

Cryvion - Major Project Report

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

Table of Contents

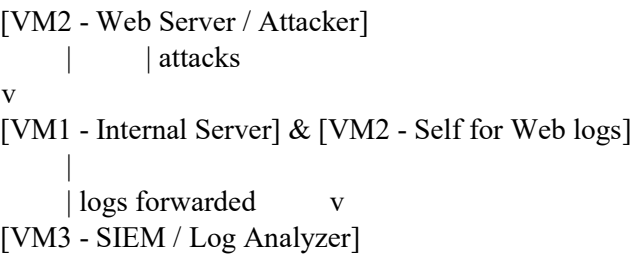
- 1. Project Overview
- 2. Environment Setup
- 3. Red Team Simulation (Attacks) o 3.1 Port Scanning o 3.2 SSH Brute Force Attack o 3.3 Web Attacks o 3.4 Privilege Escalation & Enumeration
- 4. SIEM Investigation
- 5. Hardening and Mitigation o 5.1 SSH Hardening o 5.2 Firewall Configuration (UFW) o 5.3 Apache Hardening o 5.4 Fail2Ban o 5.5 Audit Logging
- 6. Re-Attack After Hardening
- 7. Before vs After Comparison
- 8. Conclusion

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:



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@VM-SIEM:~$ sudo nmap -sS -sV -A 10.0.0.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 23:31 UTC
Nmap scan report for vm-web.internal.cloudapp.net (10.0.0.5)
Host is up (0.00092s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx/1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Welcome to nginx!
MAC Address: 12:34:56:78:9A:BC (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/25%OT=22%CT=1%CU=41666%PV=Y%DS=1%DC=D%G=Y%M=123456%
OS:TM=694DC9477P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=104%TI=Z%CI=Z%II=
OS:I%TS=A)SEQ(SP=102%GCD=1%ISR=104%TI=Z%CI=Z%TS=A)OPS(O1=M582ST11NW7%O2=M58
OS:2ST11NW7%O3=M582NNT11NW7%O4=M582ST11NW7%O5=M582ST11NW7%O6=M582ST11)WIN(W
OS:1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%
OS:0=M582NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=
OS:N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A
OS:=S+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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@VM-SIEM:~$ hydra -l root -P passwords.txt ssh://10.0.0.5
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-26 00:06:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking ssh://10.0.0.5:22/
1 of 1 target completed, 0 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-26 00:06:50
```

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@VM-SIEM:~$ nikto -h http://10.0.0.5
- Nikto v2.1.5
-----
+ Target IP:      10.0.0.5
+ Target Hostname: vm-web.internal.cloudapp.net
+ Target Port:    80
+ Start Time:     2025-12-25 23:48:15 (GMT0)
-----
+ Server: nginx/1.18.0 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x694dace0 0x264
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 6544 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time:      2025-12-25 23:48:23 (GMT0) (8 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

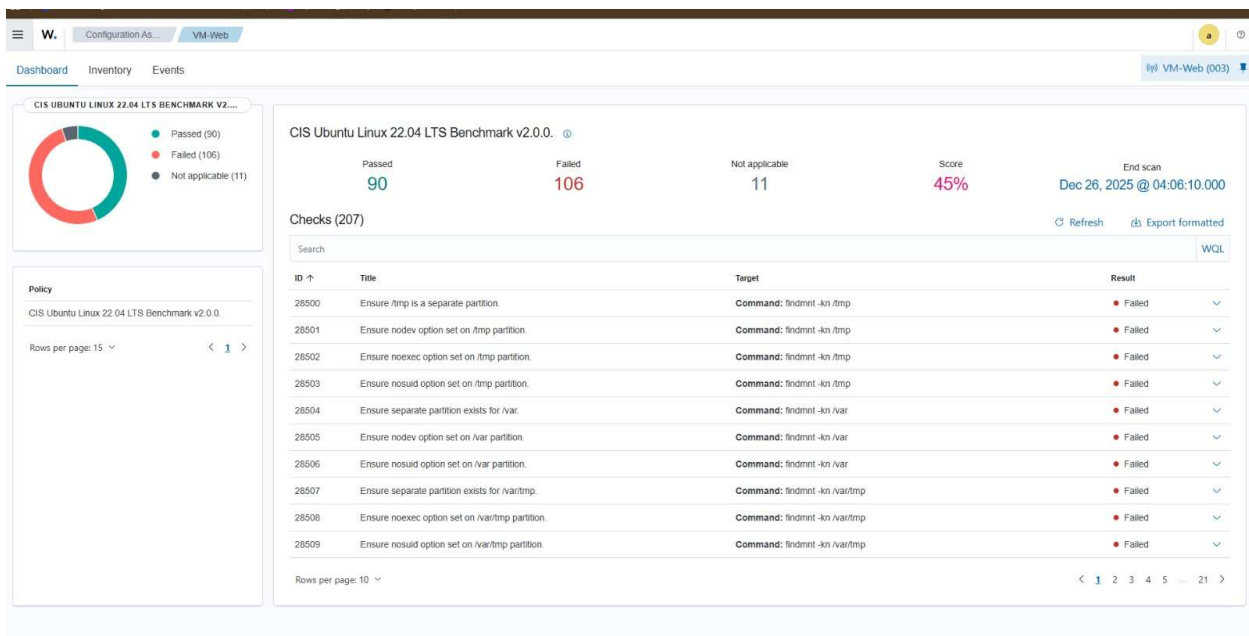
```

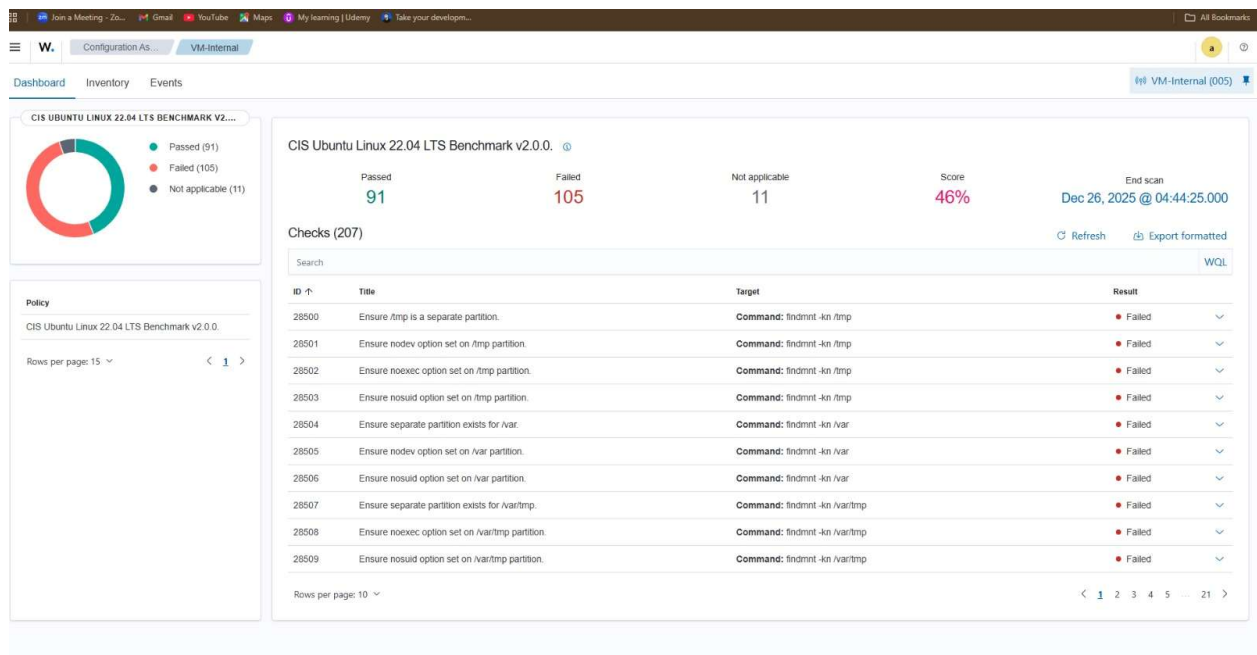
azureuser@VM-SIEM:~$ sudo netstat -tulnp | grep -E '80|443'
tcp        0      0 0.0.0.0:443          0.0.0.0:*           LISTEN     52285/node
tcp        0      0 0.0.0.0:1515         0.0.0.0:*           LISTEN     113807/wazuh-authd

```

4. SIEM Investigation

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





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`

```
azureuser@VM-SIEM:~$ nmap -A 10.0.0.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 23:53 UTC
Nmap scan report for vm-web.internal.cloudapp.net (10.0.0.5)
Host is up (0.0046s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Welcome to nginx!
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 6.57 seconds
azureuser@VM-SIEM:~$ nmap -A 10.0.0.6
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-25 23:53 UTC
Nmap scan report for vm-internal.internal.cloudapp.net (10.0.0.6)
Host is up (0.00080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
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 0.42 seconds
```

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@VM-SIEM:~$ sudo systemctl restart ssh
azureuser@VM-SIEM:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
azureuser@VM-SIEM:~$ sudo ufw allow from 10.0.0.6 to any port 2222
Rules updated
azureuser@VM-SIEM:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
azureuser@VM-SIEM:~$ |
```

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`

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@VM-SIEM:~$ sudo systemctl enable fail2ban sudo systemctl start fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install 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
Failed to enable unit: Unit file /etc/systemd/system/sudo.service is masked.
azureuser@VM-SIEM:~$ 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@VM-SIEM:~$ sudo systemctl start fail2ban
azureuser@VM-SIEM:~$ |
```

5.5 Audit Logging

`sudo apt install auditd -y` `sudo nano`

`/etc/audit/rules.d/audit.rules`

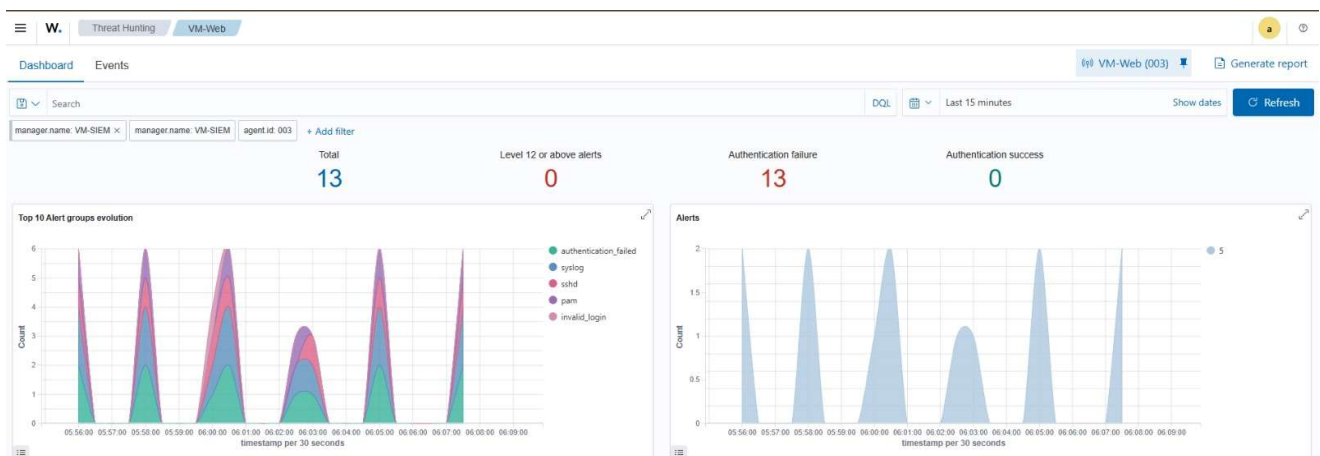
Audit rules:

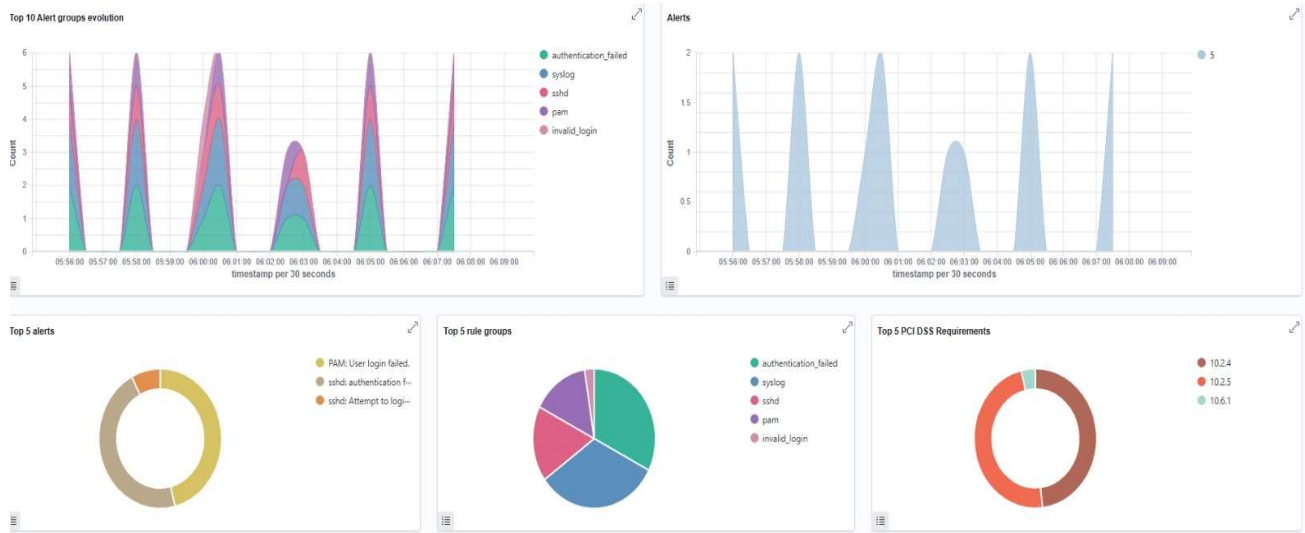
```
-w /etc/passwd -p wa -k passwd_change -w  
/var/log/auth.log -p wa -k ssh_log sudo systemctl  
restart auditd
```

6. Re-Attack After Hardening

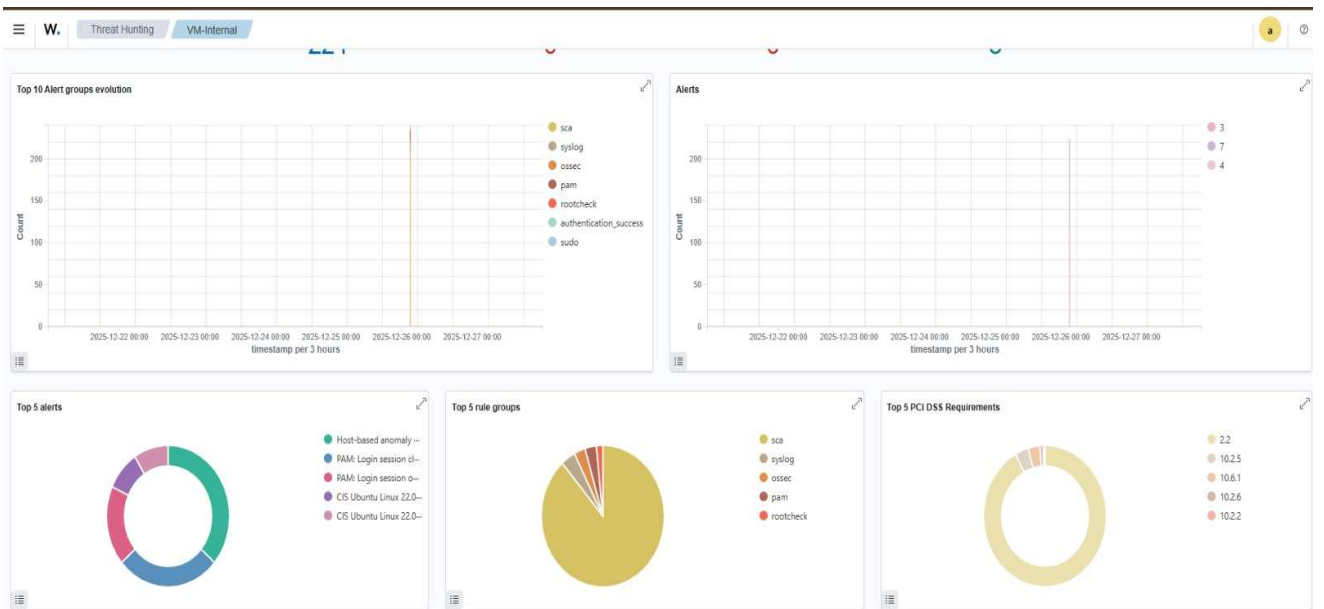
- Repeat VM2 attacks
- Result: Brute force blocked, scans logged, web attacks monitored

☐ INTERNAL SERVER DASHBOARD





□ WEBSERVER DASHBOARD



W. Configuration As... VM-Web

Dashboard Inventory Events

VM-Web (003)

CIS UBTU LINUX 22.04 LTS BENCHMARK V2...

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

CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.

Rows per page: 15

CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.

Passed 90
Failed 106
Not applicable 11
Score 45%
End scan Dec 26, 2025 @ 04:06:10.000

Checks (207)

Refresh Export formatted

| ID | Title | Target | Result |
|-------|---|-------------------------------|--------|
| 28500 | Ensure /tmp is a separate partition. | Command: findmnt -kn /tmp | Failed |
| 28501 | Ensure nodev option set on /tmp partition. | Command: findmnt -kn /tmp | Failed |
| 28502 | Ensure noexec option set on /tmp partition. | Command: findmnt -kn /tmp | Failed |
| 28503 | Ensure nosuid option set on /tmp partition. | Command: findmnt -kn /tmp | Failed |
| 28504 | Ensure separate partition exists for /var. | Command: findmnt -kn /var | Failed |
| 28505 | Ensure nodev option set on /var partition. | Command: findmnt -kn /var | Failed |
| 28506 | Ensure nosuid option set on /var partition. | Command: findmnt -kn /var | Failed |
| 28507 | Ensure separate partition exists for /var/tmp. | Command: findmnt -kn /var/tmp | Failed |
| 28508 | Ensure noexec option set on /var/tmp partition. | Command: findmnt -kn /var/tmp | Failed |
| 28509 | Ensure nosuid option set on /var/tmp partition. | Command: findmnt -kn /var/tmp | Failed |

Rows per page: 10

< 1 2 3 4 5 ... 21 >

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
