FORTRA®

RED TEAM USE CASE

Government Agency

Background

A government agency responsible for critical public services commissions a Red Team engagement to assess its cybersecurity resilience. The exercise simulates an advanced persistent threat (APT) attack, testing the agency's ability to detect, respond to, and mitigate cyber threats targeting sensitive government data, public infrastructure, and national security.

Phase 1: Initial Access Operations

The Red Team begins by gathering intelligence on the government agency's employees, vendors, and internal systems.

- **Reconnaissance:** Open-source intelligence (OSINT) reveals outdated public-facing web servers and a cloud-based document-sharing portal used for inter-agency communication.
- **Spear Phishing Attack:** A well-crafted email impersonating a senior government official is sent to DPIS employees, containing a malicious attachment disguised as a policy update created using OST's Office Intrusion Pack.
- **Web Drive-By Attack:** The Red Team exploits an unpatched content management system (CMS) vulnerability on the agency's public website, embedding a JavaScript-based exploit that executes when employees visit the site.

Phase 2: Lateral Movement & Privilege Escalation

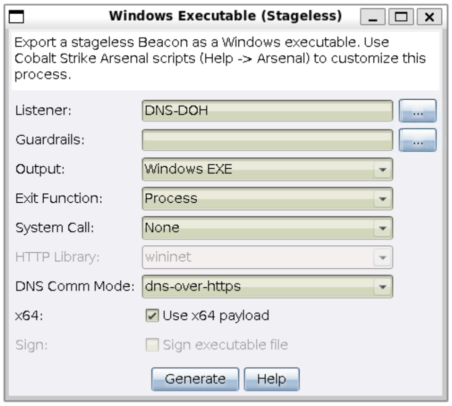
Once inside the government agency's network, the Red Team moves laterally to compromise additional systems:

- **Credential Harvesting:** Using tools from OST's Credential Pack, they extract hashed passwords from memory and perform Pass-the-Hash attacks to gain deeper access.
- **Privilege Escalation:** By exploiting an outdated endpoint security solution, they escalate privileges to administrator levels, gaining control over sensitive systems.

Phase 3: Maintaining Persistence & Evasion

To maintain access without detection, the Red Team deploys stealth techniques:

- **Quiet Transmission:** They use encrypted HTTPS and DNS tunneling to communicate with their Cobalt Strike command-and-control (C2) server.
- **Asynchronous Communication**: Malware beacons at random intervals to avoid detection by security monitoring tools.
- **Remote Access Trojans (RATs):** Custom backdoors are placed in critical systems, ensuring persistent access for future operations.



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: Simulated Attack Scenarios

The Red Team executes targeted attack simulations against government assets:

- **Data Exfiltration:** They extract classified documents, policy drafts, and sensitive citizen data to test the agency's ability to detect data breaches.
- **Critical Infrastructure Disruption:** They simulate an attack on the agency's SCADA (Supervisory Control and Data Acquisition) systems, demonstrating how adversaries could disrupt water supply or traffic control operations.
- **Disinformation & Insider Threat Simulation:** They fabricate fake internal memos and manipulate communication channels to test resilience against misinformation campaigns.

Phase 5: Red Team Engagement & Blue Team Training

The engagement involves continuous collaboration between Red and Blue Teams:

- **Shared Sessions:** The Blue Team is allowed to observe and analyze Red Team tactics in real time.
- Extensive Logging: Every attack vector is documented for forensic analysis.
- **Purple Team Exercises:** The Blue Team improves its detection capabilities based on Red Team findings.
- **Incident Response Drill:** The agency's security team practices containment, mitigation, and recovery strategies.

Outcome & Lessons Learned

- **Identified Weaknesses:** The exercise exposes vulnerabilities in third-party services, endpoint security, and insider threat detection.
- **Security Improvements:** The agency implements zero-trust architecture, network segmentation, and continuous security monitoring.
- **Enhanced Cyber Resilience:** The agency adopts a proactive security strategy, conducting regular Red Team engagements to safeguard national security assets.

This engagement highlights the importance of cybersecurity in protecting government infrastructure, sensitive data, and public services from advanced cyber threats.

Advanced Red Team Tools

Cobalt Strike and Outflank Security Tooling (OST) are two red teaming solutions that enable operators to execute the breadth of tasks that advanced red team engagements require. While both platforms operate as sophisticated standalone solutions, OST was developed to work in with Cobalt Strike, extending the capabilities of both tools.

Equip your red teamers with top-of-the-line toolkits.

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.