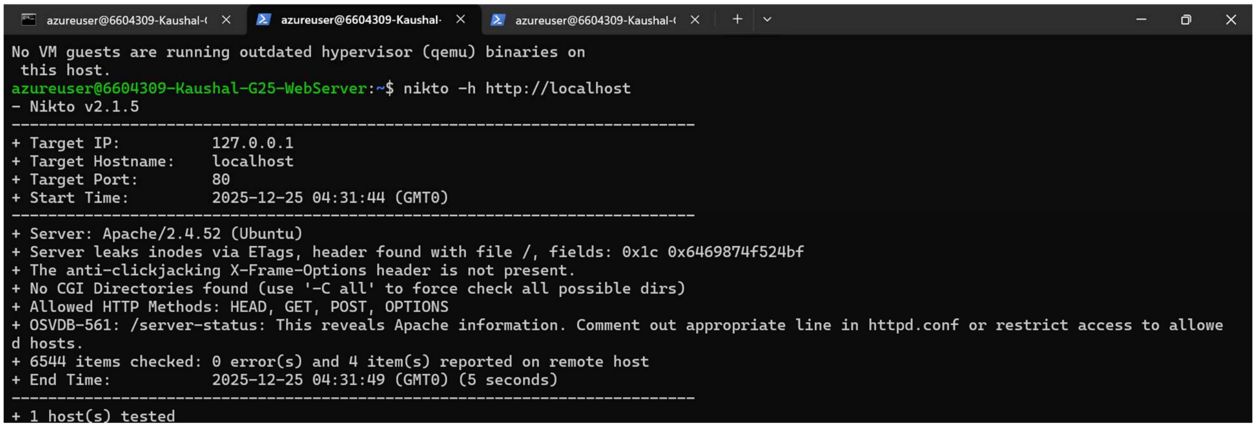
```
 this host.
azureuser@6604309-Kaushal-G25-WebServer:~$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://74.225.246.51
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-25 04:30:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt
azureuser@6604309-Kaushal-G25-WebServer:~$ hydra -l admin -P rockyou.txt ssh://localhost
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-25 04:31:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: rockyou.txt
```

3.3 Web Attacks

Commands (VM2):

```
nikto -h http://localhost
gobuster dir -u http://localhost -w /usr/share/wordlists/dirb/common.txt
```

Logs: `/var/log/apache2/access.log` & `/var/log/apache2/error.log` (VM2), Wazuh alerts (VM3)



azureuser@6604309-Kaushal-(
azureuser@6604309-Kaushal-
azureuser@6604309-Kaushal-(

```
No VM guests are running outdated hypervisor (qemu) binaries on
 this host.
azureuser@6604309-Kaushal-G25-WebServer:~$ nikto -h http://localhost
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2025-12-25 04:31:44 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x1c 0x6469874f524bf
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to allowe
d hosts.
+ 6544 items checked: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-12-25 04:31:49 (GMT0) (5 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

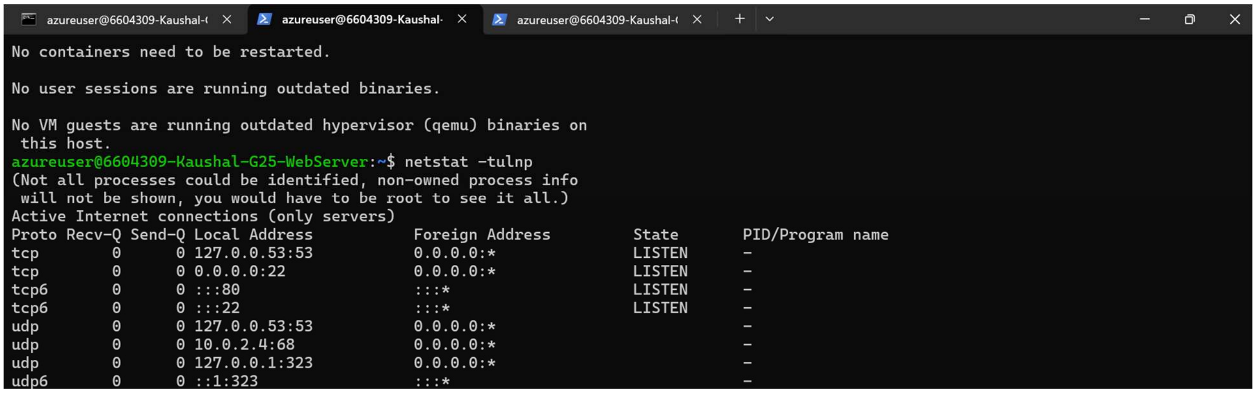
3.4 Privilege Escalation & Enumeration

Commands:

```
sudo -l
find / -perm -4000 2>/dev/null
uname -a
```

```
id
netstat -tulnp
```

Logs: Forwarded to SIEM for monitoring

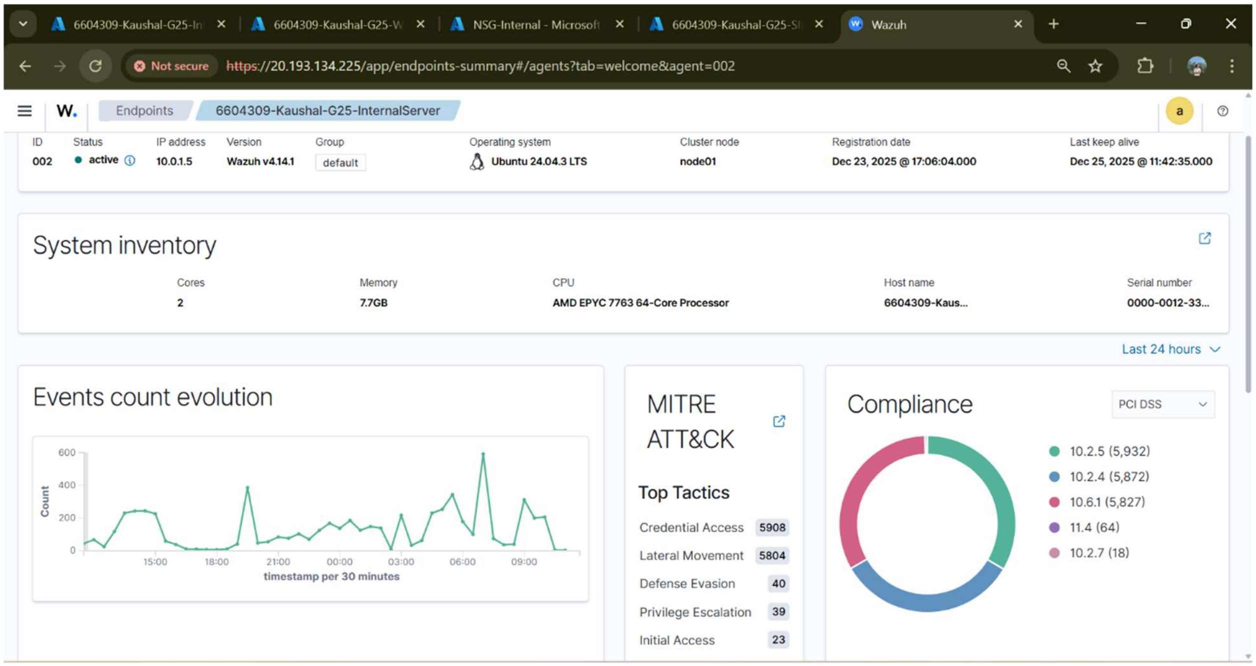

azureuser@6604309-Kaushal-(
azureuser@6604309-Kaushal-
azureuser@6604309-Kaushal-(

```
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on
 this host.
azureuser@6604309-Kaushal-G25-WebServer:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.0.2.4:68             0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp6       0      0 ::1:323                 :::*                                -
```

---

4. SIEM Investigation

- Captured all attacks via Wazuh agent
- Categorized alerts: Authentication failures, Web attacks, Scan detection, Privilege escalation



ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
002	● active	10.0.1.5	Wazuh v4.14.1	default	Ubuntu 24.04.3 LTS	node01	Dec 23, 2025 @ 17:06:04.000	Dec 25, 2025 @ 11:42:35.000

System inventory

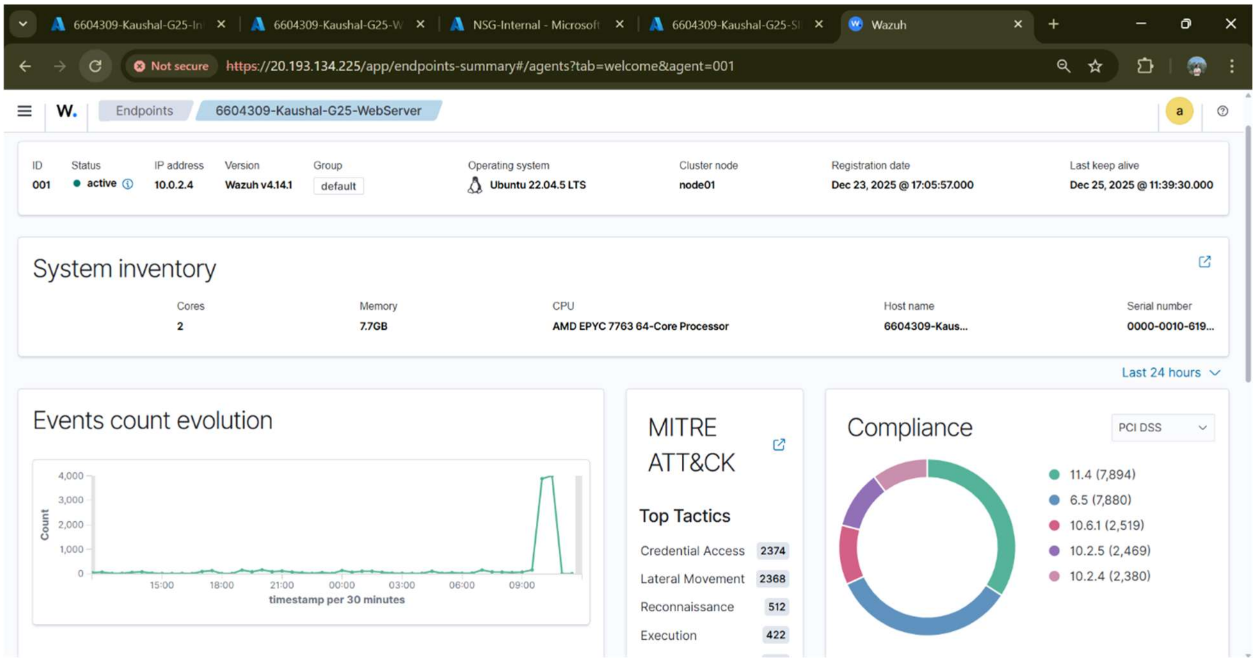
Cores	Memory	CPU	Host name	Serial number
2	7.7GB	AMD EPYC 7763 64-Core Processor	6604309-Kaus...	0000-0012-33...

Last 24 hours

MITRE ATT&CK

Top Tactics

Credential Access	5908
Lateral Movement	5804
Defense Evasion	40
Privilege Escalation	39
Initial Access	23



https://20.193.134.225/app/endpoints-summary#/agents?tab=welcome&agent=001

Endpoints / 6604309-Kaushal-G25-WebServer

ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
001	active	10.0.2.4	Wazuh v4.14.1	default	Ubuntu 22.04.5 LTS	node01	Dec 23, 2025 @ 17:05:57.000	Dec 25, 2025 @ 11:39:30.000

System inventory

Cores	Memory	CPU	Host name	Serial number
2	7.7GB	AMD EPYC 7763 64-Core Processor	6604309-Kaus...	0000-0010-619...

Last 24 hours

Events count evolution

MITRE ATT&CK

Top Tactics

Credential Access	2374
Lateral Movement	2368
Reconnaissance	512
Execution	422

Compliance

PCI DSS

- 11.4 (7,894)
- 6.5 (7,880)
- 10.6.1 (2,519)
- 10.2.5 (2,469)
- 10.2.4 (2,380)

5. Hardening and Mitigation

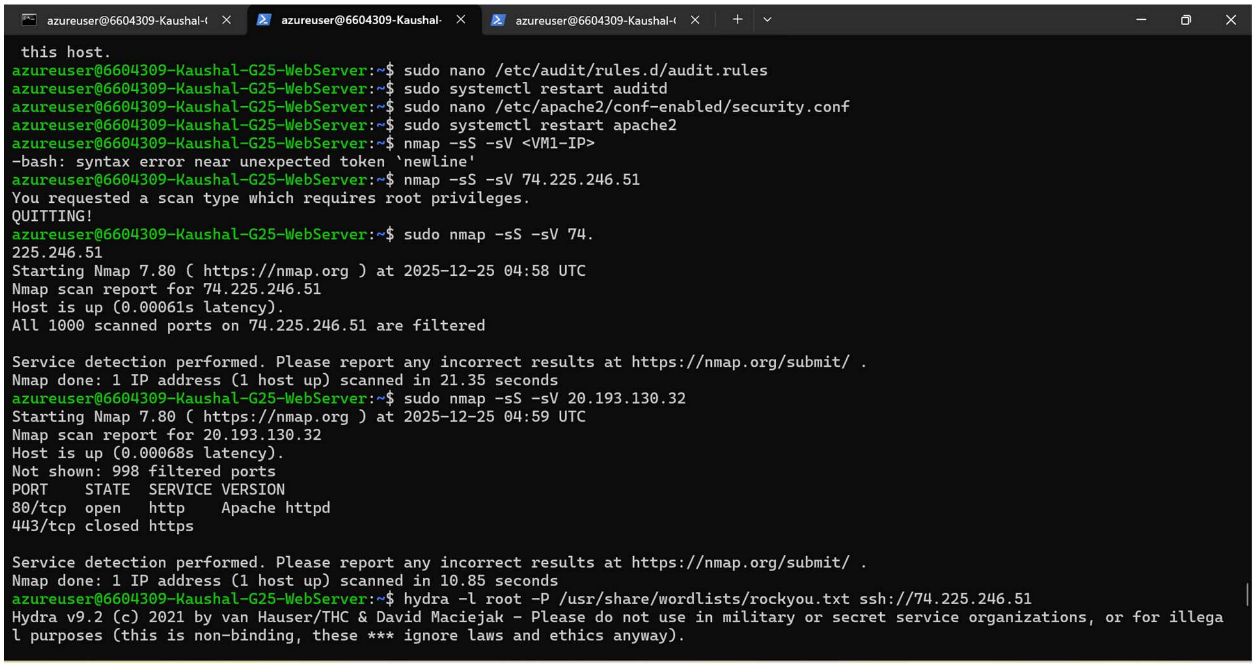
5.1 SSH Hardening

File Edited: `/etc/ssh/sshd_config`

```
Port 2222
PermitRootLogin no
PasswordAuthentication no
MaxAuthTries 3
```

Commands:

```
sudo systemctl restart ssh
sudo sshd -t
```

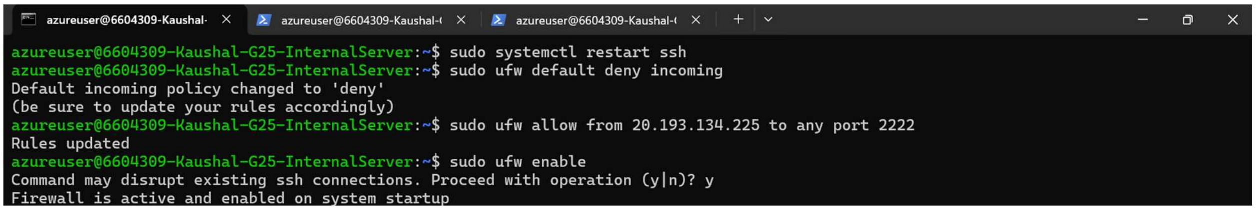


```
 this host.
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nano /etc/audit/rules.d/audit.rules
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo systemctl restart auditd
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nano /etc/apache2/conf-enabled/security.conf
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo systemctl restart apache2
azureuser@6604309-Kaushal-G25-WebServer:~$ nmap -sS -sV <VM1-IP>
-bash: syntax error near unexpected token `newline'
azureuser@6604309-Kaushal-G25-WebServer:~$ nmap -sS -sV 74.225.246.51
You requested a scan type which requires root privileges.
QUITTING!
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nmap -sS -sV 74.
225.246.51
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 04:58 UTC
Nmap scan report for 74.225.246.51
Host is up (0.00061s latency).
All 1000 scanned ports on 74.225.246.51 are filtered

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nmap -sS -sV 20.193.130.32
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 04:59 UTC
Nmap scan report for 20.193.130.32
Host is up (0.00068s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE VERSION
80/tcp  open   http    Apache httpd
443/tcp closed https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.85 seconds
azureuser@6604309-Kaushal-G25-WebServer:~$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://74.225.246.51
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

5.2 Firewall Configuration (UFW)

Commands (VM1):

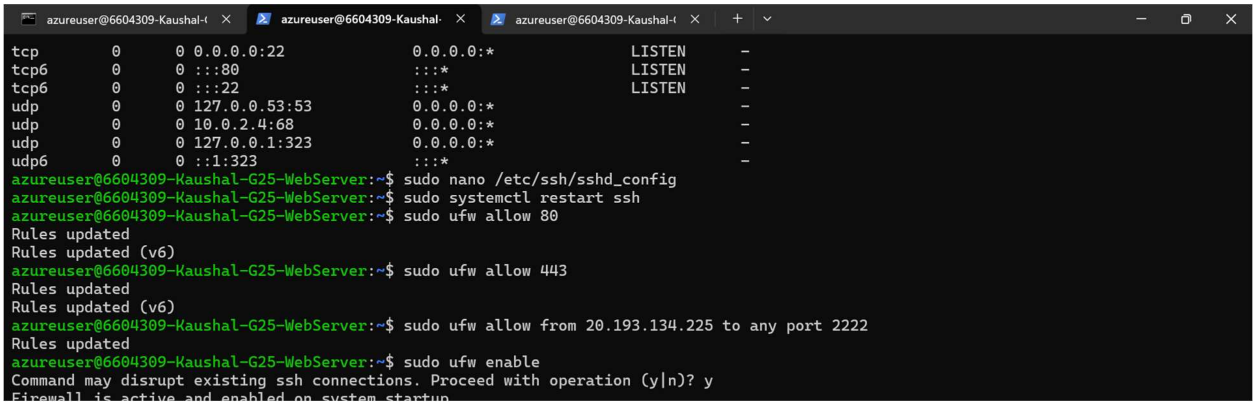
```
sudo ufw default deny incoming
sudo ufw allow from 10.0.1.7 to any port 2222
sudo ufw enable
```


azureuser@6604309-Kaushal-
azureuser@6604309-Kaushal-(
azureuser@6604309-Kaushal-(

```
azureuser@6604309-Kaushal-G25-InternalServer:~$ sudo systemctl restart ssh
azureuser@6604309-Kaushal-G25-InternalServer:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
azureuser@6604309-Kaushal-G25-InternalServer:~$ sudo ufw allow from 20.193.134.225 to any port 2222
Rules updated
azureuser@6604309-Kaushal-G25-InternalServer:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Commands (VM2):

```
sudo ufw allow 80
sudo ufw allow 443
sudo ufw allow from 10.0.1.7 to any port 2222
sudo ufw enable
```


azureuser@6604309-Kaushal-(
azureuser@6604309-Kaushal-
azureuser@6604309-Kaushal-(

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.0.2.4:68             0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp6       0      0 ::1:323                 :::*                                -
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo nano /etc/ssh/sshd_config
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo systemctl restart ssh
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo ufw allow from 20.193.134.225 to any port 2222
Rules updated
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Commands (VM3):

```
sudo ufw allow 1514
sudo ufw allow 55000
sudo ufw enable
```

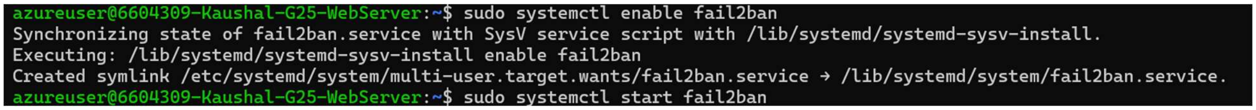
5.3 Apache Hardening

```
ServerTokens Prod
ServerSignature Off
Options -Indexes
```

```
sudo systemctl restart apache2
```

5.4 Fail2Ban

```
sudo apt install fail2ban -y
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```



```
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.
azureuser@6604309-Kaushal-G25-WebServer:~$ sudo systemctl start fail2ban
```

5.5 Audit Logging

```
sudo apt install auditd -y
sudo nano /etc/audit/rules.d/audit.rules
```

Audit rules:

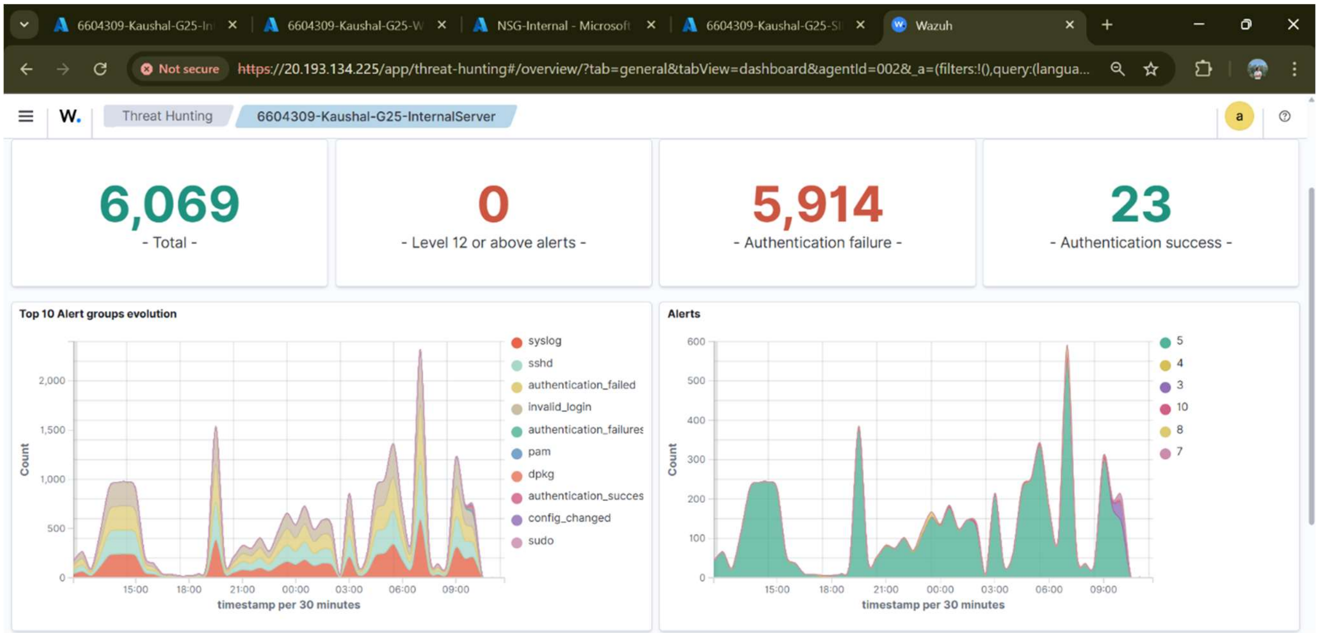
```
-w /etc/passwd -p wa -k passwd_change
-w /var/log/auth.log -p wa -k ssh_log
```

```
sudo systemctl restart auditd
```

6. Re-Attack After Hardening

- Repeat VM2 attacks
- Result: Brute force blocked, scans logged, web attacks monitored

➢ **INTERNAL SERVER DASHBOARD**



https://20.193.134.225/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=002&_a=(filters:!(),query:(langua...

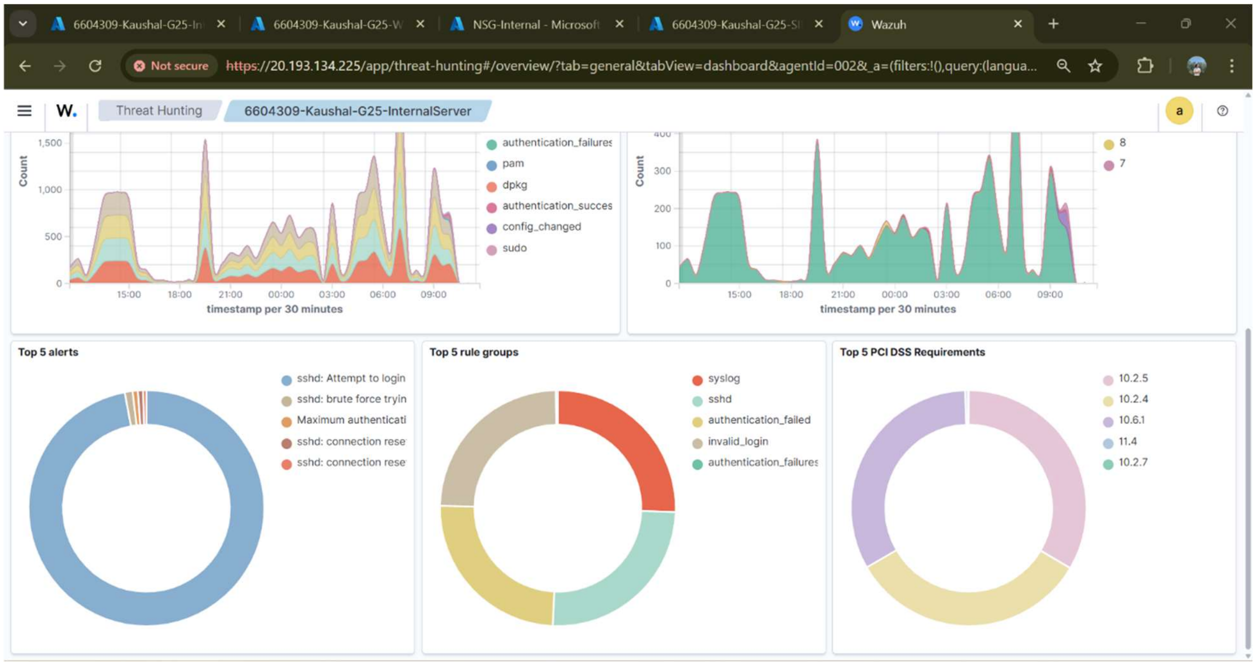
Threat Hunting / 6604309-Kaushal-G25-InternalServer

6,069 - Total -

0 - Level 12 or above alerts -

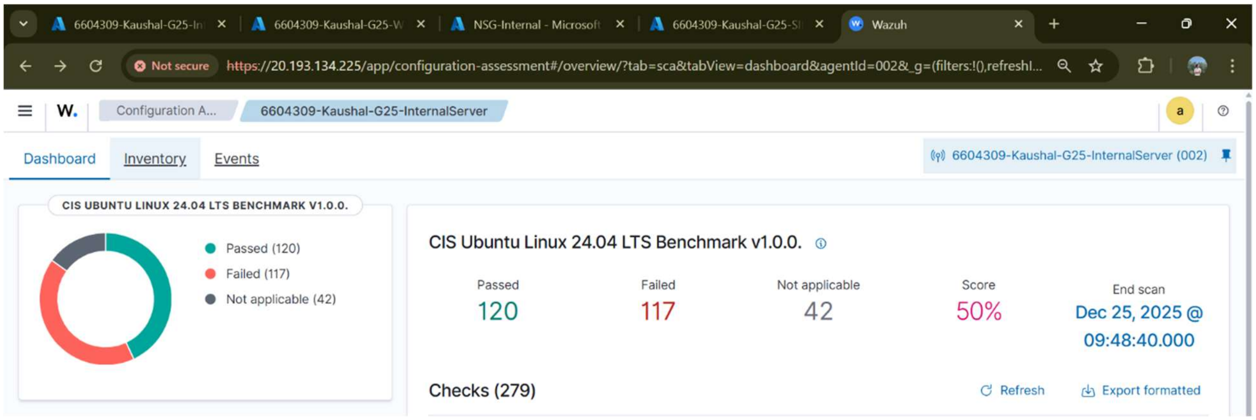
5,914 - Authentication failure -

23 - Authentication success -



https://20.193.134.225/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=002&_a=(filters:!(),query:(langua...

Threat Hunting / 6604309-Kaushal-G25-InternalServer



6604309-Kaushal-G25-In | 6604309-Kaushal-G25-W | NSG-Internal - Microsoft | 6604309-Kaushal-G25-SI | Wazuh

Not secure https://20.193.134.225/app/configuration-assessment#/overview/?tab=sca&tabView=dashboard&agentId=002&_g=(filters:!(),refreshI...

W. Configuration A... 6604309-Kaushal-G25-InternalServer

Dashboard Inventory Events

6604309-Kaushal-G25-InternalServer (002)

CIS UBUNTU LINUX 24.04 LTS BENCHMARK V1.0.0.

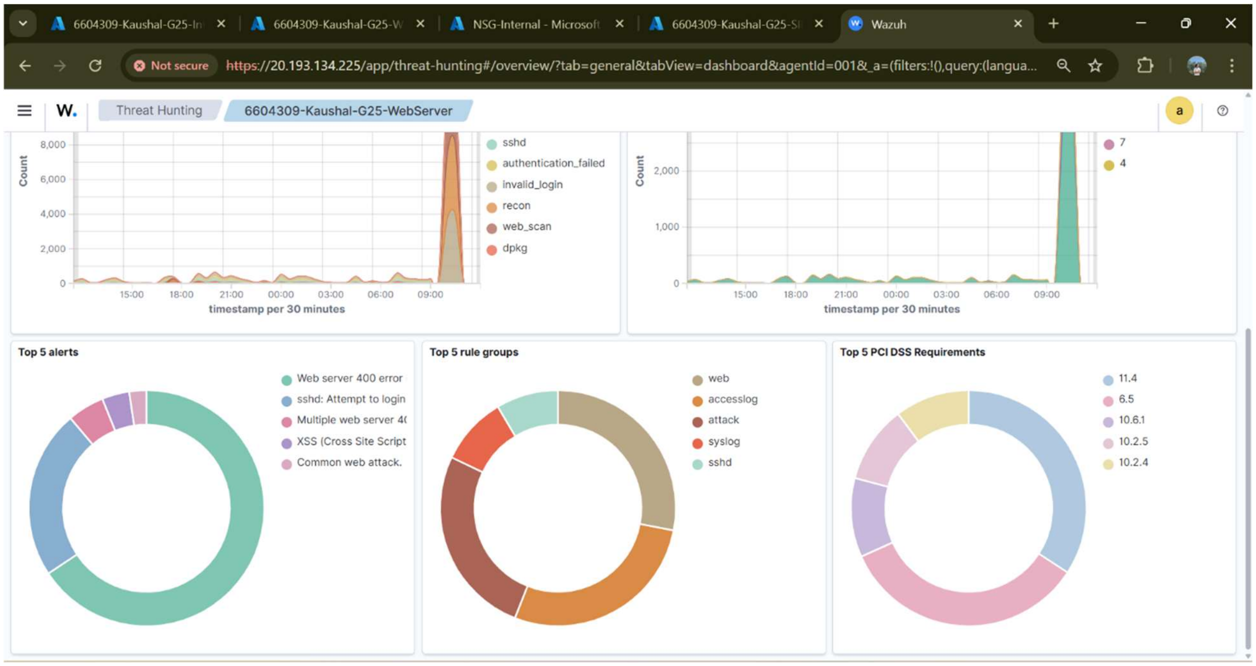
CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.

Passed	Failed	Not applicable	Score	End scan
120	117	42	50%	Dec 25, 2025 @ 09:48:40.000

Checks (279)

Refresh Export formatted

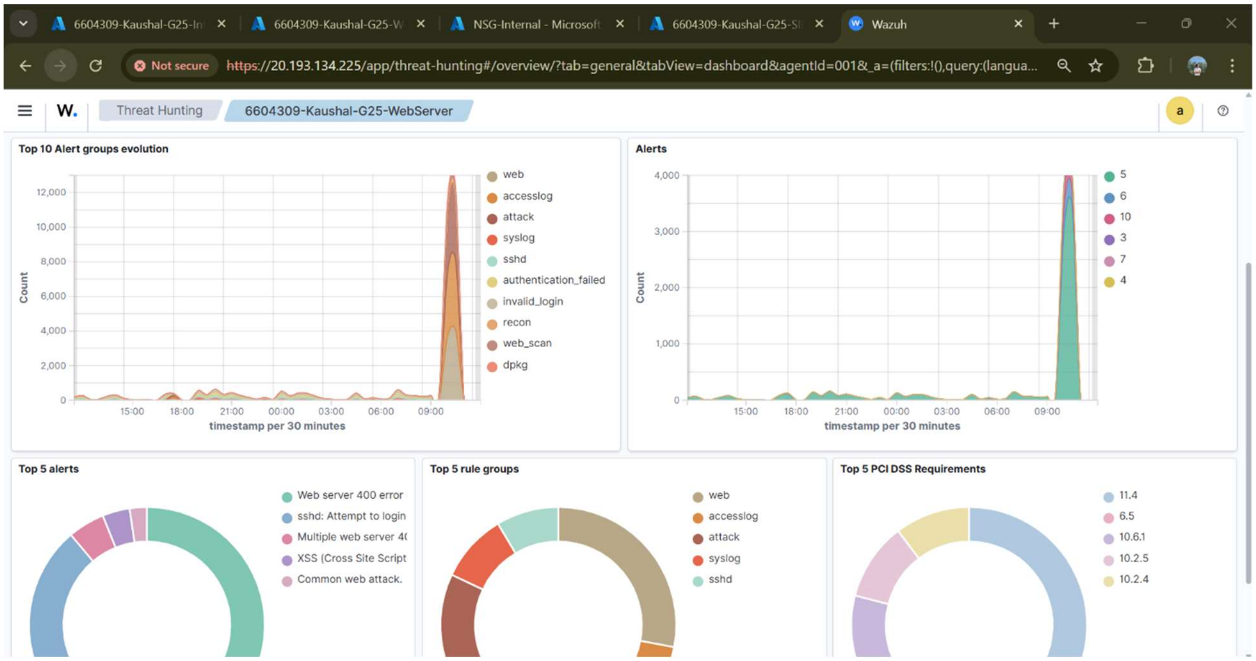
➢ WEBSERVER DASHBOARD

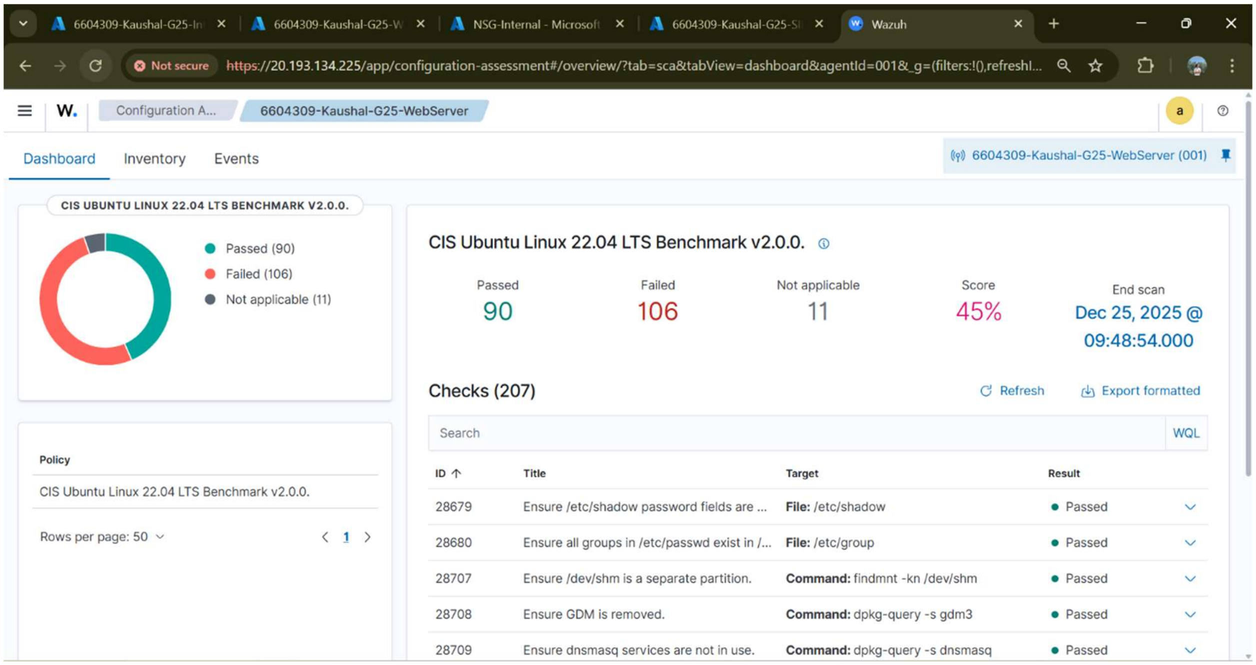


6604309-Kaushal-G25-In | 6604309-Kaushal-G25-W | NSG-Internal - Microsoft | 6604309-Kaushal-G25-SI | Wazuh

Not secure https://20.193.134.225/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=001&_a=(filters:!(),query:(langua...

W. Threat Hunting 6604309-Kaushal-G25-WebServer




6604309-Kaushal-G25-In
6604309-Kaushal-G25-W
NSG-Internal - Microsoft
6604309-Kaushal-G25-S
Wazuh
Not secure
https://20.193.134.225/app/configuration-assessment#/overview/?tab=sca&tabView=dashboard&agentId=001&_g=(filters:!(),refreshl...
W.
Configuration A...
6604309-Kaushal-G25-WebServer
a
Dashboard
Inventory
Events
6604309-Kaushal-G25-WebServer (001)

CIS UBUNTU LINUX 22.04 LTS BENCHMARK V2.0.0.

- Passed (90)
- Failed (106)
- Not applicable (11)

Policy

CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.

Rows per page: 50 ‹ 1 ›

CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.

Passed	Failed	Not applicable	Score	End scan
90	106	11	45%	Dec 25, 2025 @ 09:48:54.000

Checks (207)

Refresh Export formatted

Search WQL

ID ↑	Title	Target	Result
28679	Ensure /etc/shadow password fields are ...	**File:** /etc/shadow	● Passed
28680	Ensure all groups in /etc/passwd exist in /...	**File:** /etc/group	● Passed
28707	Ensure /dev/shm is a separate partition.	**Command:** findmnt -kn /dev/shm	● Passed
28708	Ensure GDM is removed.	**Command:** dpkg-query -s gdm3	● Passed
28709	Ensure dnsmasq services are not in use.	**Command:** dpkg-query -s dnsmasq	● Passed

7. Before vs After Comparison

Attack Type	Before Hardening	After Hardening
SSH Brute Force	Successful login attempts	Blocked / alert triggered
Port Scan	Open ports visible	Firewall blocked, only required ports open
Web Attacks	Apache discloses version	Version hidden, directory listing disabled
Privilege Escalation	Vulnerable SUID binaries	Critical binaries removed / monitored

8. Conclusion

- Simulated attacks on internal infrastructure
- Captured & analyzed all events via Wazuh SIEM
- Hardened SSH, firewall, Apache, and system policies
- Demonstrated Red Team → Blue Team → Hardening workflow

Learning Outcome: - Hands-on Linux server security - SIEM log correlation & monitoring - Applying security best practices