

9. Capstone Project: Full Adversary Simulation

Activities:

- **Tools:** Kali Linux, Metasploit, Caldera, Pacu, Google Docs.
- **Tasks:** Simulate a full red team campaign, report findings, engage community.
- **Brief:**
 - **Simulation:** Execute a campaign (recon, cloud attack, phishing, C2, exfiltration) against a lab environment. Log:

Phase	Tool Used	Action Description	MITRE Technique
Recon	Pacu	S3 bucket enum	T1580

Red Team Simulation Report:

Target Environment: AWS-centric cloud lab with hybrid on-prem interface

Objective: Identify misconfigurations, steal data, and maintain persistent C2 access

Rules of Engagement: No destructive actions; simulate realistic attacker behavior

Duration: 4 days (simulated timeline)

Logs:

Phase	Tool Used	Action Description	MITRE Technique
Recon	Pacu	S3 bucket enumeration, IAM user enumeration	T1580, T1087
Recon	amass / sublist3r	Cloud asset and subdomain discovery	T1590.002
Recon	CloudSploit	Scanned for cloud misconfigs (public EC2, open SGs)	T1538
Initial Access	GoPhish	Sent targeted phishing with AWS-themed login page	T1566.001
Initial Access	Evilginx2	Bypassed MFA and captured session tokens	T1556.004
Execution	AWS CLI + STS	Used stolen session tokens to assume role	T1078.004

Persistence	Pacu + Lambda	Deployed malicious AWS Lambda for recurring access	T1505.003
Priv Esc	Enumeration script	Abused misconfigured IAM role trust policies	T1484.002
Defense Evasion	CloudTrail tampering	Disabled logging for short window	T1562.008
Lateral Move	SSM Session Manager	Jumped between EC2s without SSH	T1021.004
C2	Cobalt Strike	Established HTTPS C2 over port 443	T1071.001
Exfiltration	AWS CLI	Exfiltrated S3 objects, RDS snapshots to attacker S3	T1567.002
Cleanup	Manual / Scripts	Removed Lambda, reverted roles, re-enabled CloudTrail	T1070.006

Findings:

Cloud Misconfigurations

- Public S3 Buckets:** 3 were world-readable, 1 had write access
- Overprivileged IAM Roles:** Several roles had Administrator Access attached
- Unused Access Keys:** 5+ IAM users had active keys unused for 90+ days
- SSM Open Access:** EC2 instances allowed session hijacking via SSM with no MFA

Community Engagement:

Purpose: Raise awareness on cloud-native attack paths and offer remediation.



- **Blue Team Analysis:** Review Wazuh logs for detection points. Log:

Timestamp	Alert Description	Source IP	Notes
2025-08-30 14:00:00	Suspicious Access	192.168.1.50	Cloud escalation

Wazuh Logs:

Timestamp	Alert Description	Source IP	Notes
2025-08-30 14:00:00	Suspicious Access	192.168.1.50	Cloud escalation
2025-08-30 14:05:32	New IAM Role Created	192.168.1.50	Malicious persistence setup
2025-08-30 14:06:10	CloudTrail Stopped	192.168.1.50	Attempt to evade logging
2025-08-30 14:07:44	Lambda Deployed	192.168.1.50	Backdoor via function
2025-08-30 14:08:12	S3 Access Anomaly	192.168.1.50	Access from unusual IP
2025-08-30 14:09:01	STS Token Usage	192.168.1.50	Temporary creds used
2025-08-30 14:10:33	C2 Beacon Detected	192.168.1.50	Cobalt Strike beacon

Detection Points:

Red Team Phase	Blue Team Detection (Wazuh)	MITRE Technique	Detection Type
Privilege Escalation	Suspicious Access + IAM Role Created	T1484.002	Rule-based correlation
Persistence	Lambda Deployed	T1505.003	CloudTrail audit logs
Defense Evasion	CloudTrail Stopped	T1562.008	Critical system alert

Exfiltration	S3 Access Anomaly	T1567.002	Behavior anomaly
Credential Abuse	STS Token Usage (outside normal times)	T1078.004	Identity analytics
C2 Communication	C2 Beacon Detected via HTTPS to known bad IP	T1071.001	NIDS integration

- **Evasion Test:** Bypass AV with an obfuscated payload; confirm in logs.

Obfuscated Payload Bypass:

Goal: Simulate delivery and execution of an obfuscated payload that evades antivirus (AV) and EDR

Payload Type: Reverse shell (PowerShell-based), obfuscated

Test Environment: Windows 8.x endpoint with AV enabled, monitored via Wazuh agent

Timestamp	Alert Description	Source IP	Notes
2025-08-30 14:11:05	Suspicious PowerShell Exec	192.168.1.50	Obfuscated PS + Base64 use
2025-08-30 14:11:07	Network Connection	192.168.1.50	HTTPS to 10.0.0.99:443



- **Reporting:** Write a 200-word PTES report in Google Docs:

Executive Summary

Executive Summary

Operation Name: Oxidian Cloud
Simulation Date: August 30, 2025
Scope: Simulated red team attack on cloud-hybrid lab environment to evaluate detection, response, and resiliency against modern threat actor TTPs.
Objective: Identify vulnerabilities, test evasion techniques, assess incident detection and response capabilities.

Key Findings

- Successfully gained initial access via phishing and session hijack (bypassing MFA with Evilginx2).
- Escalated privileges using misconfigured IAM roles and established persistence via malicious AWS Lambda function.
- Attempted defense evasion by disabling AWS CloudTrail logs temporarily.
- Achieved data exfiltration by copying sensitive S3 bucket contents and RDS snapshots.
- Established C2 (Command and Control) via encrypted HTTPS channel using Cobalt Strike.

Blue Team Detections (via Wazuh)

Time	Detection	Tool	Notes
14:00:00	Suspicious Access Detected	Wazuh	Privilege escalation attempt

Findings (include blue team detections)

Key Findings

- Successfully gained initial access via phishing and session hijack (bypassing MFA with Evilginx2).
- Escalated privileges using misconfigured IAM roles and established persistence via malicious AWS Lambda function.
- Attempted defense evasion by disabling AWS CloudTrail logs temporarily.
- Achieved data exfiltration by copying sensitive S3 bucket contents and RDS snapshots.
- Established C2 (Command and Control) via encrypted HTTPS channel using Cobalt Strike.

Blue Team Detections (via Wazuh)

Time	Detection	Tool	Notes
14:00:00	Suspicious Access Detected	Wazuh	Privilege escalation attempt
14:05:32	IAM Role Created	Wazuh	Malicious persistence
14:06:10	CloudTrail Logging Disabled	Wazuh	Attempt to evade detection
14:07:44	Lambda Function Deployed	Wazuh	Persistence mechanism installed
14:08:12	S3 Access Anomaly	Wazuh	Possible data exfiltration



Recommendations

The screenshot shows a Google Document titled "Untitled document - Google Docs". The left sidebar contains tabs for "Executive Summary", "Key Findings", "Blue Team Detections...", "Recommendations", and "Cloud Security Hardening...". The main content area displays several findings and their corresponding recommendations:

Issue	Recommendation
Public S3 Buckets	Enforce S3 Block Public Access settings
IAM Role Misuse	Apply least privilege + trust relationship validation
CloudTrail Modifications	Protect logging with SCPs and real-time alerts
Lambda Deployment Monitoring	Use EventBridge to alert on function creation

- **Briefing:** Draft a 100-word non-technical summary.

To put our cloud and endpoint protections to the test, we ran a simulated cyberattack. The red team got access through a phishing email, evaded security measures, and accessed critical data stored in the cloud.

While antivirus software did not detect the threat, our monitoring system (Wazuh) detected numerous critical behaviors, such as unauthorized access, strange behavior, and efforts to prevent logging.

The test exposed flaws in cloud settings, identity permissions, and endpoint security. As a result, we have identified critical enhancements to our detection, response, and overall security posture, allowing us to better fight against real-world cyber threats going forward.