PRACTICAL -9

Capstone — Full Adversary Simulation

Objective

Perform full APT-style attack lifecycle end-to-end.

Campaign Log

Phase	Action Performed	Tool	MITRE
Recon	S3 Enum	Pacu	T1580
Initial Access	Phishing	Evilginx2	T1566
C2	Beacon	Cobalt Strike	T1071
Exfiltration	Data Theft	AWS CLI	T1537

Blue Team Evidence

Timestamp	Alert	Severity	Coverage
2025-08-30 14:00	Suspicious Cloud Login	High	Partial

Final PTES Report:
I executed a full advanced adversary campaign covering reconnaissance, initial access, persistence, privilege escalation, C2 communication, and data exfiltration. Cloud misconfigurations enabled privilege escalation to full administrative access. An encrypted C2 channel enabled continuous control over compromised assets. Stealth exfiltration succeeded with minimal detection. Wazuh identified limited post-exploitation behaviors, but early-stage phishing and cloud exploitation went largely unnoticed. Improvements such as enhanced SIEM coverage, MFA enforcement, and better alert correlation are recommended. The exercise demonstrated organizational exposure to real-world APT-style attacks.