FORTRA®

RED TEAM USE CASE

Financial Institution

Background

A large financial institution conducts an assumed breach exercise to test its cybersecurity resilience. The Red Team is tasked with simulating an advanced persistent threat (APT) attack, while the Blue Team monitors, detects, and mitigates threats in real-time.

Phase 1: Initial Access Operations

The Red Team conducts reconnaissance on the Financial Institution's employees using open-source intelligence (OSINT). They identify a senior financial analyst, "John Doe," who frequently engages in industry webinars.

- **Spear Phishing Attack:** A well-crafted email mimicking an industry event invitation is sent to John. The email contains a malicious Microsoft Compiled HTML Help (CHM) generated with the Outflank Security Tooling's (OST's) In Phase Builder.
- **Payload Execution:** Once John clicks the link, a malicious payload executes, establishing an initial foothold through an encrypted reverse shell.

Phase 2: Lateral Movement & Credential Harvesting

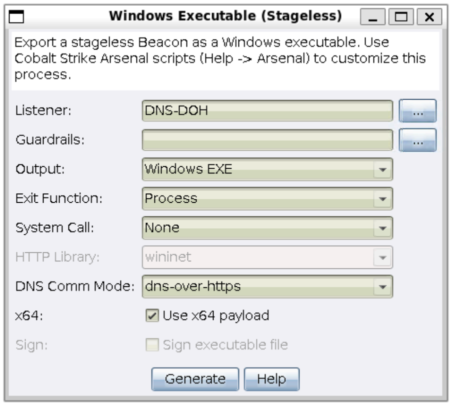
With initial access to John's workstation, the Red Team moves laterally within the financial institution's network:

- **Credential Harvesting:** They dump credentials from the memory using OST's Credential Pack and extract NTLM hashes from the workstation.
- **Privilege Escalation:** By exploiting a misconfigured service with SYSTEM privileges, they escalate privileges to domain administrator.

Phase 3: Maintaining Persistence

To ensure long-term access, the Red Team establishes multiple persistence mechanisms:

- **Quiet Transmission:** They configure C2 communication over HTTPS and DNS tunneling through Cobalt Strike, allowing them to bypass traditional network monitoring tools.
- **Asynchronous Communication:** A Beaconing mechanism is used to send periodic encrypted packets to evade detection.



Windows Executable (Stageless)

Export a stageless Beacon as a Windows executable. Use Cobalt Strike Arsenal scripts (Help -> Arsenal) to customize this process.

Listener: DNS-DOH

Guardrails:

Output: Windows EXE

Exit Function: Process

System Call: None

HTTP Library: wininet

DNS Comm Mode: dns-over-https

x64: ☑ Use x64 payload

Sign: □ Sign executable file

Phase 4: Actions on Targets

With initial access to John's workstation, the Red Team performs previously agreed actions within the financial institution's network:

- **Money Transfer:** Using Hidden Desktop, the Red team is able to launch the internal banking application from a compromised asset and proves that it is possible transfer money to an external account.

Phase 5: Red Team Engagement & Purple Teaming

The exercise involves real-time collaboration with the Financial Institution's security teams:

- **Shared Sessions:** The Red Team allows the Blue Team to observe certain attack techniques in real-time.
- **Extensive Logging:** All Red Team activities are logged for forensic analysis.
- **Purple Team Exercises:** The Red and Blue Teams analyze detections, fine-tune security tools, and improve response procedures.
- **Blue Team Training:** Defensive teams are trained to detect and mitigate similar real-world threats.

Outcome & Lessons Learned

- **Identified Gaps:** The exercise reveals weaknesses in the Financial Institution's email filtering, endpoint detection, and privilege management.
- **Security Enhancements:** Multi-factor authentication (MFA), stricter browser security policies, and improved lateral movement detection are implemented.
- **Continuous Improvement:** The organization adopts a proactive security strategy, conducting regular assumed breach exercises to stay ahead of emerging threats.

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.