MAJOR PROJECT REPORT

Title

Attack, Detect & Secure a Cloud-Based Linux Infrastructure

Student Details

- **Name:** Haripad Patar
- **Course:** B.Tech (Computer Science / Cyber Security Lab)
- **Project Type:** Major Project
- **Cloud Platform Used:** AWS EC2 (Equivalent to Azure – Faculty Approved)
- **Operating System:** Ubuntu Server 24.04 LTS

1. Overview

In this major project, the student performed the role of both Red Team (Attacker) and Blue Team (Defender) to simulate real-world cyber-attacks on a cloud-based Linux infrastructure. The objective was to generate attack logs, analyze them, identify misconfigurations, apply security hardening, and validate improved security posture through re-attack testing.

The infrastructure was initially deployed in the Minor Project phase and intentionally left vulnerable. This Major Project focuses on attack simulation, detection, investigation, and system hardening.

2. Objective

- Simulate real-world cyber attacks on a Linux server
- Generate authentication and web access logs
- Identify security misconfigurations
- Apply Linux server hardening techniques
- Demonstrate improved security after hardening

3. Infrastructure Details

- **Instance Type:** t3.micro
- **Public IP:** Assigned dynamically
- **Services Installed:**
  - OpenSSH
  - Apache Web Server
- **Firewall:** AWS Security Group + UFW (after hardening)

4. Phase 1 – Red Team (Attack Simulation)

4.1 Network & Service Scanning

Tool Used: Nmap

- TCP SYN scan performed to identify open ports
- Open ports discovered:
  - Port 22 (SSH)

  - Port 80 (HTTP)

Result: The system exposed SSH and web services to the public network.

4.2 Web Enumeration

Tool Used: Nikto

- Apache default configuration detected
- HTTP headers and accessible paths identified
- Web access logs generated in Apache

4.3 SSH Authentication Attempts

- Multiple unauthorized SSH login attempts were performed
- Authentication failures recorded in system logs

Logs Generated:

- /var/log/auth.log

5. Phase 2 – Blue Team (Investigation & Detection)

5.1 Log Analysis

The following logs were analyzed:

- SSH authentication logs (auth.log)
- Apache access logs (access.log)

Indicators observed:

- Failed login attempts
- Repeated access attempts from external IPs
- Unrestricted inbound access

5.2 Identified Misconfigurations

- Password-based SSH authentication enabled
- Root login permitted
- Firewall not enabled on host
- Open inbound access from all IPs

6. Security Hardening (Implemented)

6.1 SSH Hardening

The following configurations were applied:

- Root login disabled
- Password-based authentication disabled
- Key-based authentication enforced

Configuration Applied:

```
PermitRootLogin no

PasswordAuthentication no
```

6.2 Firewall Hardening (UFW)

- Host-based firewall enabled
- Default policy set to deny incoming traffic
- Only required ports allowed

Allowed Ports:

- 22/tcp (SSH)
- 80/tcp (HTTP)

7. Re-Attack After Hardening

After applying security controls, the same SSH attack attempts were repeated.

Result:

- SSH access denied for unauthorized users
- Password-based login blocked
- Reduced attack surface confirmed

Observed Message:

```
Permission denied (publickey).
```

8. Before vs After Comparison

Security Aspect	Before Hardening	After Hardening
SSH Root Login	Allowed	Disabled
Password Auth	Enabled	Disabled
Firewall	Disabled	Enabled
Attack Result	Login attempts possible	Access denied

9. SIEM Deployment Note

A Wazuh SIEM deployment was attempted. Due to limited cloud resources, full dashboard installation was not feasible. However, SIEM architecture, alert flow, and log correlation were demonstrated using system logs and attack evidence. This reflects real-world SOC environments where lightweight nodes forward logs to centralized SIEM servers.

10. Conclusion

This project successfully demonstrated end-to-end cybersecurity operations including attack simulation, log analysis, vulnerability identification, and system hardening. The before-and-after comparison clearly shows an improved security posture. The project reflects real-world defensive practices used in modern SOC environments.

11. Learning Outcomes

- Hands-on experience with Red Team attacks
- Linux log analysis and investigation skills
- Practical server hardening techniques
- Understanding of real-world SIEM constraints
- End-to-end security lifecycle implementation

End of Report