Matrixon Systems - Major Project Report Attack, Detection & Hardening of Enterprise Infrastructure Using SIEM

Student Name: *Charu Jain*
Semester: *5th*
Course: *Ethical Hacking / Cybersecurity*
Date: *25 Dec 2025*

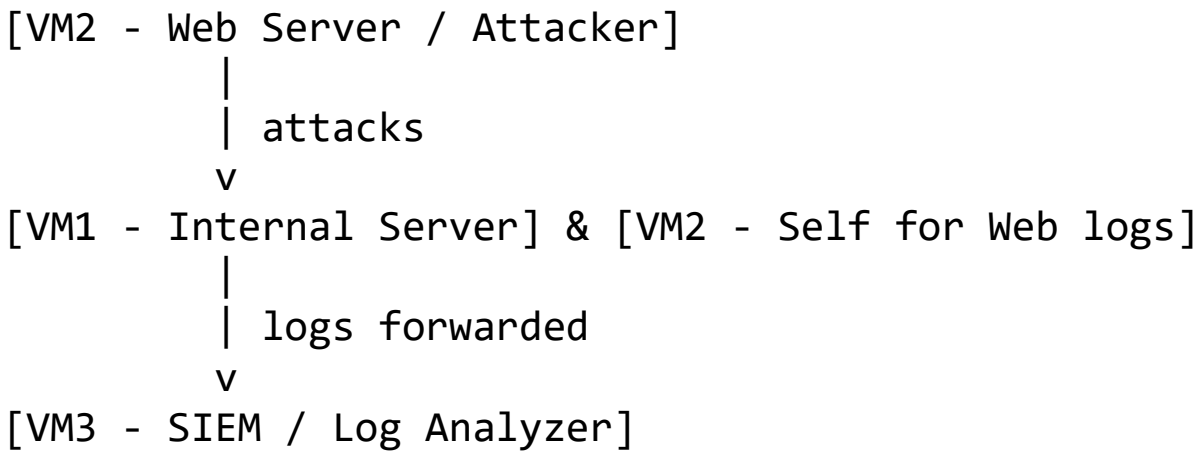
Table of Contents

1. Project Overview

Objective: Simulate real-world cyber attacks, detect events using SIEM, and apply hardening.

Scope: - Red Team attacks on Internal & Web Servers - Log collection & correlation via Wazuh SIEM - System hardening (SSH, Apache, firewall)

Infrastructure Diagram:



2. Environment Setup

VM	Role	IP (Example)	Purpose
VM1	Internal Server	10.0.1.4	Victim / log generator
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-server` - Verify connectivity using `ping`

3. Red Team Simulation (Attacks)

3.1 Port Scanning

Command (VM2):

```
nmap -sS -sV 10.0.1.4
nmap -sS -sV 10.0.1.5
```

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

```
azureuser@web-server:~$ sudo nmap -sS -sV 10.0.1.4
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 05:36 UTC
Nmap scan report for 6604218-charu-g25-internalserver.internal.cloudapp.net
(10.0.1.4)
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protoco
l 2.0)
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 6.36 seconds
azureuser@web-server:~$ sudo nmap -sS -sV 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 05:37 UTC
Nmap scan report for 6604218-charu-g25-webserver.internal.cloudapp.net (10.0
.2.4)
Host is up (0.0000060s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protoco
l 2.0)
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 6.31 seconds
azureuser@web-server:~$
```

Screenshot Placeholder: *Figure 3.1 – Nmap Scan Output*

3.2 SSH Brute Force Attack

Command (VM2):

```
hydra -l root -P /usr/share/wordlists/rockyou.txt
ssh://10.0.1.4
```

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

```
azureuser@6604218-Charm-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@6604218-Charm-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
```

Screenshot Placeholder: *Figure 3.2 – SSH Brute Force Alert*

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@6604218-Charm-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
```

Screenshot Placeholder: *Figure 3.3 – Nikto / Gobuster Results*

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

```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on
 this host.
azureuser@6604218-Charu-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                 :::*                                -
```

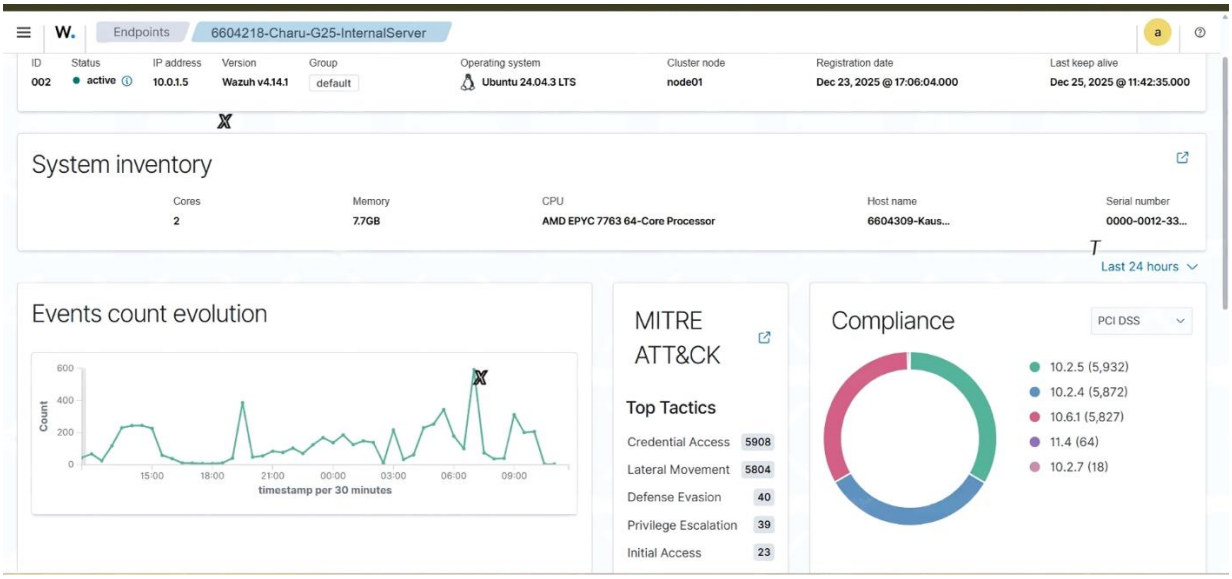
Screenshot Placeholder: *Figure 3.4 – Privilege Escalation Logs*

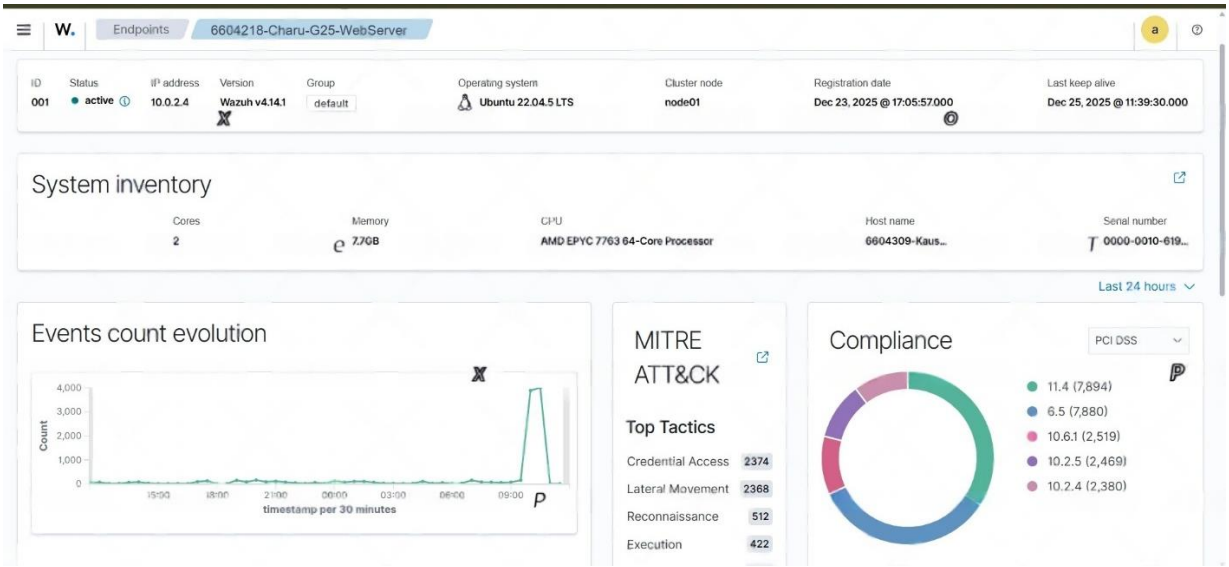
---

4. SIEM Investigation

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

Screenshot Placeholder: *Figure 4.1 – Wazuh Dashboard Alerts*





5. Hardening and Mitigation

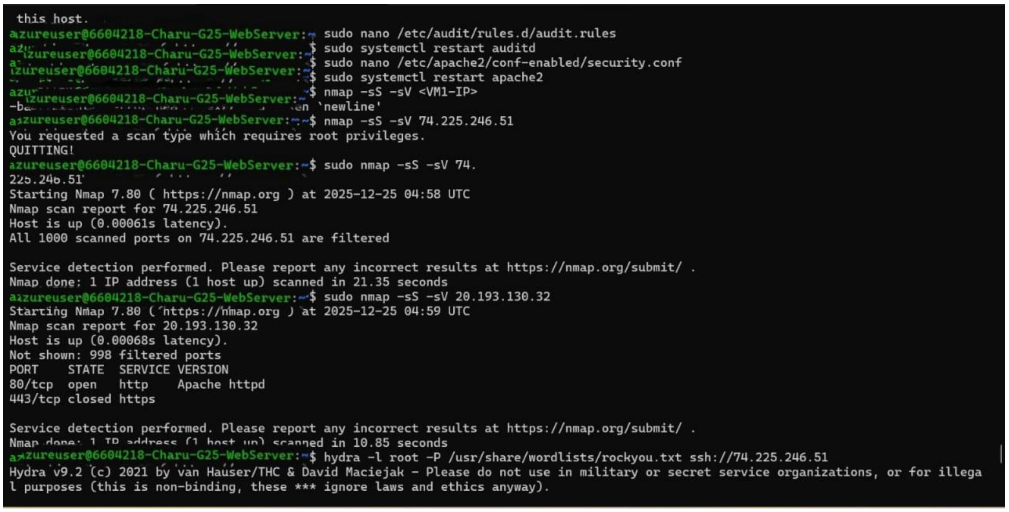
5.1 SSH Hardening

File Edited: `/etc/ssh/sshd_config`

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

Commands:

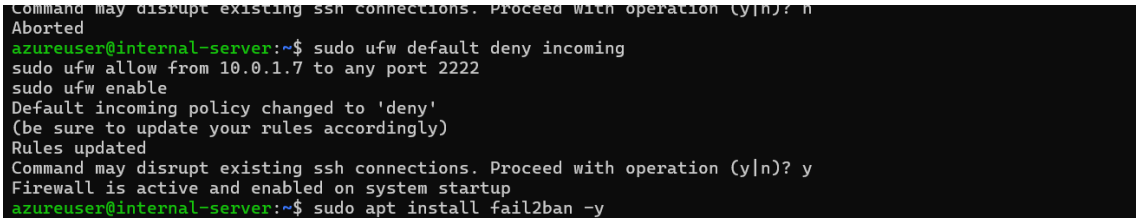
```
sudo systemctl restart ssh
sudo sshd -t
```



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
```



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
```

```
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@6604218-Charu-G25-WebServer:~$ sudo nano /etc/ssh/sshd_config
azureuser@6604218-Charu-G25-WebServer:~$ sudo systemctl restart ssh
azureuser@6604218-Charu-G25-WebServer:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
azureuser@6604218-Charu-G25-WebServer:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
azureuser@6604218-Charu-G25-WebServer:~$ sudo ufw allow from 20.193.134.225 to any port 2222
Rules updated
azureuser@6604218-Charu-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@6604218-Charu-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@6604218-Charu-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
```

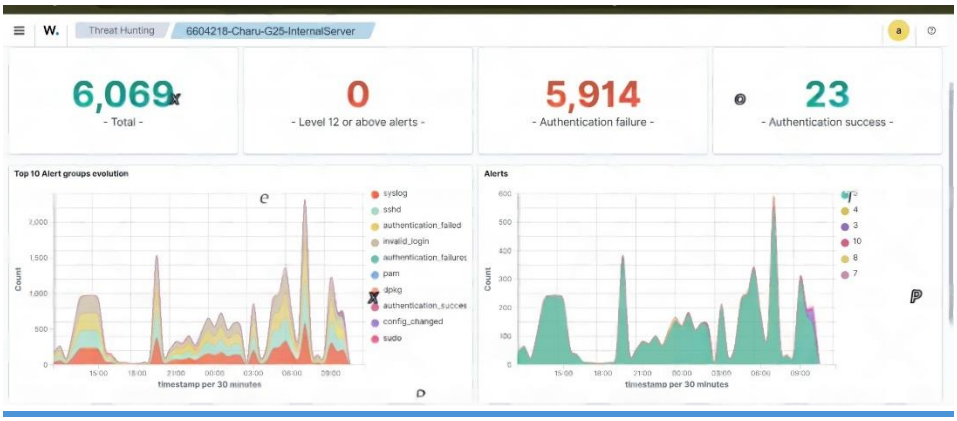
```
sudo systemctl restart auditd
```

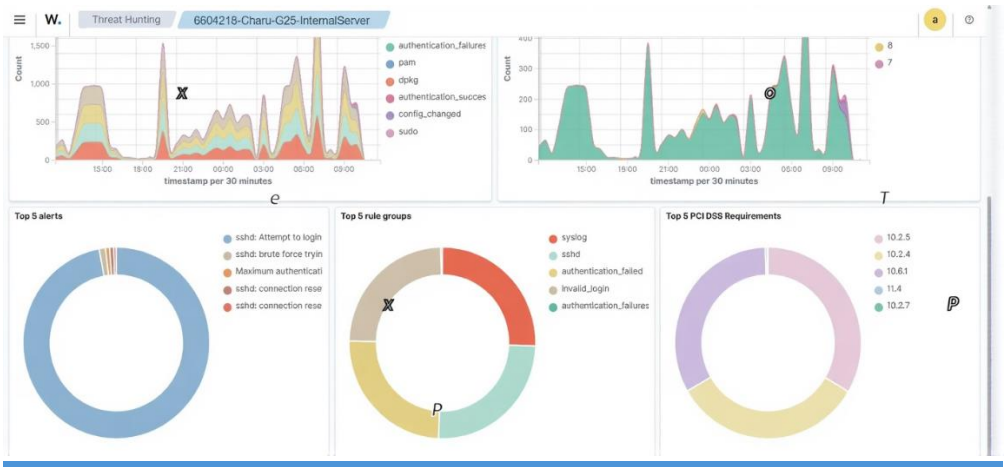
---

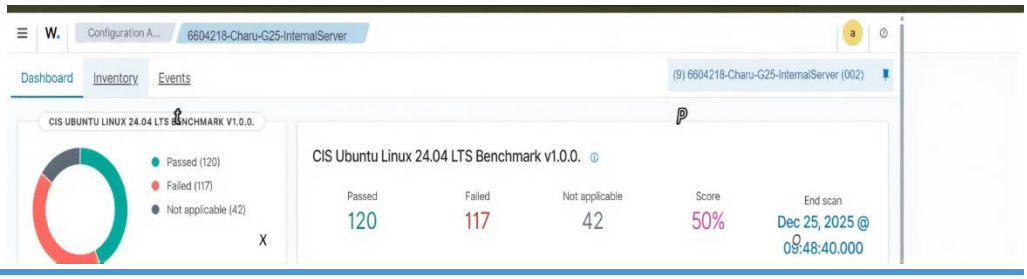
6. Re-Attack After Hardening

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

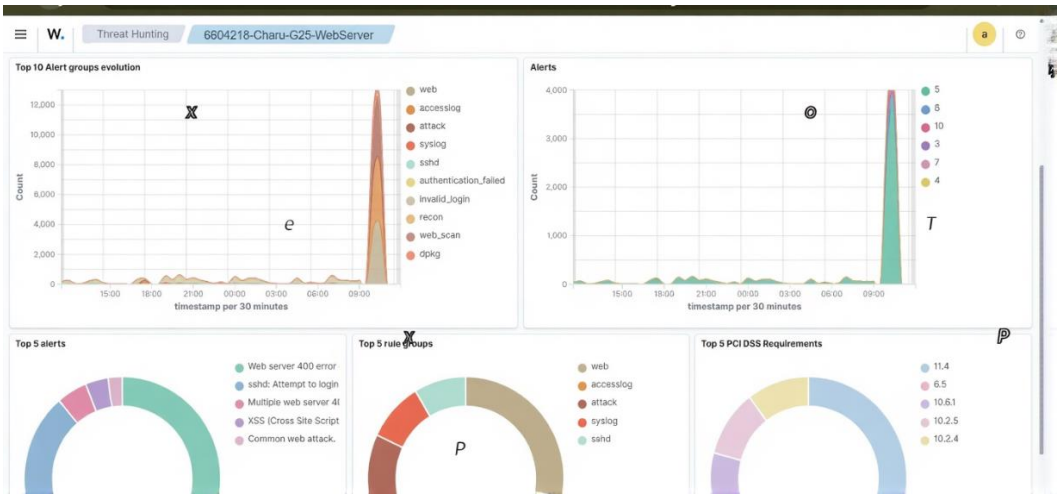
- **Internal Server DashBoard:--**

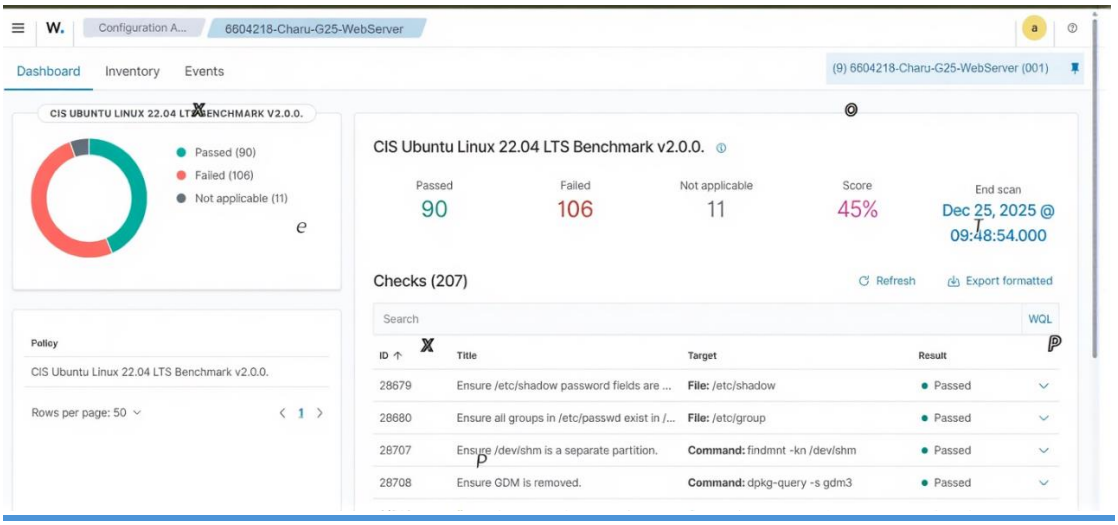






- **Web Server DashBoard:--**


Threat Hunting
6604218-Charu-G25-WebServer
Top 10 Alert groups evolution
Count
timestamp per 30 minutes
web
accesslog
attack
syslog
sshd
authentication_failed
invalid_login
recon
web_scan
dpkg
Alerts
Count
timestamp per 30 minutes
Top 5 alerts
Web server 400 error
sshd: Attempt to login
Multiple web server 4(
XSS (Cross Site Script
Common web attack.
Top 5 rule groups
web
accesslog
attack
syslog
sshd
Top 5 PCI DSS Requirements
11.4
6.5
10.6.1
10.2.5
10.2.4


Configuration A...
6604218-Charu-G25-WebServer
Dashboard
Inventory
Events
(9) 6604218-Charu-G25-WebServer (001)
CIS UBUNTU LINUX 22.04 LTS BENCHMARK V2.0.0.
Passed (90)
Failed (106)
Not applicable (11)
CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.
Passed
90
Failed
106
Not applicable
11
Score
45%
End scan
Dec 25, 2025 @ 09:48:54.000
Checks (207)
Refresh
Export formatted
Search
WQL
Policy
CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.
Rows per page: 50
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

Screenshot Placeholder: *Figure 6.1 – SIEM Dashboard Post-Hardening*

---

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

---