Capstone Project Report

Full Red Team Engagement Simulation

Introduction

This capstone project demonstrates a simulated **full red team engagement** conducted within a controlled lab environment. The objective was to emulate a real-world cyberattack by following the complete attack lifecycle—reconnaissance, initial access, exploitation, lateral movement, persistence, and data exfiltration—while simultaneously evaluating blue team detection capabilities using security logs.

All activities were performed in an **isolated virtual lab** using Kali Linux as the attacker machine and a Windows system as the victim. No real systems or external networks were targeted.

Scope and Tools Used

Scope

- Internal lab network only
- No real users, domains, or production data
- Simulated phishing and exploitation

Tools

- Kali Linux
- Recon-ng
- Metasploit Framework
- Covenant Command & Control
- Wazuh (Blue Team Monitoring)
- Google Docs (Reporting)

Attack Simulation Overview

The engagement followed the **MITRE ATT&CK framework**, ensuring realism and structured documentation.

Attack Phases

1. Reconnaissance
2. Initial Access (Phishing)
3. Execution & Persistence
4. Privilege Escalation

5. Lateral Movement

6. Data Exfiltration

Red Team Activity Log

Phase	Tool Used	Action Description	MITRE Technique
Reconnaissance	Recon-ng	Created workspace and simulated subdomain enumeration	T1595
Initial Access	Metasploit	Reverse TCP payload executed via phishing simulation	T1566
Execution	Metasploit	Payload execution and meterpreter session	T1059
Persistence	Covenant	Deployed C2 agent for long-term access	T1053
Privilege Escalation	Metasploit	Used local exploit suggester	T1068
Lateral Movement	Metasploit	SMB-based credential reuse	T1021

Exfiltration	Covenant	Data exfiltration over encrypted C2 channel	T1041

Detailed Attack Description

- **Reconnaissance**

Reconnaissance was conducted using Recon-ng by creating a workspace and defining a lab domain (`lab.local`). Subdomain enumeration modules were executed to simulate OSINT-based information gathering.

Although the lab environment was offline, this step successfully demonstrated how attackers prepare targets before exploitation.

- **Initial Access**

Initial access was achieved using a phishing simulation. A malicious payload was generated using Metasploit and executed on the victim machine, simulating a user clicking a phishing attachment.

This resulted in a successful reverse shell connection to the attacker system.

- **Execution and Persistence**

Once access was obtained, commands were executed to gather system information and user privileges. A Covenant C2 agent was deployed to establish persistence, ensuring continued access even after session interruption.

- **Privilege Escalation**

Local privilege escalation checks were performed using Metasploit’s automated modules. Misconfigurations in the system allowed the attacker to gain elevated privileges.

- **Lateral Movement**

Using harvested credentials, the attacker attempted lateral movement across the internal network via SMB authentication. This simulated the spread of an attacker inside a compromised organization.

- **Data Exfiltration**

Test files were exfiltrated using Covenant’s encrypted command-and-control channel, simulating the theft of sensitive organizational data.

Blue Team Analysis (Wazuh Logs)

Detected Security Events

Timestamp	Alert Description	Source IP	Notes

2025-08-29 13:00:00	Suspicious Login	192.168.1.50	Phishing-based credential compromise
2025-08-29 13:12:45	Abnormal Process Execution	192.168.1.50	Payload execution detected
2025-08-29 13:25:10	SMB Authentication Anomaly	192.168.1.51	Lateral movement attempt
2025-08-29 13:40:30	Suspicious Network Traffic	192.168.1.50	Possible data exfiltration

Observations

- Phishing was not blocked at the email level
- Endpoint detection reacted **after execution**, not before
- Lateral movement detection worked but was delayed

Evasion Test Results

Technique Used

- Obfuscated PowerShell payload

- Base64 encoding
- String fragmentation

Outcome

- Mock antivirus failed to detect the payload
- Behavioral alerts were triggered post-execution

Impact

This demonstrates the weakness of signature-based defenses and highlights the importance of behavior-based detection.

Executive Summary

This capstone project simulated a full red team engagement to assess the effectiveness of defensive security controls in a controlled lab environment. The attack followed a realistic lifecycle beginning with reconnaissance and ending with simulated data exfiltration. A phishing-based initial access technique allowed the attacker to successfully compromise the victim system.

Post-compromise activities included privilege escalation, lateral movement, and persistent command-and-control access. While security monitoring tools such as Wazuh detected several suspicious events, alerts were generated only after key attack stages had already occurred.

The evasion test further revealed that obfuscated payloads could bypass traditional antivirus detection, emphasizing the need for behavioral monitoring. Overall, the exercise demonstrated that while detection mechanisms exist, earlier prevention and faster response are required to limit attacker movement.

Recommendations

- Deploy advanced phishing email filtering
- Implement behavioral EDR solutions
- Improve SIEM correlation rules
- Conduct regular red team and purple team exercises
- Provide user security awareness training

Briefing

This project tested how well an organization can defend against a cyberattack by simulating a real attacker inside a safe lab environment. The attack began with a fake email and progressed through the internal network, attempting to steal data. Security tools did detect suspicious behavior, but only after the attacker had already gained access. This shows the need for stronger email security, faster detection, and better endpoint protection. Improving these controls will help stop attacks earlier and reduce potential damage.

Conclusion

The full red team engagement successfully demonstrated real-world attack techniques and defensive gaps. The project highlights the importance of proactive security controls, continuous monitoring, and regular testing to improve organizational cyber resilience.