Operation Lazarus - Detailed Red Team Report

Operation Lazarus - Detailed Red Team Breach & Extraction Report

Objective:

Simulate a real-world adversarial red team attack focused on multi-stage exploitation, lateral movement, privilege escalation, persistence, and data exfiltration of Project Lazarus AI prototype.

Phase 1 - Reconnaissance and Vulnerability Discovery:

- Action: Nmap scan identified Apache 2.4.49 with CVE-2021-41773 vulnerability.

- Reason: Known path traversal and potential RCE vulnerability makes this a high-value entry point.

Phase 2 - Initial Exploitation:

- Action: Exploited Apache CVE-2021-41773 to access /etc/passwd.

- Outcome: Identified users 'alice' and 'bob', confirming valid targets.

- Reason: /etc/passwd helps enumerate users, potential privilege paths.

Phase 3 - Backdoor Setup and Privilege Mapping:

- Action: Scanned /home/bob/, discovered SSH keys, scripts, and 'notes.txt'.

- 'notes.txt' leaked Alice's password hint.

- Action: Inspected 'backup.sh' and 'cleanup.sh'.

- Finding: 'backup.sh' writable, runs as bob via cron. 'cleanup.sh' runs as root and cleans /tmp.

- Reason: Scripts often hide hardcoded credentials or exploitable logic.

Phase 4 - Privilege Escalation Planning:

- Action: Poisoned /tmp with a reverse shell payload targeting the root execution of cleanup.sh.

- Reason: cleanup.sh running as root allows for privilege escalation.

Phase 5 - Persistence Setup:

- Action: Modified 'backup.sh' to inject a persistent reverse shell.

- Reason: Guarantees future access via cron job.

Phase 6 - Lateral Movement and Data Collection:

- Action: SSH into Alice's account using leaked password 'redsky!123'.

- Action: Discovered 'project_lazarus_v1.py' (AI Prototype).

- Action: Located 'config.php' in /var/www/html/ revealing DB credentials.

- Reason: Target AI prototype and supporting infrastructure.

Phase 7 - Data Exfiltration:

- Action: SCP exfiltrated 'project_lazarus_v1.py'.

- Action: Extracted full MySQL database using dumped credentials.

- Reason: Capturing both intellectual property and operational data maximizes breach impact.

Phase 8 - Cleanup and Covering Tracks:

- Action: Wiped /var/log/syslog, auth.log, apache2 logs, and bash history.

- Reason: Avoid detection and forensic traceability.

Outcome:

- Full system compromise achieved.

- Root privilege obtained.

Operation Lazarus - Detailed Red Team Report

- Lazarus AI prototype and database exfiltrated.
- Persistence ensured via cron.

Key Lessons:

- Apache patch management is critical.
- Cron jobs remain underestimated for both persistence and escalation.
- Password hygiene failures lead to easy lateral movement.
- Logging and alerting are crucial to detect stealth attacks.

Mission Complete.