MAJOR PROJECT REPORT

Red Team & Blue Team Cyber Security Simulation on Azure

Student Details

- **Student Name(s): Deepak Kumar Bareth**
- **ERP / Roll No: 6604295**
- **Group No: *10***
- **Assigned Company Name (Resource Group): *Cyber-Project-RG***
- **Azure Subscription:** Azure for Students

---

1. Introduction

This Major Project is a continuation of the Minor Project infrastructure deployment. In this phase, students act as both **Red Team (Attackers)** and **Blue Team (Defenders)** to simulate real-world cyber-attacks, analyze logs using a SIEM platform, identify misconfigurations, apply security hardening, and validate improvements through re-attacks.

---

2. Project Objectives

- Simulate real-world cyber-attacks on a cloud-based enterprise
- Generate and analyze security logs using SIEM
- Identify vulnerabilities and misconfigurations
- Apply system, network, and application hardening
- Compare security posture before and after hardening

---

3. Infrastructure Overview (From Minor Project)

3.1 Azure Environment

- **Resource Group:** Cyber-Project-RG
- **Region: *Central india***

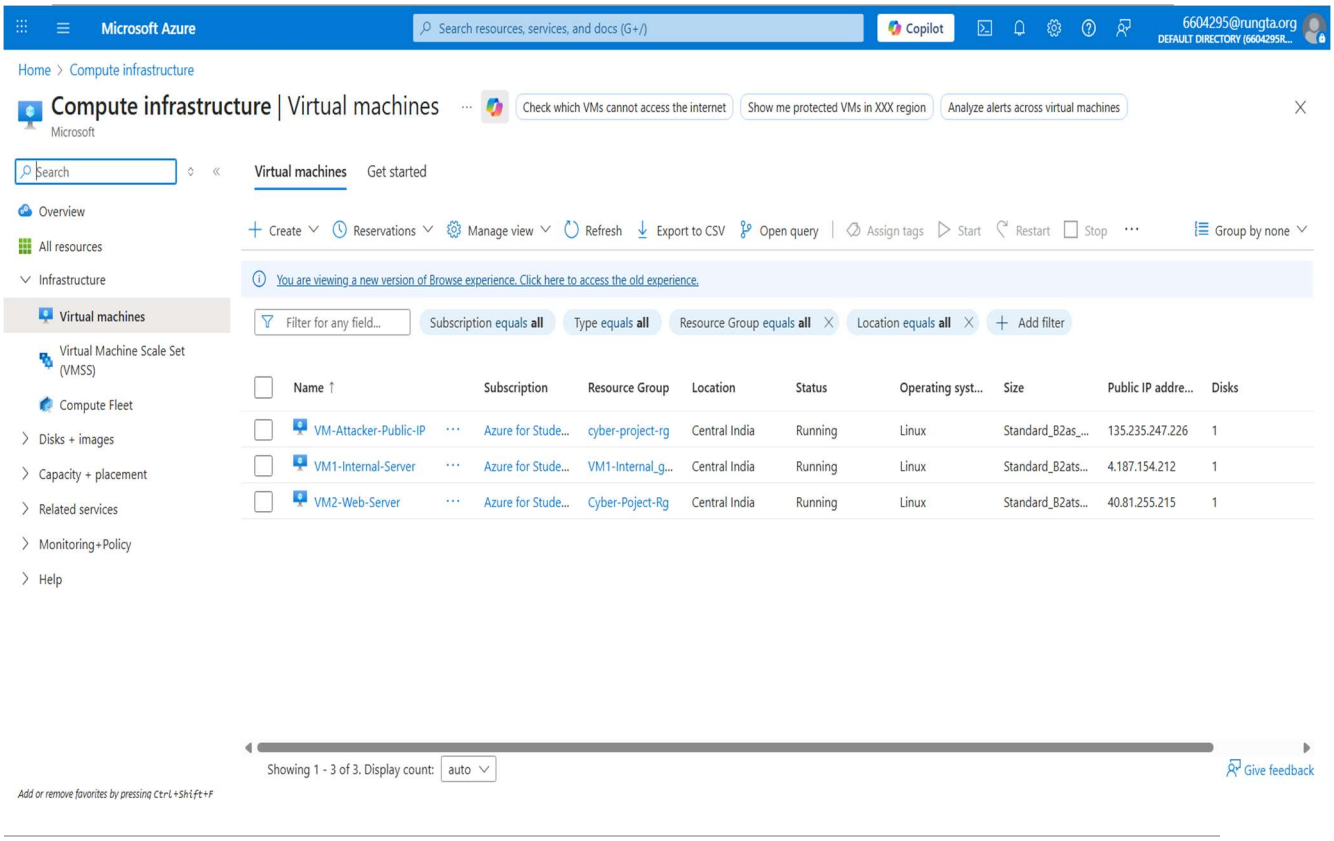
3.2 Network Architecture

- **VNet:** Company-VNet (10.0.0.0/16)
- **Internal Subnet:** 10.0.1.0/24
- **DMZ Subnet:** 10.0.2.0/24

3.3 Virtual Machine Inventory

VM Name	OS	Purpose	IP Address	Subnet	Size

VM1 – Internal Server	Ubuntu 20.04	FreeIPA + File Server	Internal
VM2 – Web Server	Ubuntu 20.04	Apache/Nginx	DMZ
VM3 – SIEM Server	Ubuntu 20.04	Wazuh / ELK	Internal



4. Phase 1 – Red Team Attack Simulation

4.1 Team Roles

- Attacker
- Defender
- Documenter

4.2 Attack Scenarios Performed

4.2.1 Port Scanning & Enumeration

- **Tool Used:** Nmap
- **Target:** VM1, VM2
- **Objective:** Identify open ports and services

📸*Screenshot: Nmap scan output & SIEM log*

```
Deepak@SIEM-VM:~$ curl ifconfig.me
4.187.158.213Deepak@SIEM-VM:~$ nmap -A 4.187.158.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-25 03:25 UTC
Nmap scan report for 4.187.158.213
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 69:1b:15:02:6f:db:fc:80:fc:2c:6e:a4:ca:c8:09:09 (ECDSA)
|_  256 f5:e3:ee:eb:1e:9f:f5:2f:84:ba:cc:4c:0d:4d:7b:5f (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (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 15.71 seconds
Deepak@SIEM-VM:~$
```

4.2.2 SSH Brute Force Attack

- **Tool Used:** Hydra
- **Target:** VM1 & VM2
- **Logs Generated:** auth.log, Wazuh alerts

📸*Screenshot: Hydra output & SIEM brute-force alert*

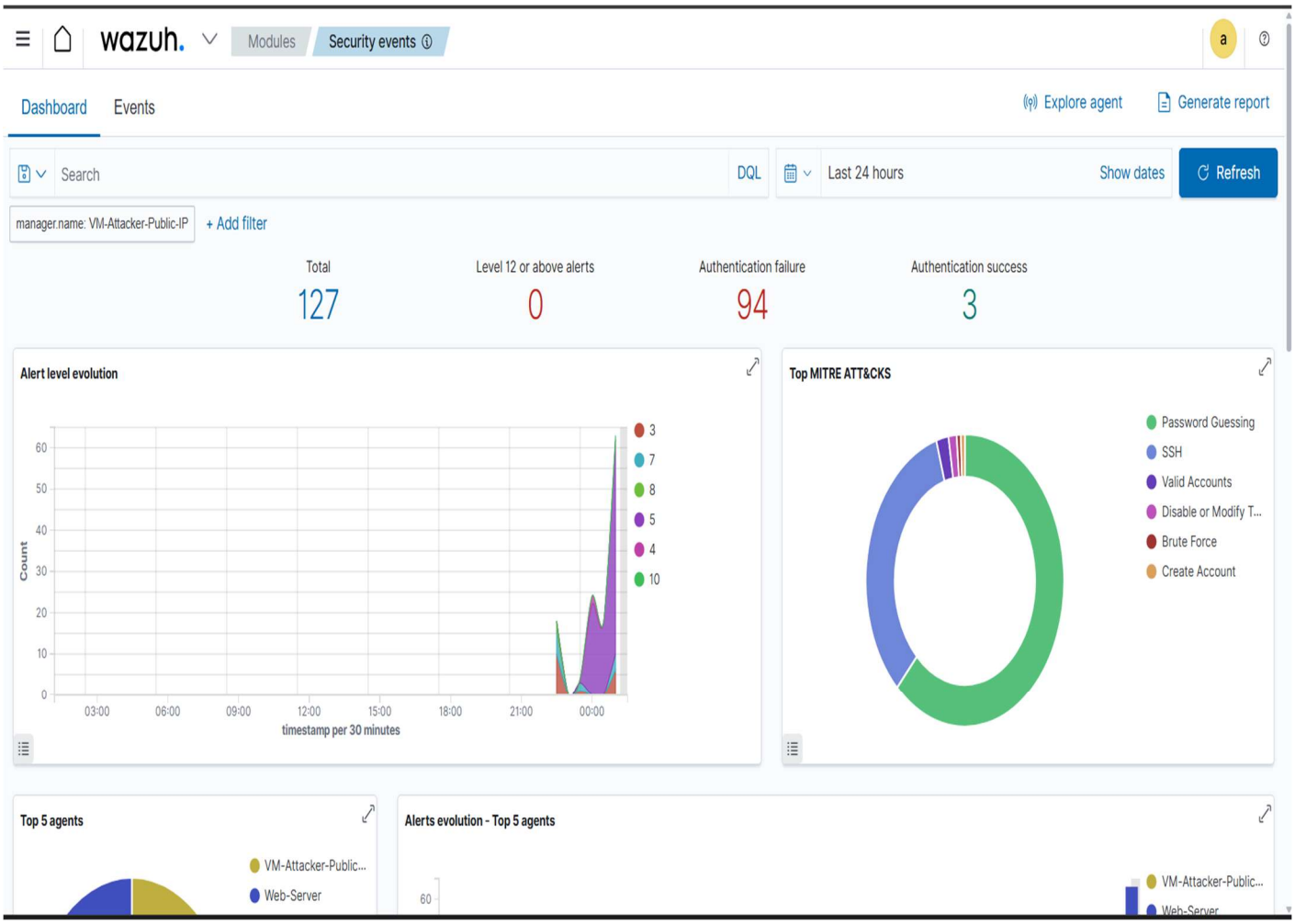
```
Deepak@SIEM-VM:~$ nano passwords.txt
Deepak@SIEM-VM:~$ hydra -l testuser -P passwords.txt ssh://4.187.158.213
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-25 03:38:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://4.187.158.213:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-25 03:38:21
Deepak@SIEM-VM:~$
```

4.2.3 Privilege Escalation Attempts

- **Techniques:** SUID binaries, sudo misconfiguration
- **Logs:** audit.log, auth.log

Screenshot: Privilege escalation attempt logs



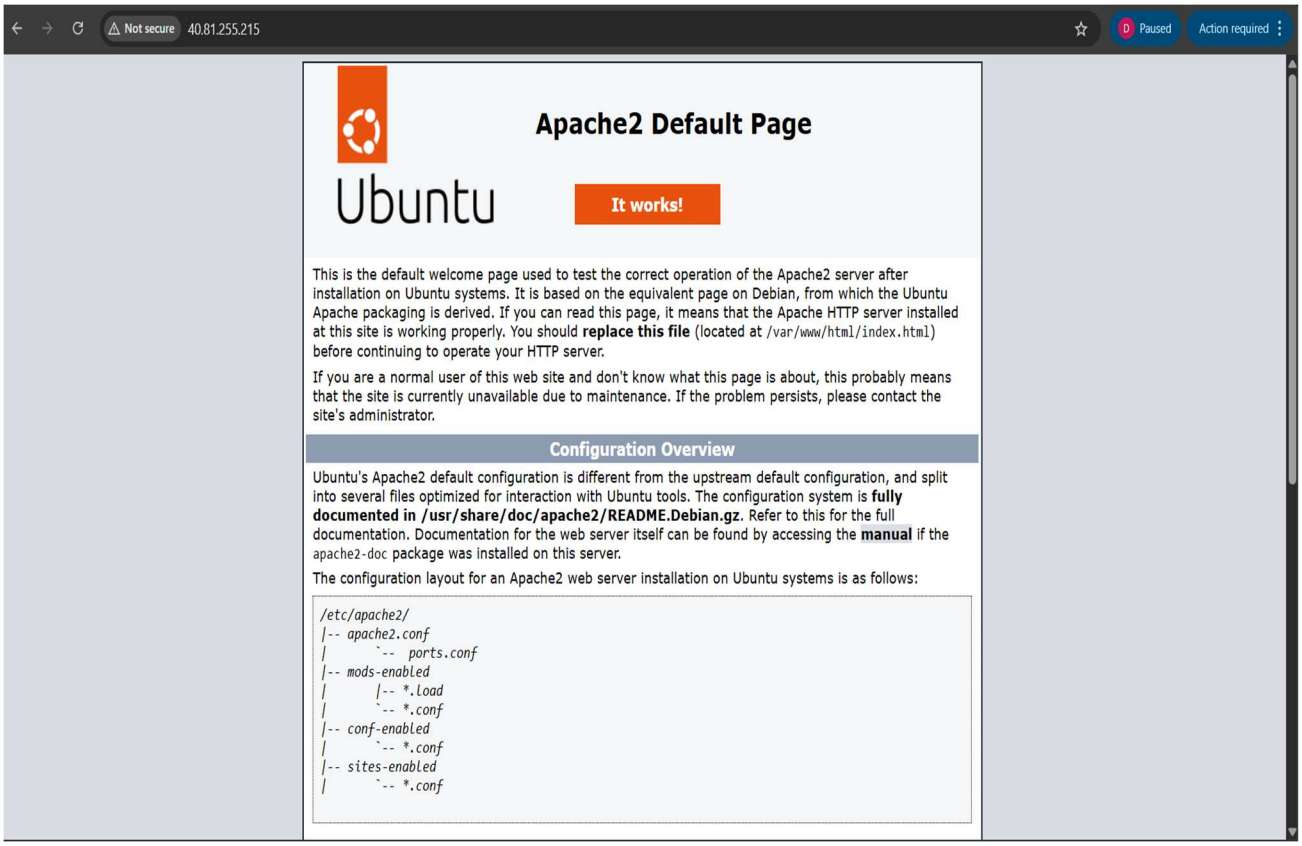
4.2.4 Web Attacks on Web Server

- Directory Traversal
- SQL Injection
- File Enumeration

Tools Used: Nikto, Gobuster, Curl

Screenshot: Apache logs & SIEM alerts

```
deepaak@VM2-Web-Server:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 2086 kB of archives.
After this operation, 8090 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11.2 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9116 B]
Get:5 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.8 [1331 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.8 [163 kB]
Progress: [ 98%] [#################################################..] utils amd64 2.4.58-1ubuntu8.8 [97.7 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.8 [90.2 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Fetched 2086 kB in 1s (3892 kB/s)
Preconfiguring packages ...
Scanning processes...
deepaak@VM2-Web-Server:~$ utdated hypervisor (qemu) binaries on this host.
```



4.2.5 FreeIPA Enumeration

- LDAP queries
- User enumeration

```
Deepak@SIEM-VM:~$ whoami
Deepak
Deepak@SIEM-VM:~$ sudo apt install nmap nikto gobuster hydra -y
[sudo] password for Deepak:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
nikto is already the newest version (1:2.1.5-3.1).
gobuster is already the newest version (3.6.0-1ubuntu0.24.04.3).
hydra is already the newest version (9.5-1build3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Deepak@SIEM-VM:~$
```

 *Screenshot: FreeIPA related logs*

---

5. Phase 2 – Blue Team Investigation

5.1 SIEM Log Analysis

Logs analyzed: - Syslog - auth.log - audit.log - Apache access & error logs

5.2 Indicators of Compromise (IOC)

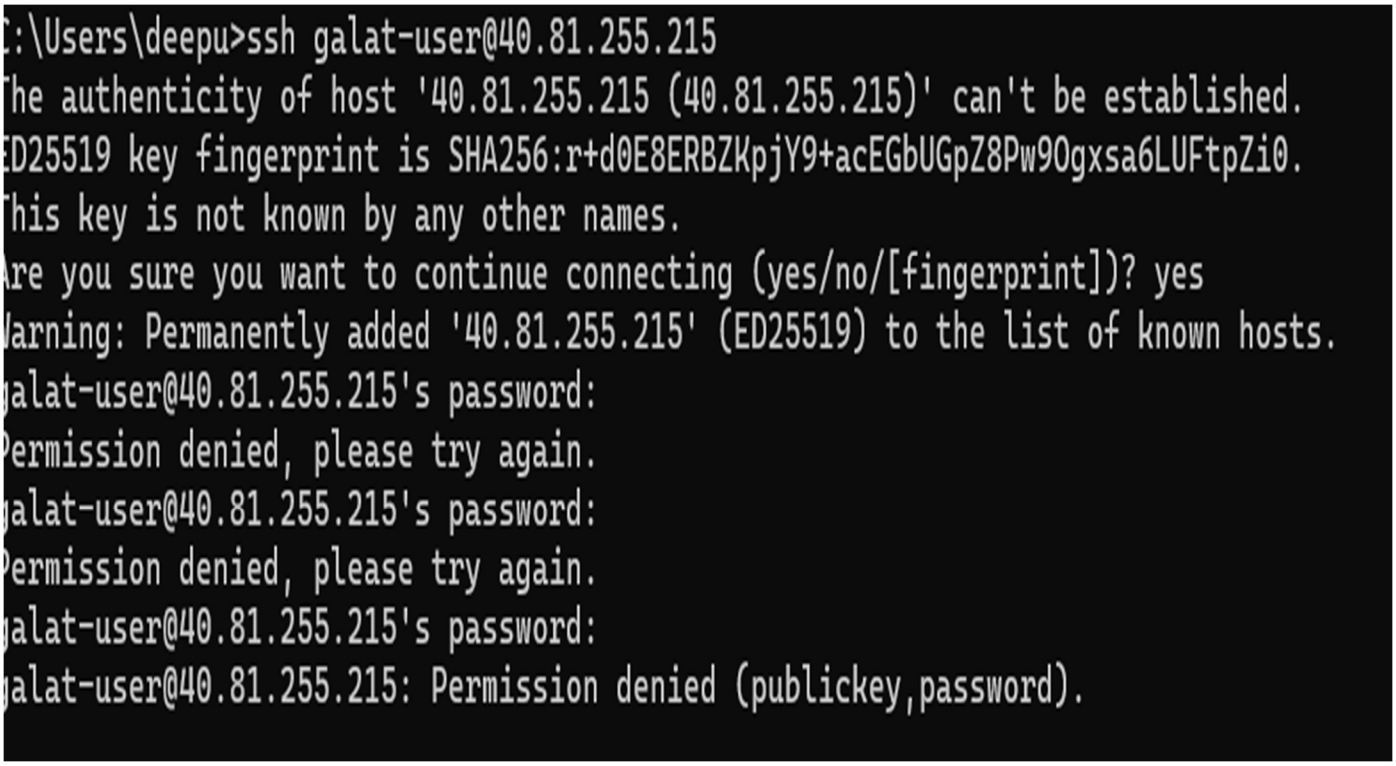
IOC Type	Value	Description
IP Address		Attacker IP
Username		Brute-force target

URL	Malicious request

5.3 Identified Misconfigurations

- SSH password authentication enabled
- Open ports without firewall rules
- Weak credentials
- No DMZ isolation
- No rate limiting
- Default Apache configuration

📸 *Screenshot: Evidence of misconfigurations*



6. Phase 3 – Security Hardening Implementation

6.1 Logging Enhancements

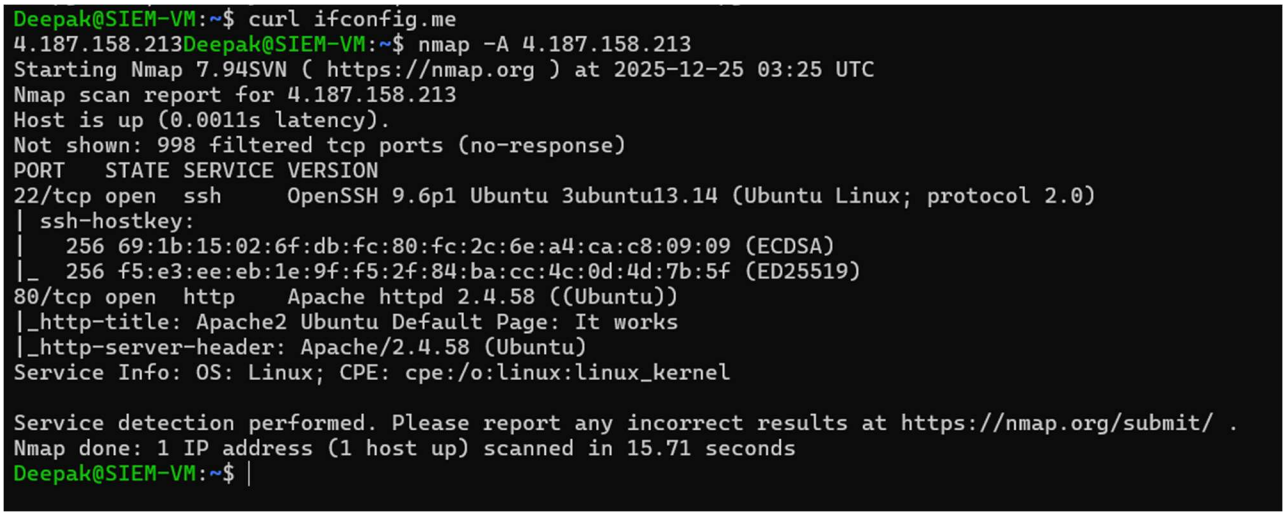
- Sysmon for Linux installed
- Custom Auditd rules configured
- Enhanced Apache logging

6.2 SSH Hardening

- Root login disabled
- Key-based authentication enabled
- SSH port changed
- Rate limiting applied

6.3 Firewall & NSG Hardening

- UFW configured
- SSH restricted to SIEM VM
- DMZ to Internal traffic restricted
- NSG rules tightened



Screenshot: Firewall & NSG rules

6.4 Server & Application Hardening

- Unnecessary services disabled
- Password policies enforced
- Least privilege permissions
- Apache hardened
- FreeIPA secured

---

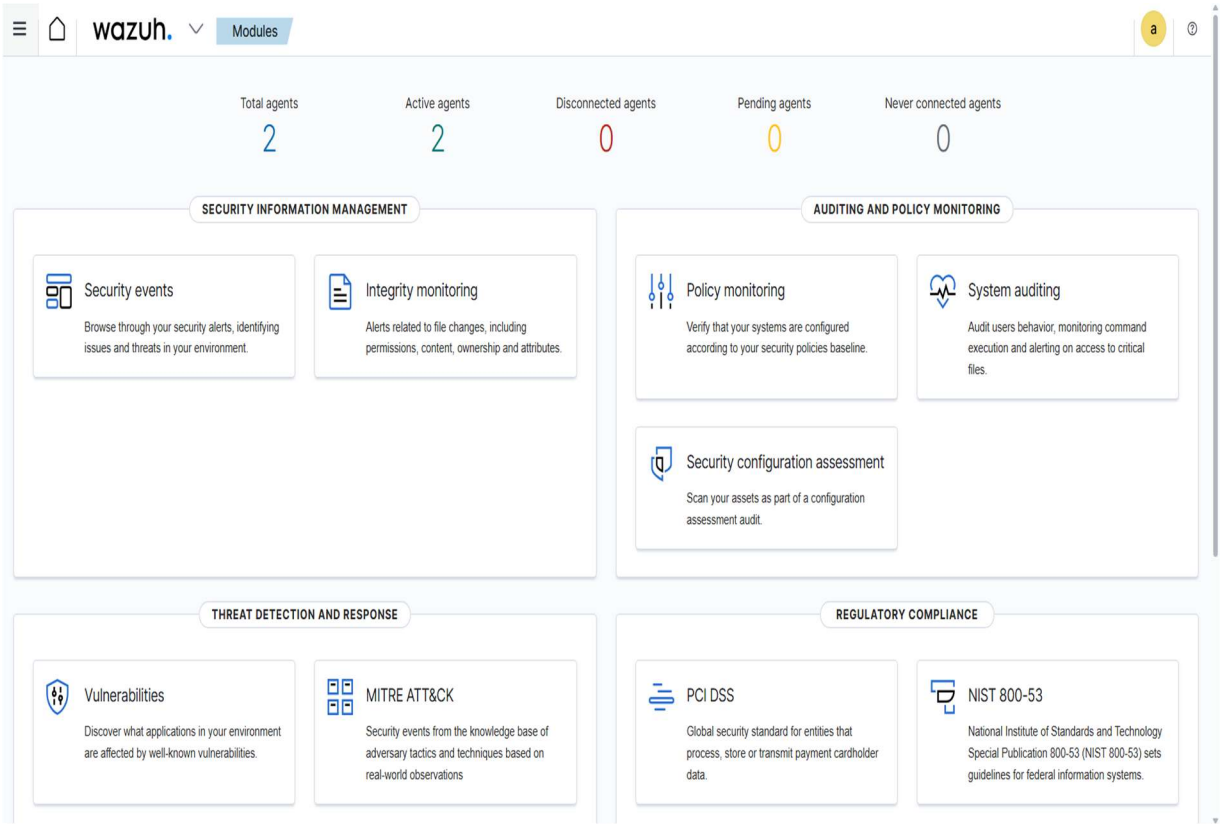
7. Phase 4 – Re-Attack After Hardening

7.1 Repeated Attacks

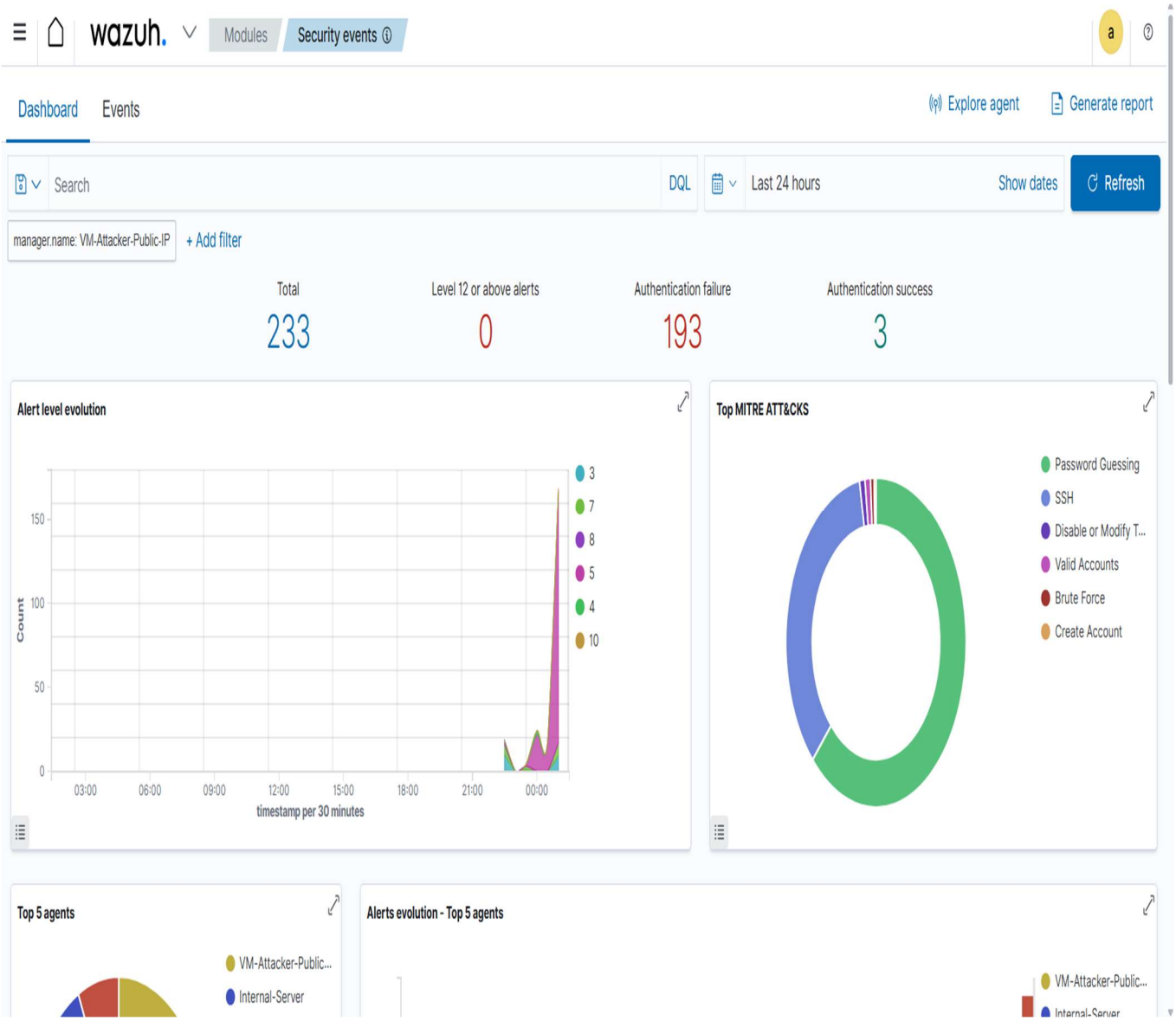
- Nmap scan
- SSH brute force
- Web attacks

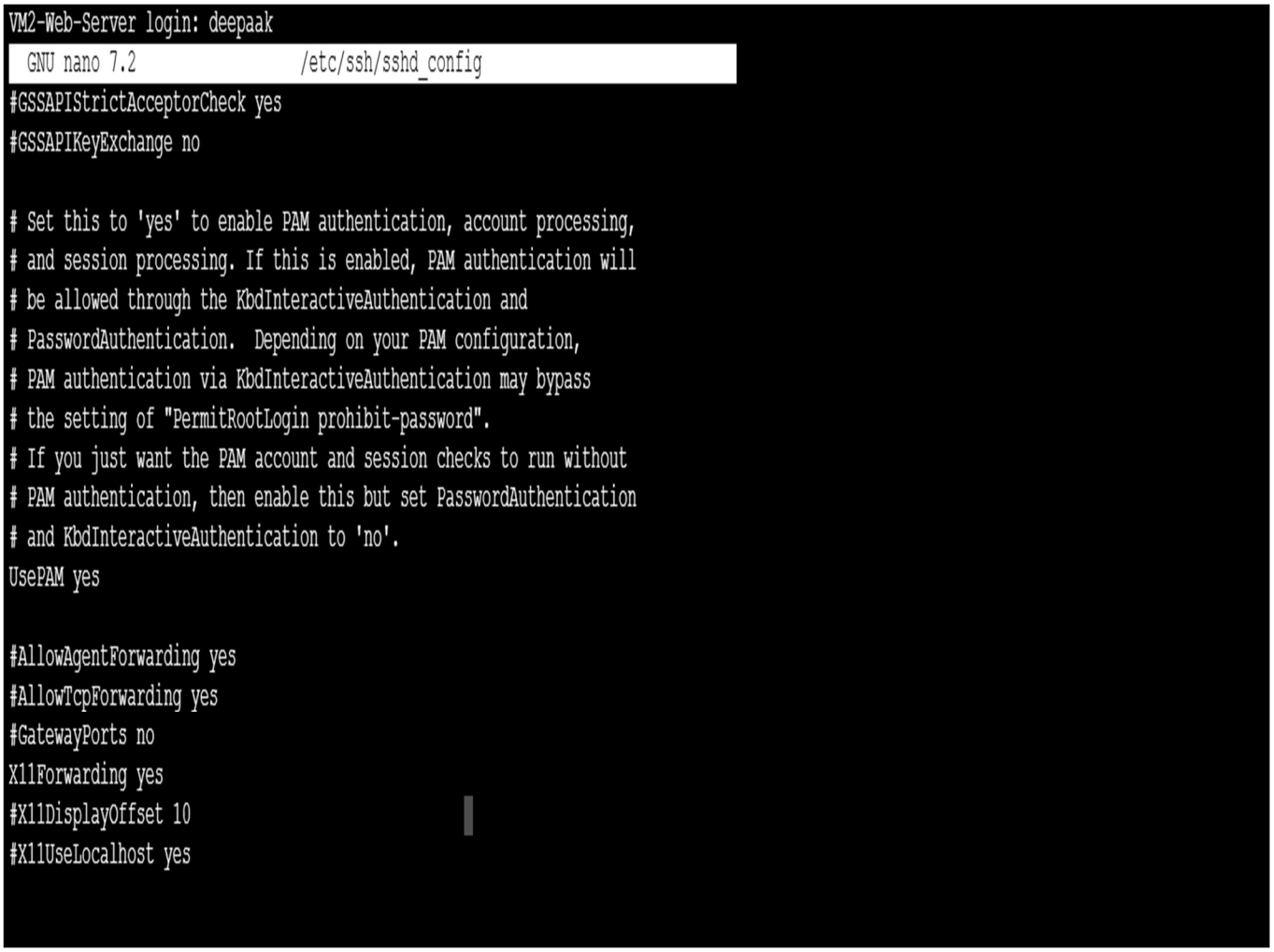
7.2 Observations

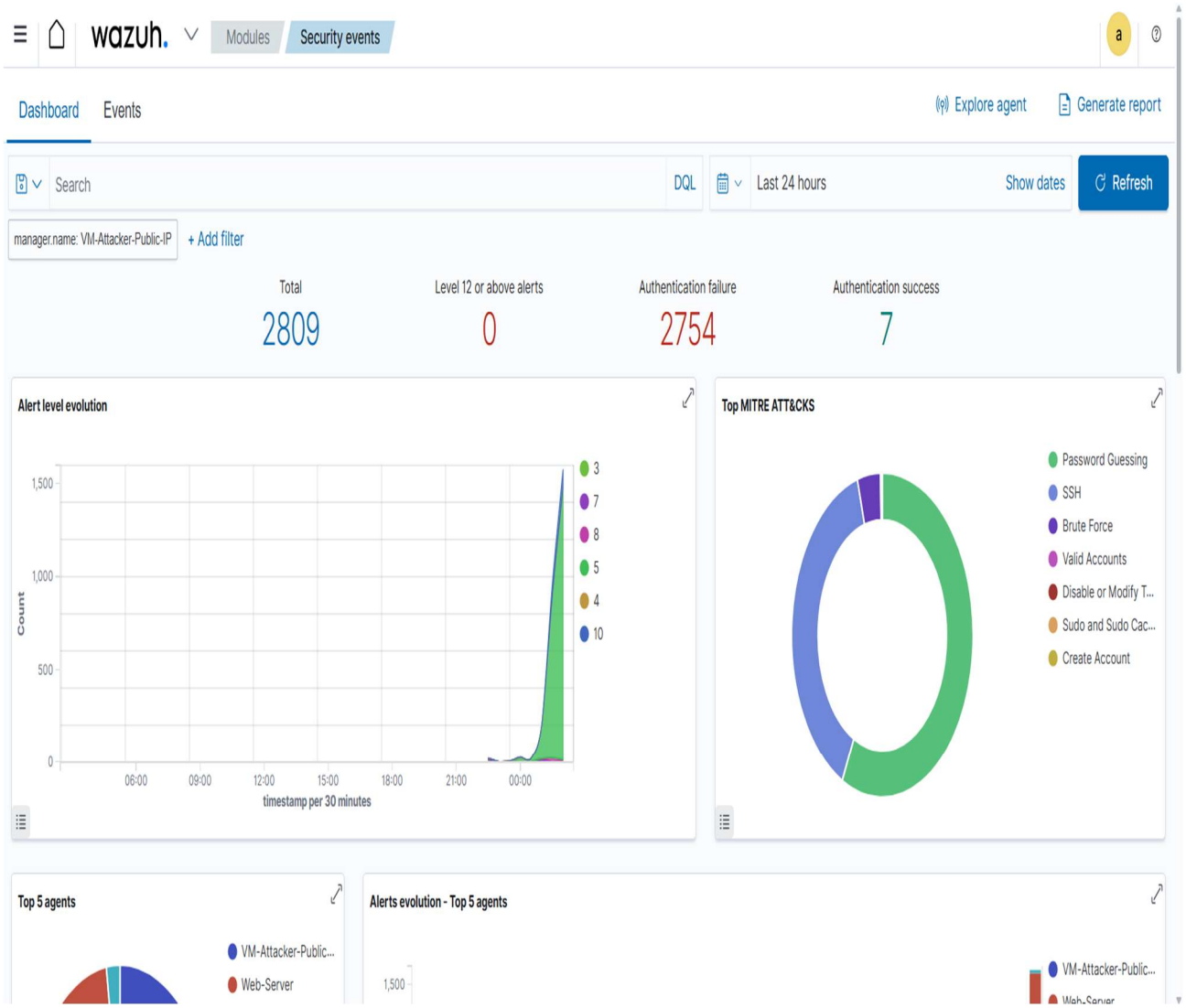
- Attacks failed or limited
- Reduced logs
- Clear SIEM alerts



- Improved detection accuracy




VM2-Web-Server login: deepaak
GNU nano 7.2 /etc/ssh/sshd_config
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
Set this to 'yes' to enable PAM authentication, account processing,
and session processing. If this is enabled, PAM authentication will
be allowed through the KbdInteractiveAuthentication and
PasswordAuthentication. Depending on your PAM configuration,
PAM authentication via KbdInteractiveAuthentication may bypass
the setting of "PermitRootLogin prohibit-password".
If you just want the PAM account and session checks to run without
PAM authentication, then enable this but set PasswordAuthentication
and KbdInteractiveAuthentication to 'no'.
UsePAM yes
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes


wazuh.
Modules
Security events
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: VM-Attacker-Public-IP
+ Add filter
Total
2809
Level 12 or above alerts
0
Authentication failure
2754
Authentication success
7
Alert level evolution
1,500
1,000
500
0
Count
06:00
09:00
12:00
15:00
18:00
21:00
00:00
timestamp per 30 minutes
3
7
8
5
4
10
Top MITRE ATT&CKS
Password Guessing
SSH
Brute Force
Valid Accounts
Disable or Modify T...
Sudo and Sudo Cac...
Create Account
Top 5 agents
VM-Attacker-Public...
Web-Server
Alerts evolution - Top 5 agents
1,500
VM-Attacker-Public...

Screenshot: Before vs After SIEM comparison

8. Before vs After Comparison

Aspect	Before Hardening	After Hardening
SSH Security	Weak	Strong
Firewall	None	Enabled
Logs	Basic	Enhanced
Attack Success	High	Low

---

9. Final Security Posture

After applying security hardening, the infrastructure demonstrates: - Reduced attack surface - Improved logging and monitoring - Stronger access control - Effective incident detection

---

10. Conclusion

This project successfully demonstrated the full lifecycle of a cyber-attack and defense scenario in a cloud environment, highlighting the importance of logging, monitoring, and systematic hardening.

---

11. References

- Azure Documentation
- Wazuh Documentation
- Linux Security Guides
