Operation Lazarus - Red Team Breach Report

Operation Lazarus - Red Team Breach & Extraction Report

Objective:

Simulate a red team operation to extract Project Lazarus and demonstrate real-world attack techniques.

Outcome:

Full network compromise, data exfiltration, persistence, and track wiping.

Technical Kill Chain:

- Recon: Nmap & Apache CVE-2021-41773
- Initial Access: Path traversal to /etc/passwd
- Lateral Movement: SSH access via leaked password
- Privilege Escalation: Cron job root shell via /tmp poisoning
- Persistence: Reverse shell in backup cron
- Data Exfiltration: Lazarus AI model, MySQL DB dump
- Cleanup: Logs and history wiped

Loot Summary:

- Lazarus AI prototype
- Full MySQL DB dump
- SSH private keys
- Alice's plaintext password

Key Lessons:

- Importance of patch management (Apache)

- Criticality of cron job review and securing /tmp

- Realistic persistence via cron

- Logging and auditing defenses are crucial

Mission Complete.