Apollo 13- Red vs. Blue Team Penetration Testing Exercise

Red Team: Jimmy- Jack - Naila

Blue Team: Calvin - Muhammad - Burton

AWS EC2 - Kali Linux - Windows Server 2022 - Wazuh SIEM

PURPOSE

Design and deploy a realistic enterprise network in AWS EC2, then conduct a controlled Red Team vs. Blue Team cybersecurity exercise, demonstrating real attack technologies and live defensive monitoring against a fictional company, Apollo Corporation

NETWORK ARCHITECTURE

- Kali Linux - attacker machine (10.0.5.103)
- Legacy admin server
- App Server
- File Server
- Database Server - Public web server (Nginx)
- Windows Server 2022 domain controller (AD DS)
- Windows workstations (x2)
- Wazuh SIEM - blue team monitoring (10.0.8.207)

TOOLS USED

Nmap | Gobuster | Feroxbuster | Nikto | SQLMap | Hydra | smbclient | Metasploit | tcpdump | Wazuh | AWS CloudTrail | CloudWatch

METHODOLOGY

Recon → Vulnerability discovery→ Exploitation → Post- exploitation / data exfiltration → Impact assessment. Blue team monitored in real time via Wazuh and AWS-native tools.

KEY TAKEAWAYS

Misconfigurations are as dangerous as unpatched vulnerabilities. Passive recon alone yielded employee PII and full infrastructure mapping. Active monitoring and hardening (parameterized queries, disabled debug mode, key-based SSH) prevented full compromise.

KEY FINDINGS

CRITICAL

Unauthenticated API endpoints on app server - full employee PII, IT tickets, and infrastructure inventory exfiltrated with no credentials

HIGH

Anonymous write access on SMB public share - attacker could plant malicious files

HIGH

SMB null session share enumeration - internal share structure exposed unauthenticated

MEDIUM

The public web server's robots.txt disclosed internal paths including /admin/, /internal/, and /backup/ providing an attacker a free directory map of sensitive endpoints.

MEDIUM

Legacy portal and web server lacked key security headers, leaving users exposed to clickjacking and MIME sniffing attacks.

OUTCOME

Red team exfiltrated sensitive data through misconfigured APIs and SMB - no software exploit required.

Blue team detected and disrupted Hydra brute force attack via Wazuh, rebooting the server mid-scan. Full RCE was not achieved.