EchoSphereNetworks

Title: Attack, Detection & Hardening of Enterprise Infrastructure Using SIEM
Student Name: Subodh pun
Semester: 5th
Semester: 6604306
Course: Certified Ethical Hacking
Date: 25 Dec 2025

1. Project Overview

Objective

To simulate real-world cyberattacks, detect and analyze security events using a SIEM solution, and implement appropriate system hardening measures to improve overall system security.

Scope

- **Conducting red team–style attacks against internal and web servers**
- **Collecting, centralizing, and correlating security logs using the Wazuh SIEM platform**
- **Detecting and analyzing security events and alerts generated during attacks**
- **Implementing system hardening measures, including secure configurations for SSH, Apache web server, and firewall rules**

.

Infrastructure Diagram:

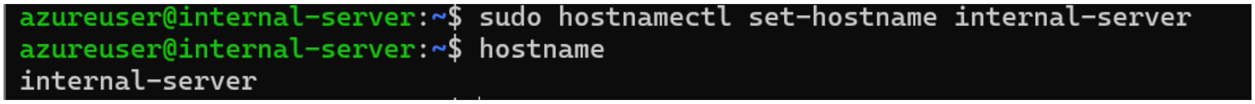
```
[VM2 - Web Server / Attacker]
            |
            | attacks
            v
[VM1 - Internal Server] & [VM2 - Self for Web logs]
            |
            | logs forwarded
            v
[VM3 - SIEM / Log Analyzer]
```

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

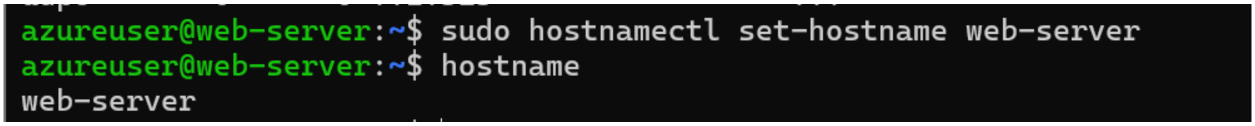
Preparatory Steps: - Update all VMs: `sudo apt update && sudo apt upgrade -y` - Set hostnames: VM1 → `internal-server`, VM2 → `web-server`, VM3 → `siem`

1.Setting host name from 6604306-Subodh-G26-InternalServer to internal-server



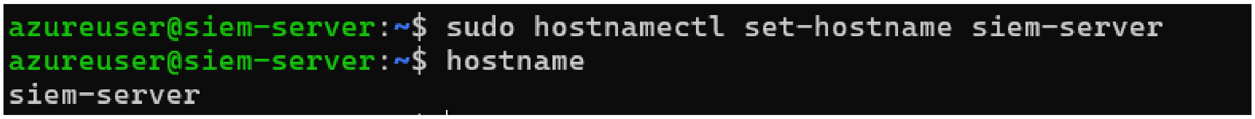
```
azureuser@internal-server:~$ sudo hostnamectl set-hostname internal-server
azureuser@internal-server:~$ hostname
internal-server
```

2.Setting host name from 6604306-Subodh-G26-WebServer to web-server



```
azureuser@web-server:~$ sudo hostnamectl set-hostname web-server
azureuser@web-server:~$ hostname
web-server
```

3.Setting host name from 6604306-Subodh-G26-SIEMServer to siem-server



```
azureuser@siem-server:~$ sudo hostnamectl set-hostname siem-server
azureuser@siem-server:~$ hostname
siem-server
```

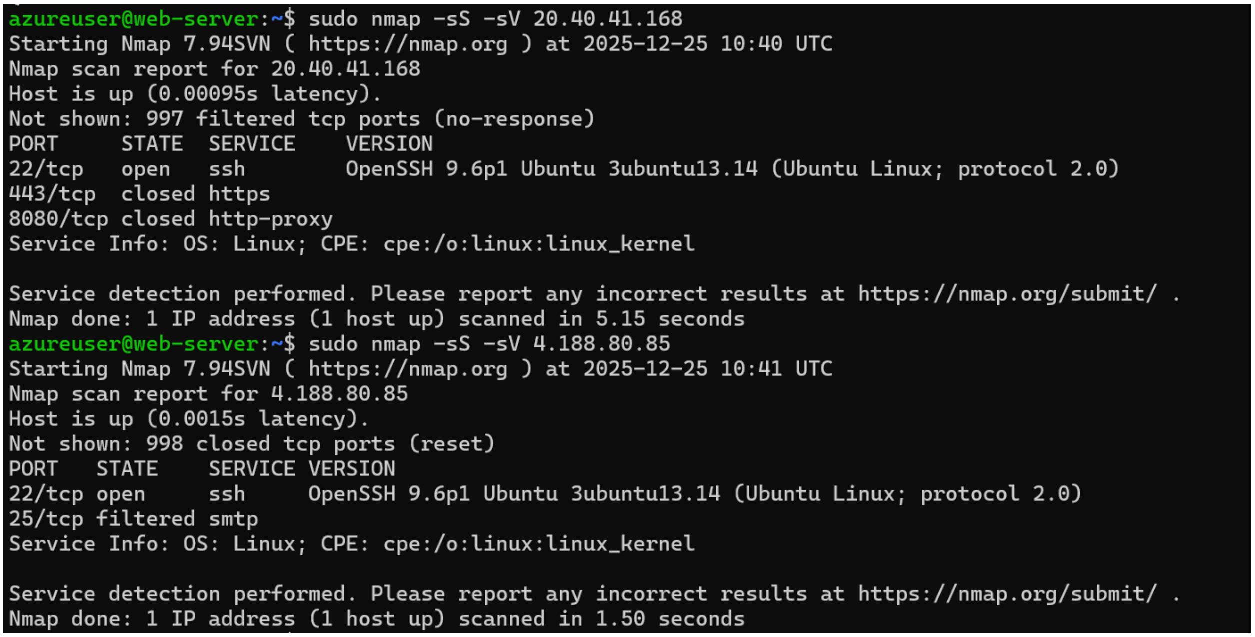
3. Red Team Simulation (Attacks)

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@web-server:~$ sudo nmap -sS -sV 20.40.41.168
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-25 10:40 UTC
Nmap scan report for 20.40.41.168
Host is up (0.00095s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
443/tcp  closed https
8080/tcp closed http-proxy
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 5.15 seconds
azureuser@web-server:~$ sudo nmap -sS -sV 4.188.80.85
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-25 10:41 UTC
Nmap scan report for 4.188.80.85
Host is up (0.0015s latency).
Not shown: 998 closed tcp ports (reset)
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 1.50 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)

3.3 Web Attacks

Commands (VM2):

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

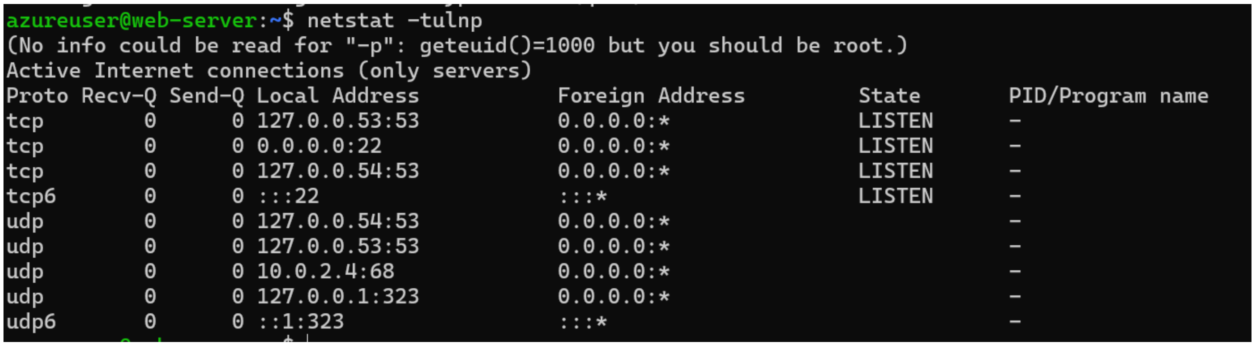
Logs: `/var/log/apache2/access.log` & `/var/log/apache2/error.log` (VM2), Wazuh alerts (VM3)

3.4 Privilege Escalation & Enumeration

Commands:

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

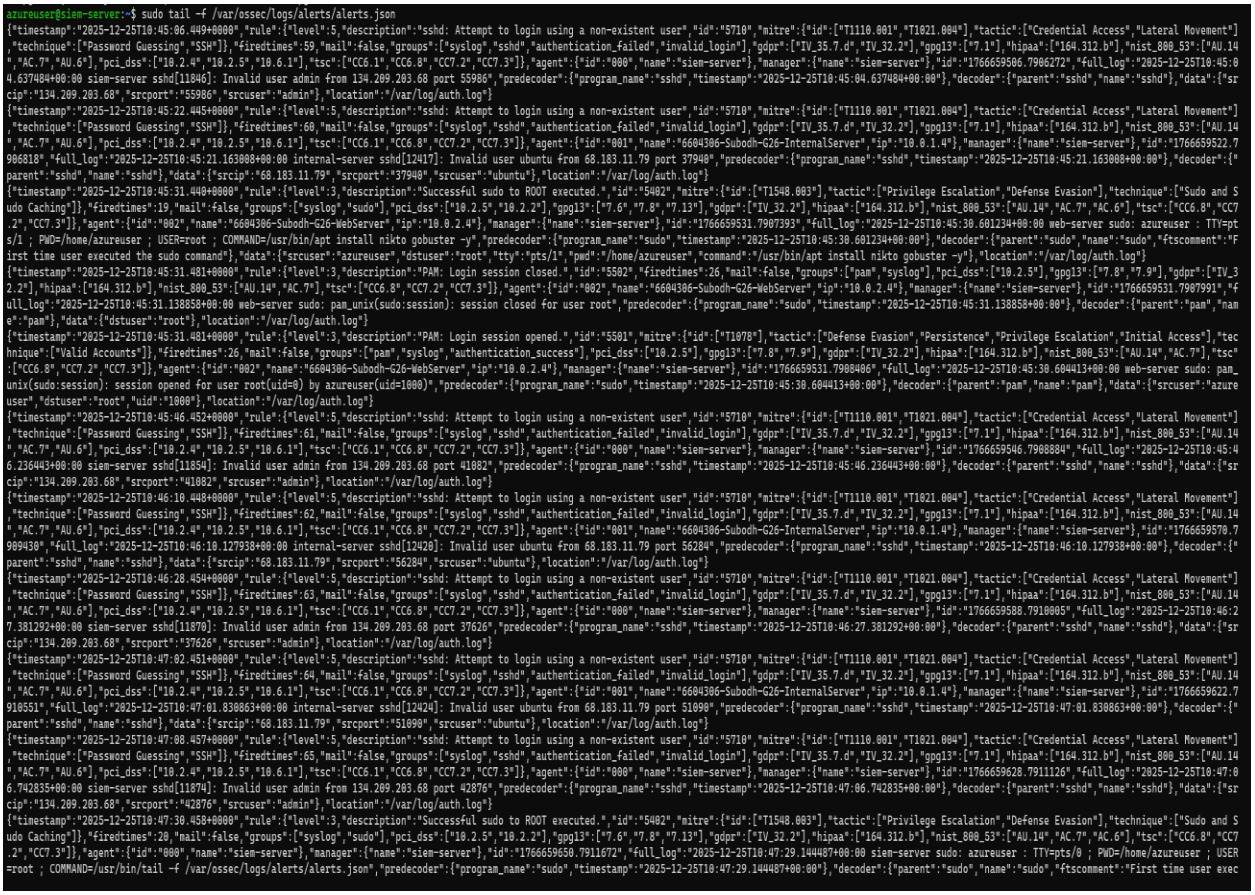
Logs: Forwarded to SIEM for monitoring



```
azureuser@web-server:~$ netstat -tulnp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
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      -
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.54:53           0.0.0.0:*                           -
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



```
azureuser@siem-server:~$ sudo tail -f /var/ossec/logs/alerts/alerts.json
{"timestamp":"2025-12-25T10:45:06.449+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":59,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659506.7906272","full_log":"2025-12-25T10:45:0
4.637484+00:00 siem-server sshd[11846]: Invalid user admin from 134.209.203.68 port 55986","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:45:04.637484+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"55986","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:22.445+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":60,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"6604306-Subodh-G26-InternalServer","ip":"10.0.1.4"},"manager":{"name":"siem-server"},"id":"1766659522.7
906818","full_log":"2025-12-25T10:45:21.163008+00:00 internal-server sshd[12417]: Invalid user ubuntu from 68.183.11.79 port 37940","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:45:21.163008+00:00"},"decoder":{"
parent":"sshd","name":"sshd"},"data":{"srcip":"68.183.11.79","srcport":"37940","srcuser":"ubuntu"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:31.440+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic":["Privilege Escalation","Defense Evasion"],"technique":["Sudo and S
udo Caching"]},"firedtimes":19,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","10.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7
.2","CC7.3"]},"agent":{"id":"002","name":"6604306-Subodh-G26-WebServer","ip":"10.0.2.4"},"manager":{"name":"siem-server"},"id":"1766659531.7907393","full_log":"2025-12-25T10:45:30.601234+00:00 web-server sudo: azureuser : TTY=pt
s/1 ; PWD=/home/azureuser ; USER=root ; COMMAND=/usr/bin/apt install nikto gobuster -y","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:45:30.601234+00:00"},"decoder":{"parent":"sudo","name":"sudo","ftscomment":"F
irst time user executed the sudo command"},"data":{"srcuser":"azureuser","dstuser":"root","tty":"pts/1","pwd":"/home/azureuser","command":"/usr/bin/apt install nikto gobuster -y"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:31.481+0000","rule":{"level":3,"description":"PAM: Login session closed.","id":"5502","firedtimes":26,"mail":false,"groups":["pam","syslog"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_3
2.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"002","name":"6604306-Subodh-G26-WebServer","ip":"10.0.2.4"},"manager":{"name":"siem-server"},"id":"1766659531.7907991","f
ull_log":"2025-12-25T10:45:31.138858+00:00 web-server sudo: pam_unix(sudo:session): session closed for user root","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:45:31.138858+00:00"},"decoder":{"parent":"pam","nam
e":"pam"},"data":{"dstuser":"root"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:31.481+0000","rule":{"level":3,"description":"PAM: Login session opened.","id":"5501","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"tec
hnique":["Valid Accounts"]},"firedtimes":26,"mail":false,"groups":["pam","syslog","authentication_success"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc"
:["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"002","name":"6604306-Subodh-G26-WebServer","ip":"10.0.2.4"},"manager":{"name":"siem-server"},"id":"1766659531.7908406","full_log":"2025-12-25T10:45:30.604413+00:00 web-server sudo: pam_
unix(sudo:session): session opened for user root(uid=0) by azureuser(uid=1000)","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:45:30.604413+00:00"},"decoder":{"parent":"pam","name":"pam"},"data":{"srcuser":"azure
user","dstuser":"root","uid":"1000"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:46.452+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":61,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659546.7908884","full_log":"2025-12-25T10:45:4
6.236443+00:00 siem-server sshd[11854]: Invalid user admin from 134.209.203.68 port 41082","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:45:46.236443+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"41082","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:46:10.448+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":62,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"6604306-Subodh-G26-InternalServer","ip":"10.0.1.4"},"manager":{"name":"siem-server"},"id":"1766659570.7
909430","full_log":"2025-12-25T10:46:10.127938+00:00 internal-server sshd[12420]: Invalid user ubuntu from 68.183.11.79 port 56284","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:46:10.127938+00:00"},"decoder":{"
parent":"sshd","name":"sshd"},"data":{"srcip":"68.183.11.79","srcport":"56284","srcuser":"ubuntu"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:46:28.454+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":63,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659588.7910005","full_log":"2025-12-25T10:46:2
7.381292+00:00 siem-server sshd[11870]: Invalid user admin from 134.209.203.68 port 37626","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:46:27.381292+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"37626","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:47:02.451+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":64,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"6604306-Subodh-G26-InternalServer","ip":"10.0.1.4"},"manager":{"name":"siem-server"},"id":"1766659622.7
910551","full_log":"2025-12-25T10:47:01.830863+00:00 internal-server sshd[12424]: Invalid user ubuntu from 68.183.11.79 port 51090","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:47:01.830863+00:00"},"decoder":{"
parent":"sshd","name":"sshd"},"data":{"srcip":"68.183.11.79","srcport":"51090","srcuser":"ubuntu"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:47:08.457+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":65,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659628.7911126","full_log":"2025-12-25T10:47:0
6.742835+00:00 siem-server sshd[11874]: Invalid user admin from 134.209.203.68 port 42876","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:47:06.742835+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"42876","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:47:30.458+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic":["Privilege Escalation","Defense Evasion"],"technique":["Sudo and S
udo Caching"]},"firedtimes":20,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","10.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7
.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659650.7911672","full_log":"2025-12-25T10:47:29.144487+00:00 siem-server sudo: azureuser : TTY=pts/0 ; PWD=/home/azureuser ; USER
=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.json","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:47:29.144487+00:00"},"decoder":{"parent":"sudo","name":"sudo","ftscomment":"First time user exec
```

5. Hardening and Mitigation

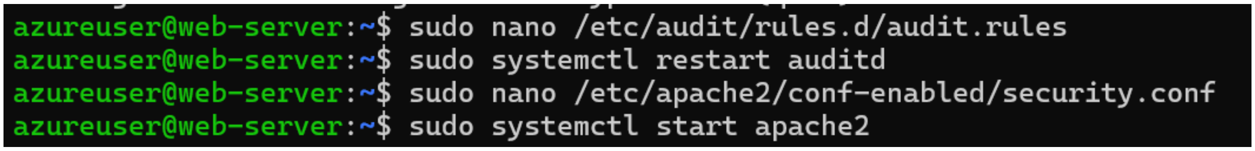
5.1 SSH Hardening

File Edited: `/etc/ssh/sshd_config`

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

Commands:

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

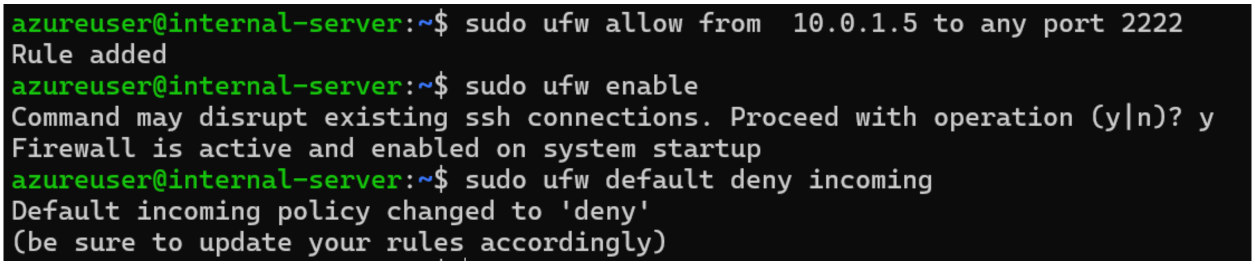


```
azureuser@web-server:~$ sudo nano /etc/audit/rules.d/audit.rules
azureuser@web-server:~$ sudo systemctl restart auditd
azureuser@web-server:~$ sudo nano /etc/apache2/conf-enabled/security.conf
azureuser@web-server:~$ sudo systemctl start apache2
```

5.2 Firewall Configuration (UFW)

Commands (VM1):

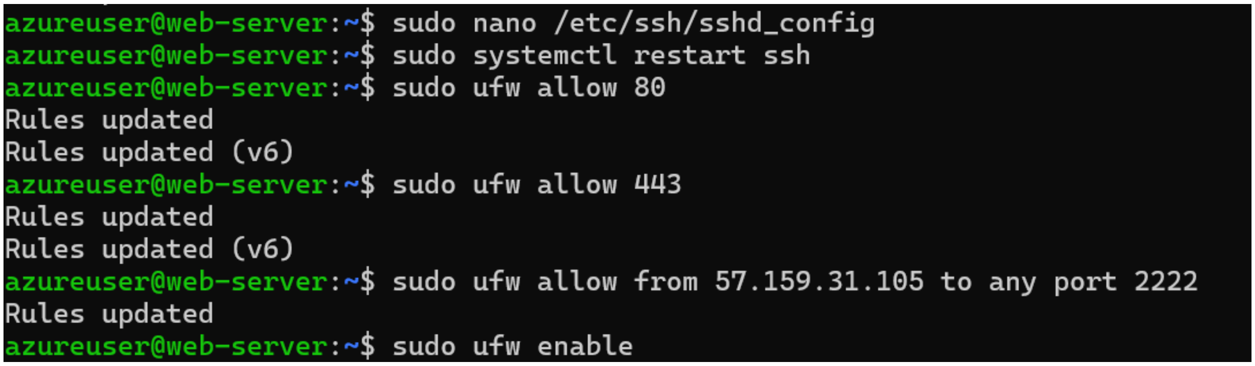
```
sudo ufw default deny incoming
sudo ufw allow from 10.0.1.7 to any port 2222
sudo ufw enable
```



```
azureuser@internal-server:~$ sudo ufw allow from  10.0.1.5 to any port 2222
Rule added
azureuser@internal-server:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
azureuser@internal-server:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

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@web-server:~$ sudo nano /etc/ssh/sshd_config
azureuser@web-server:~$ sudo systemctl restart ssh
azureuser@web-server:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
azureuser@web-server:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
azureuser@web-server:~$ sudo ufw allow from 57.159.31.105 to any port 2222
Rules updated
azureuser@web-server:~$ sudo ufw enable
```

Commands (VM3):

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

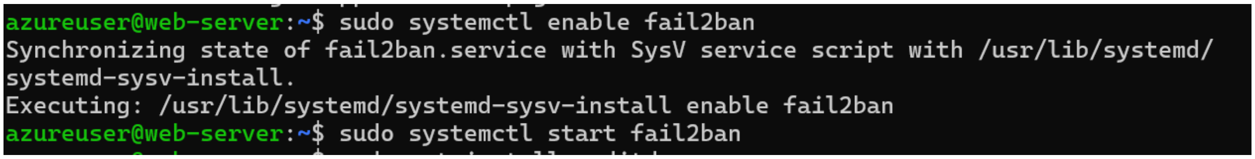
5.3 Apache Hardening

```
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@web-server:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/
systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
azureuser@web-server:~$ sudo systemctl start fail2ban
```

5.5 Audit Logging

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

Audit rules:

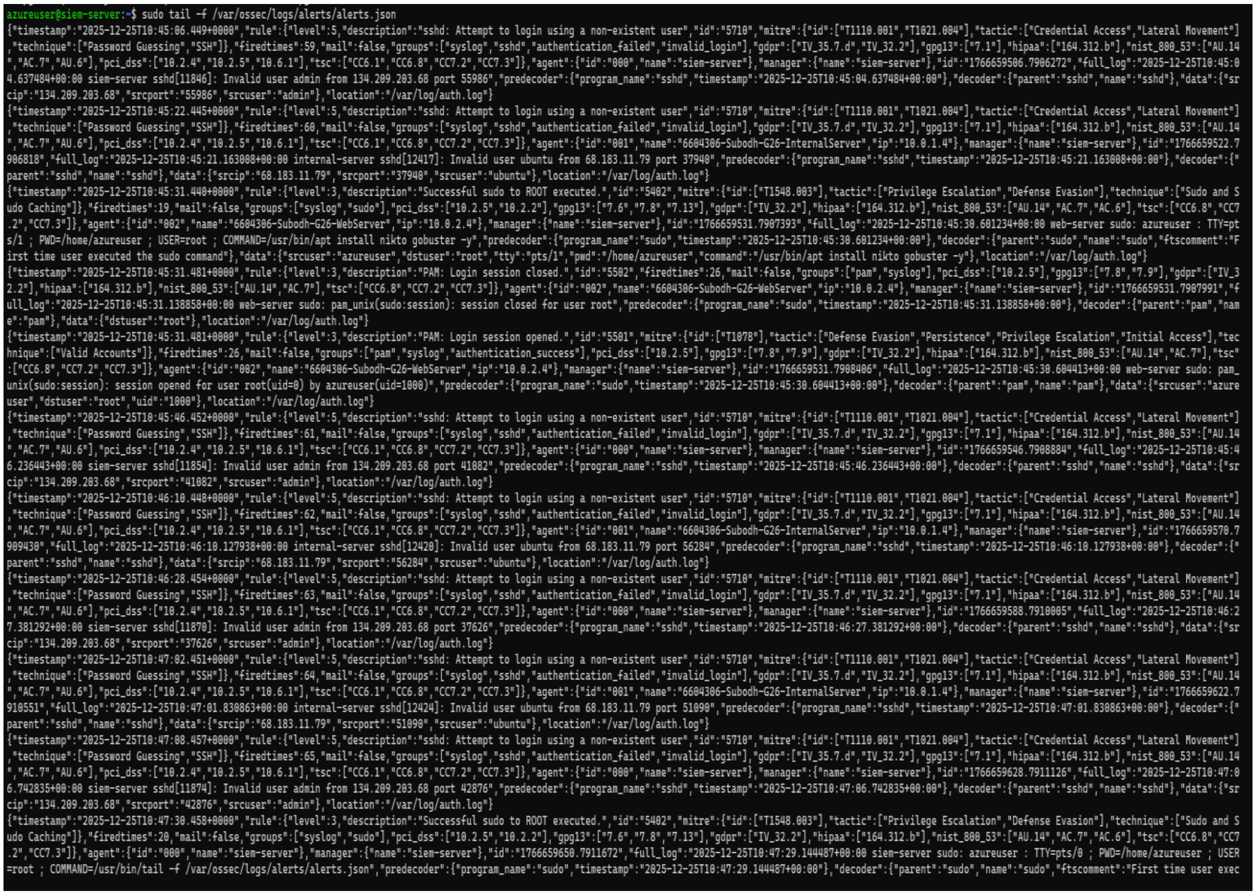
```
-w /etc/passwd -p wa -k passwd_change
-w /var/log/auth.log -p wa -k ssh_log
```

```
sudo systemctl restart auditd
```

---

6. Re-Attack After Hardening

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



```
azureuser@siem-server:~$ sudo tail -f /var/ossec/logs/alerts/alerts.json
{"timestamp":"2025-12-25T10:45:06.449+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":59,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659506.7906272","full_log":"2025-12-25T10:45:0
4.637484+00:00 siem-server sshd[11846]: Invalid user admin from 134.209.203.68 port 55986","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:45:04.637484+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"55986","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:22.445+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":60,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"6604306-Subodh-G26-InternalServer","ip":"10.0.1.4"},"manager":{"name":"siem-server"},"id":"1766659522.7
906818","full_log":"2025-12-25T10:45:21.163008+00:00 internal-server sshd[12417]: Invalid user ubuntu from 68.183.11.79 port 37940","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:45:21.163008+00:00"},"decoder":{"
parent":"sshd","name":"sshd"},"data":{"srcip":"68.183.11.79","srcport":"37940","srcuser":"ubuntu"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:31.440+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic":["Privilege Escalation","Defense Evasion"],"technique":["Sudo and S
udo Caching"]},"firedtimes":19,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","10.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7
.2","CC7.3"]},"agent":{"id":"002","name":"6604306-Subodh-G26-WebServer","ip":"10.0.2.4"},"manager":{"name":"siem-server"},"id":"1766659531.7907393","full_log":"2025-12-25T10:45:30.601234+00:00 web-server sudo: azureuser : TTY=pt
s/1 ; PWD=/home/azureuser ; USER=root ; COMMAND=/usr/bin/apt install nikto gobuster -y","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:45:30.601234+00:00"},"decoder":{"parent":"sudo","name":"sudo","ftscomment":"F
irst time user executed the sudo command"},"data":{"srcuser":"azureuser","dstuser":"root","tty":"pts/1","pwd":"/home/azureuser","command":"/usr/bin/apt install nikto gobuster -y"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:31.481+0000","rule":{"level":3,"description":"PAM: Login session closed.","id":"5502","firedtimes":26,"mail":false,"groups":["pam","syslog"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_3
2.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"002","name":"6604306-Subodh-G26-WebServer","ip":"10.0.2.4"},"manager":{"name":"siem-server"},"id":"1766659531.7907991","f
ull_log":"2025-12-25T10:45:31.138858+00:00 web-server sudo: pam_unix(sudo:session): session closed for user root","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:45:31.138858+00:00"},"decoder":{"parent":"pam","nam
e":"pam"},"data":{"dstuser":"root"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:31.481+0000","rule":{"level":3,"description":"PAM: Login session opened.","id":"5501","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"tec
hnique":["Valid Accounts"]},"firedtimes":26,"mail":false,"groups":["pam","syslog","authentication_success"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc"
:["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"002","name":"6604306-Subodh-G26-WebServer","ip":"10.0.2.4"},"manager":{"name":"siem-server"},"id":"1766659531.7908406","full_log":"2025-12-25T10:45:30.604413+00:00 web-server sudo: pam_
unix(sudo:session): session opened for user root(uid=0) by azureuser(uid=1000)","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:45:30.604413+00:00"},"decoder":{"parent":"pam","name":"pam"},"data":{"srcuser":"azure
user","dstuser":"root","uid":"1000"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:45:46.452+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":61,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659546.7908884","full_log":"2025-12-25T10:45:4
6.236443+00:00 siem-server sshd[11854]: Invalid user admin from 134.209.203.68 port 41082","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:45:46.236443+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"41082","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:46:10.448+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":62,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"6604306-Subodh-G26-InternalServer","ip":"10.0.1.4"},"manager":{"name":"siem-server"},"id":"1766659570.7
909430","full_log":"2025-12-25T10:46:10.127938+00:00 internal-server sshd[12420]: Invalid user ubuntu from 68.183.11.79 port 56284","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:46:10.127938+00:00"},"decoder":{"
parent":"sshd","name":"sshd"},"data":{"srcip":"68.183.11.79","srcport":"56284","srcuser":"ubuntu"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:46:28.454+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":63,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659588.7910005","full_log":"2025-12-25T10:46:2
7.381292+00:00 siem-server sshd[11870]: Invalid user admin from 134.209.203.68 port 37626","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:46:27.381292+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"37626","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:47:02.451+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":64,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"001","name":"6604306-Subodh-G26-InternalServer","ip":"10.0.1.4"},"manager":{"name":"siem-server"},"id":"1766659622.7
910551","full_log":"2025-12-25T10:47:01.830863+00:00 internal-server sshd[12424]: Invalid user ubuntu from 68.183.11.79 port 51090","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:47:01.830863+00:00"},"decoder":{"
parent":"sshd","name":"sshd"},"data":{"srcip":"68.183.11.79","srcport":"51090","srcuser":"ubuntu"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:47:08.457+0000","rule":{"level":5,"description":"sshd: Attempt to login using a non-existent user","id":"5710","mitre":{"id":["T1110.001","T1021.004"],"tactic":["Credential Access","Lateral Movement"]
,"technique":["Password Guessing","SSH"]},"firedtimes":65,"mail":false,"groups":["syslog","sshd","authentication_failed","invalid_login"],"gdpr":["IV_35.7.d","IV_32.2"],"gpg13":["7.1"],"hipaa":["164.312.b"],"nist_800_53":["AU.14
","AC.7","AU.6"],"pci_dss":["10.2.4","10.2.5","10.6.1"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659628.7911126","full_log":"2025-12-25T10:47:0
6.742835+00:00 siem-server sshd[11874]: Invalid user admin from 134.209.203.68 port 42876","predecoder":{"program_name":"sshd","timestamp":"2025-12-25T10:47:06.742835+00:00"},"decoder":{"parent":"sshd","name":"sshd"},"data":{"sr
cip":"134.209.203.68","srcport":"42876","srcuser":"admin"},"location":"/var/log/auth.log"}
{"timestamp":"2025-12-25T10:47:30.458+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic":["Privilege Escalation","Defense Evasion"],"technique":["Sudo and S
udo Caching"]},"firedtimes":20,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","10.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7
.2","CC7.3"]},"agent":{"id":"000","name":"siem-server"},"manager":{"name":"siem-server"},"id":"1766659650.7911672","full_log":"2025-12-25T10:47:29.144487+00:00 siem-server sudo: azureuser : TTY=pts/0 ; PWD=/home/azureuser ; USER
=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.json","predecoder":{"program_name":"sudo","timestamp":"2025-12-25T10:47:29.144487+00:00"},"decoder":{"parent":"sudo","name":"sudo","ftscomment":"First time user exec
```

8 Conclusion

- Successfully simulated real-world cyberattacks on internal infrastructure to evaluate security posture
- Effectively captured, centralized, and analyzed all relevant security events using the Wazuh SIEM platform
- Implemented comprehensive system hardening measures, including secure configurations for SSH, firewall rules, Apache web server, and system security policies
- Clearly demonstrated the complete **Red Team → Blue Team → System Hardening** workflow, highlighting detection, response, and remediation capabilities

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

---