Capstone Project: Full Adversary Simulation

1. Simulation Overview

This capstone project simulated a full red team campaign against a controlled lab environment to evaluate offensive capabilities and defensive detection effectiveness. The engagement followed a realistic adversary lifecycle including reconnaissance, cloud exploitation, phishing-based access, command and control (C2), evasion, and data exfiltration. All activities were conducted in an isolated environment using ethical red teaming principles.

2. Tools Used

- Kali Linux (Attacker platform)
- **Pacu** – Cloud reconnaissance and privilege abuse
- **MITRE Caldera** – Adversary simulation and automation
- **Metasploit** – Payload delivery and C2 support
- **Wazuh** – Blue team detection and log analysis
- Google Docs – Reporting

3. Campaign Execution Log

Phase	Tool Used	Action Description	MITRE Technique
Recon	Pacu	Enumerated misconfigured S3 buckets	T1580
Initial Access	Caldera	Simulated phishing-based agent delivery	T1566.001
Privilege Escalation	Pacu	IAM role abuse	T1078.004
Command & Control	Metasploit	Encrypted C2 session established	T1071
Evasion	Metasploit	Obfuscated payload bypassed AV	T1027
Exfiltration	Caldera	Simulated data transfer	T1537

4. Blue Team Detection Analysis

Timestamp	Alert Description	Source IP	Notes
2026-01-13 14:00:00	Suspicious Access	192.168.0.5	Cloud privilege escalation
2026-01-13 14:07:00	Abnormal PowerShell	192.168.0.5	Post-exploitation activity
2026-01-13 14:15:00	Encrypted Traffic	192.168.0.5	Possible C2 communication

Observation:
Early-stage reconnaissance and phishing generated minimal alerts. Detection improved during privilege escalation and post-exploitation, indicating gaps in early-stage visibility.

5. Evasion Test Validation

An obfuscated payload was deployed during the exploitation phase. Endpoint antivirus did not immediately block execution, and successful session establishment confirmed evasion effectiveness. Subsequent behavioral alerts were observed in Wazuh logs during execution, validating delayed detection.

6. PTES-Compliant Report

Executive Summary

This assessment simulated a full adversary campaign to evaluate security posture across cloud, identity, endpoint, and monitoring controls. The red team successfully progressed through multiple attack stages, including reconnaissance, privilege escalation, command and control, and evasion. While defensive controls detected later-stage activity, early phases such as phishing and cloud reconnaissance were not immediately identified, increasing overall risk.

Findings

- Cloud misconfigurations enabled unauthorized access and privilege escalation
- Phishing-based access allowed attacker foothold
- Encrypted C2 traffic blended with normal network activity
- Obfuscated payloads bypassed initial endpoint defenses
- Blue team detection was delayed until post-exploitation stages

Recommendations

- Enforce least-privilege IAM policies
- Strengthen phishing detection and MFA enforcement
- Deploy behavior-based endpoint detection (EDR)
- Improve correlation of cloud and endpoint logs
- Conduct regular adversary emulation exercises

7. Executive Briefing

This assessment demonstrated how a cyber attacker could gain access, escalate privileges, and maintain control over systems before being detected. While security controls identified some malicious activity, early warning signs such as phishing and cloud misuse were not immediately detected. These gaps increase the risk of data breaches and prolonged attacker presence. Strengthening identity security, improving monitoring, and enhancing endpoint detection will significantly reduce the organization’s exposure to advanced cyber threats.