FORTRA

Red Team Operations Lifecycle

Step-by-Step using Cobalt Strike and OST

Table of Context

Pre-Engagement Preparation

Infrastructure Setup:

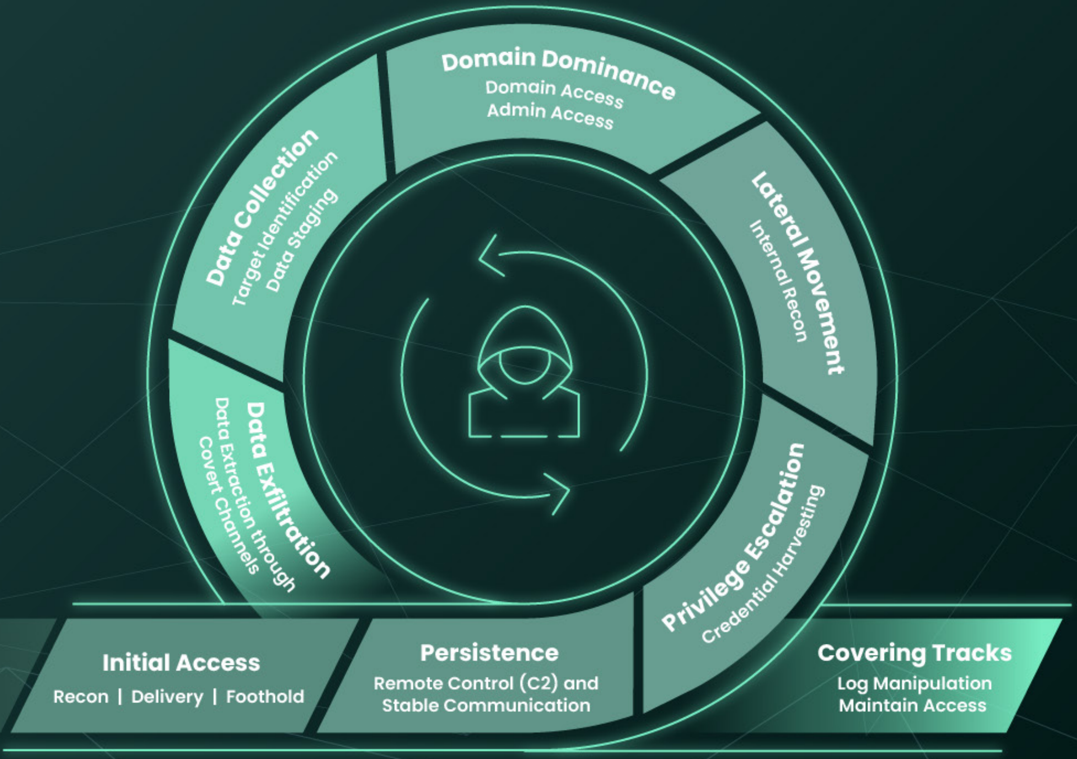
- Deploy team server on VPS with proper OPSEC
- Configure domain fronting or CDN for C2 infrastructure
- Create custom malleable C2 profile mimicking legitimate traffic (Office365, Google, etc.)
- Set up redirectors to obscure team server location
- Prepare phishing infrastructure (domains, email accounts)

Payload Preparation:

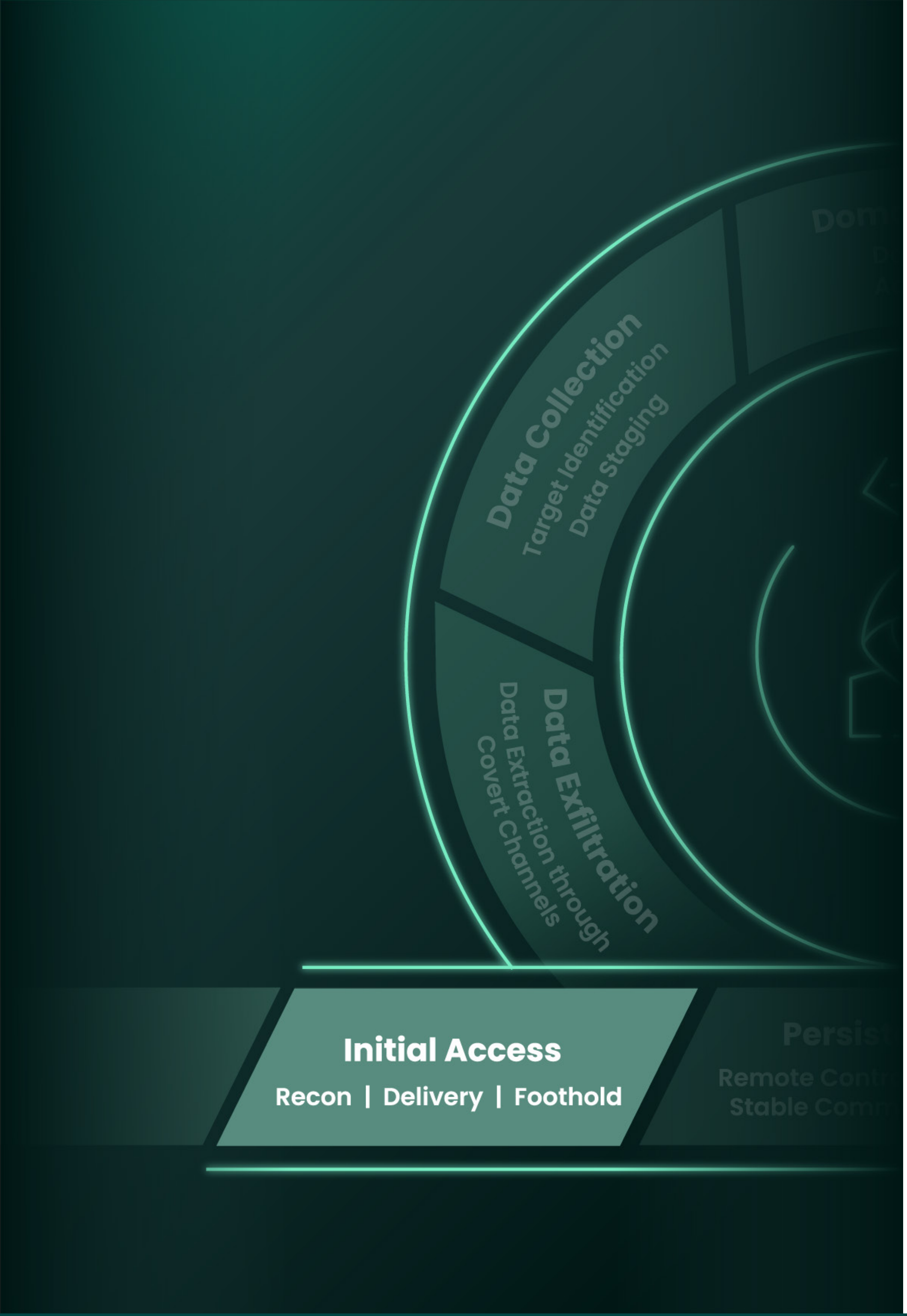
- Generate Cobalt Strike raw beacon payloads
- Use Outflank's Beacon Booster tool for enhanced evasion.
- Consider using the In-Phase builder to generate the phishing artifacts.
- Test against target's known security products in isolated environment
- Prepare multiple delivery methods
  (macros, HTA, shortcut files, DLL side-loading)
- Create decoy documents relevant to target organization
- Obfuscate payloads to evade signature-based detection

FORTRA

Red Team Operations Lifecycle



This section outlines critical practices and tools that enable a red team to operate covertly, maintain persistence, and deliver actionable insights without tipping off the target.



Lifecycle Phases

Phase 1: Initial Access

Reconnaissance

- Gather OSINT on target organization
- Identify key personnel for spear-phishing
- Map external attack surface (email servers, VPN, web applications)
- Enumerate publicly exposed systems and services

Delivery

- Craft convincing spear-phishing emails with pretext
- Attach weaponized documents containing Cobalt Strike payload
- Alternative vectors: LinkedIn messages with malicious links, compromised vendor accounts
- Monitor for beacon callbacks on team server

Establishing Foothold

- Receive initial beacon callback
- Verify connection and system information
- Assess security posture (AV/EDR running, logging levels)
- Establish secondary C2 channel as backup

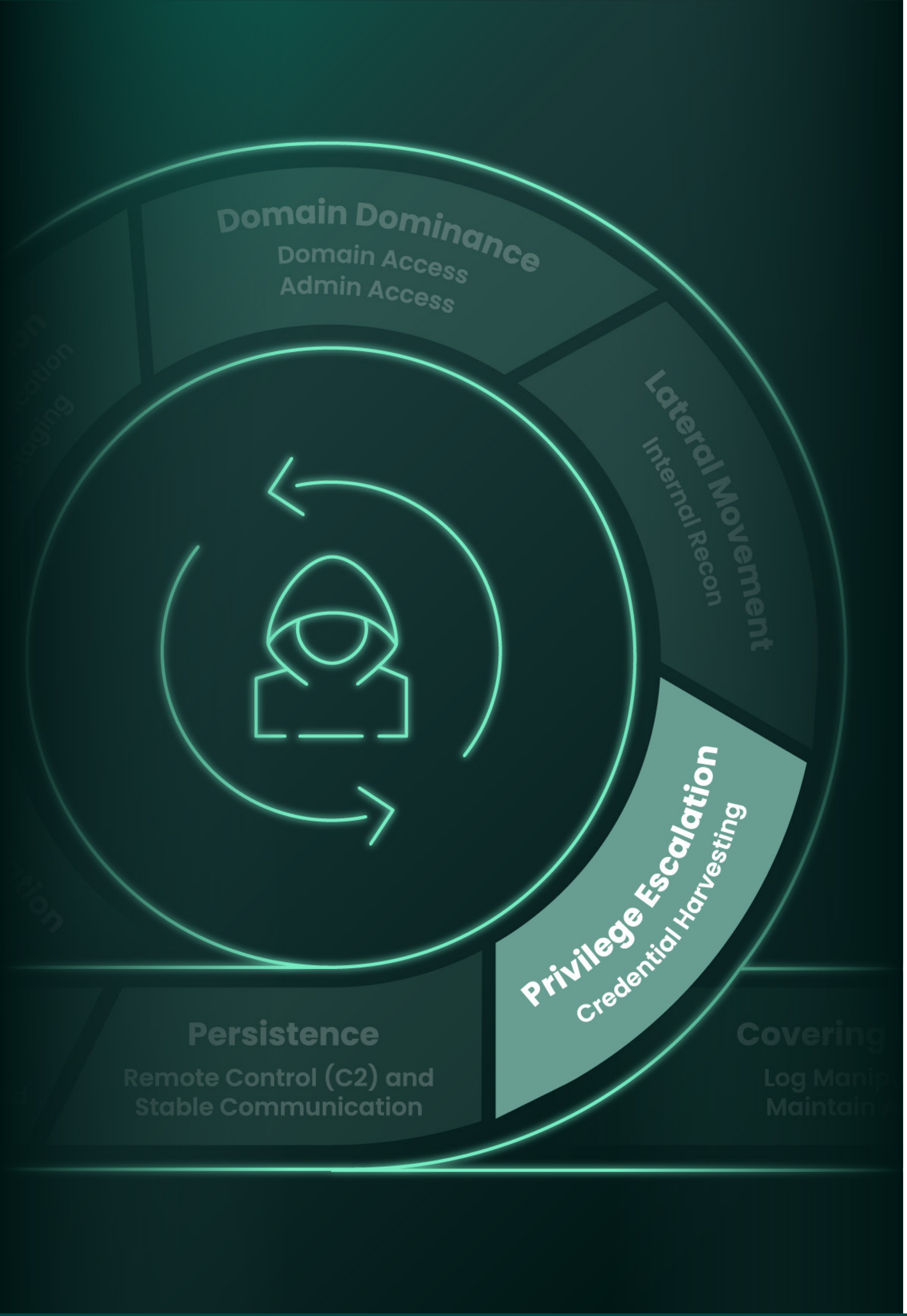
Phase 2: Persistence

Immediate Actions

- Migrate beacon to more stable process (explorer.exe, svchost.exe)
- Use Outflank's process injection techniques for evasion:
- Create persistence mechanism:
- Registry run keys
- Scheduled tasks
- WMI event subscriptions
- Service creation
- Use Outflank's Sideload Trigger to find DLL hijacking candidates
- Test persistence

Beacon Management

- Configure appropriate sleep/jitter times based on environment
- Use SMB beacons for internal pivoting (no direct internet connection)
- Deploy multiple persistence methods across different systems



Phase 3: Privilege Escalation

Local Privilege Escalation

- Identify exploitable services, misconfigurations
- Exploit kernel vulnerabilities if necessary
- Use elevate commands in Cobalt Strike (UAC bypass, exploit modules)

Credential Harvesting

- Use Outflank's credential pack:
  - DumpertNG for advanced LSASS dumping using process snapshot technique
  - KernelKatz for credential extraction by leveraging a kernel driver.
- Extract credentials from memory, registry, files
- Capture password hashes for pass-the-hash attacks
- Keylog high-value targets to capture credentials
- Search for credentials in files, scripts, configuration files

Domain Dominance
Domain Access
Admin Access
Lateral Movement
Internal Recon
Privilege Escalation
Credential Harvesting
Persistence
Remote Control (C2) and
Stable Communication
Covering
Log Mani
Maintain

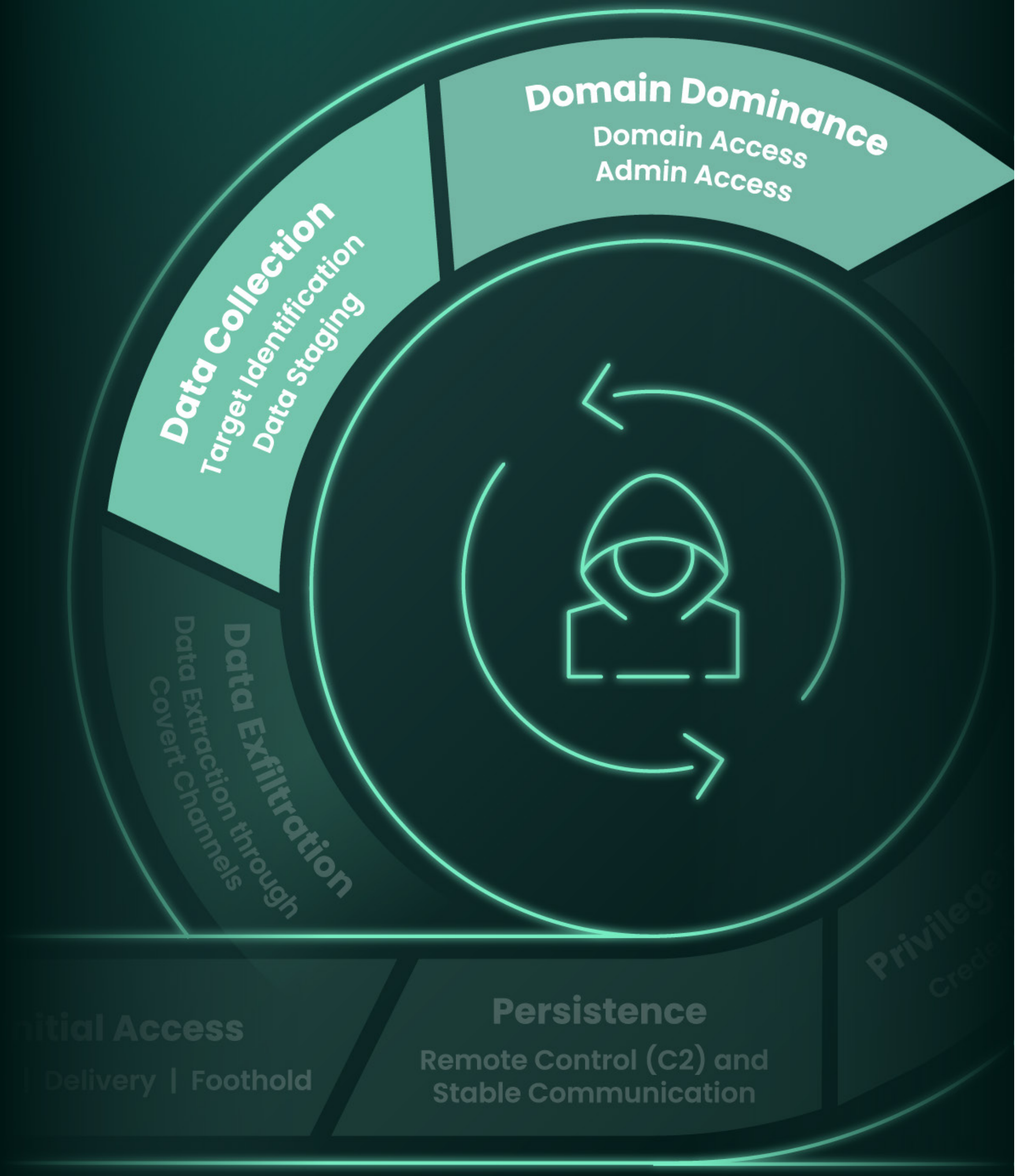
Phase 4: Lateral Movement

Internal Reconnaissance

- Enumerate domain users, groups, computers
- Identify domain admins and privileged accounts
- Map network topology and trust relationships
- Locate high-value targets (file servers, databases, domain controllers)

Movement Techniques

- Use pass-the-hash with captured NTLM hashes
- Pass-the-ticket with Kerberos tickets
- PSExec to deploy beacons on remote systems
- RDP with stolen credentials for interactive access
- Abuse SMB to deploy beacons through named pipes
- Use Outflank's Shovel NG.
- Beacon Deployment
- Deploy beacons on newly compromised systems
- Chain beacons through pivoting for segmented networks
- Maintain access to multiple systems for redundancy



Phase 5: Domain Dominance

Domain Controller Compromise

- Target domain controller systems
- Extract domain credentials using Outflank's Credential Pack
- Create Golden/Silver tickets for persistent domain access

Administrative Access

- Compromise domain admin accounts
- Add backdoor accounts to privileged groups
- Deploy beacons on critical infrastructure
- Establish multiple persistence mechanisms at domain level

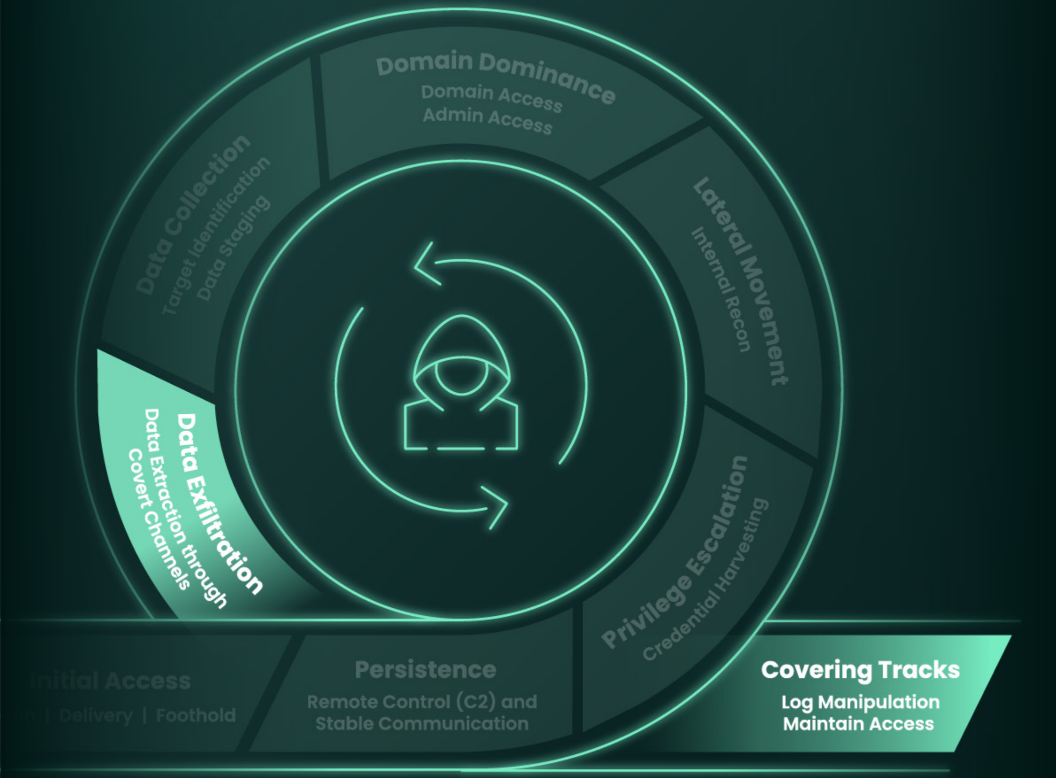
Phase 6: Data Collection

Target Identification

- Locate sensitive data repositories
- Identify databases, file shares, SharePoint sites
- Search for documents containing sensitive keywords
- Access email servers and archives

Data Staging

- Download target files to compromised systems
- Compress and encrypt data for exfiltration
- Stage data in obscure locations
- Use Cobalt Strike's file browser to navigate and download



Phase 7: Data Exfiltration

Covert Channels

- Exfiltrate via HTTPS C2 channel (blends with normal traffic)
- Use DNS tunneling for highly restricted networks
- Stage data on cloud storage (OneDrive, Dropbox) using legitimate accounts
- Upload to external servers via encrypted connections

Phase 8: Covering Tracks

Log Manipulation

- Clear relevant Windows Event Logs
- Remove artifacts from compromised systems
- Delete staged files and tools
- Sanitize command history

Maintaining Access

- Keep selective persistence mechanisms active
- Use stealthy communication profiles
- Prepare for blue team response and maintain access despite remediation attempts

Operational Security Considerations for a Successful Red Team Lifecycle

This section outlines critical practices and tools that enable a red team to operate covertly, maintain persistence, and deliver actionable insights without tipping off the target.

	In Operation/Pre Operation	Post Operation
Communication	**Communication Discipline** • Use malleable C2 profiles that mimic legitimate traffic • Randomize beacon callbacks with sleep/jitter • Avoid patterns in C2 communication • Use domain fronting or CDN to obscure C2 infrastructure	**Cleanup Coordination** • Provide list of all compromised systems • Document all persistence mechanisms for removal • Share IOCs generated during operation • Remove beacons and artifacts • Restore any modified configurations • Remove an y Outflank tooling artifacts
Documentation	**Maintain Operation** • Document all compromised systems • Record credentials obtained • Track lateral movement path • Note detection events • Screenshot critical achievements • Time-stamp all activities	**Report Preparation** • Create detailed attack path diagram • Document techniques that succeeded/failed • List credentials compromised • Identify detection gaps • Provided timeline of activities • Include recommendations from operator perspective • Document effectiveness of Outflank evasion techniques vs. targets security stack
Techniques	**Evasion Techniques** • process injections into trusted processes • Execute in memory (fileless) • Use living-off-the-land binaries (LOLBins) • Avoid dropping files to disk when possible • Disable command logging in Cobalt Strike • Integrate Outflank Security Tooling for advanced evasion • Watch for signs of detection (antivirus alerts, beacons dying) • Monitor target's security blog/Twitter for incident response activity • Adjust TTPs if detection occurs • Have contingency plan for burned infrastructure	**Evidence Collection** • screenshot domain admin access • Document path to domain controller • Capture proof of sensitive data access • Record all persistence mechanisms deployed • Log all systems with active beacons

Key Outflank Tools for Cobalt Strike Operations

C2-Tool-Collection

- In-Phase Builder: Initial payload stager
- Custom process injection techniques

Credential Access

- DumpertNG
- KernelKatz: Alternative credential extraction method

Execution & Evasion

- Beacon Object Files (BOFs): In-process execution without spawning
- Sharpfuscator: Obfuscate .NET tools to improve in-memory evasion
- AceLdr: Custom reflective loader for enhanced evasion
- Post-Exploitation
- Credential Pack: Stealthy credential harvesting
- Multiple lateral movement Tools
- Custom Kerberos abuse tools

Benefits of Integration

- Significantly reduced detection rates
- Bypass modern EDR solutions
- Minimize forensic artifacts
- Execute without spawning suspicious processes
- Evade memory scanning and behavioral detection

Assumptions and Operational Philosophy for Successful Red Teaming:

- Signed legal authorization from executive leadership
- Defined scope and boundaries of testing
- Rules of engagement documented and approved
- Emergency contact procedures established
- Coordination points with blue team leadership (if applicable)
- Data handling agreements for any information accessed
- Stealth over speed: Prioritize remaining undetected to test detection capabilities fully
- Realistic simulation: Use TTPs that mirror actual adversary behavior
- Objective-driven: Focus on achieving specific goals (domain compromise, data access, etc.)
- Thorough documentation: Maintain detailed logs for post-engagement reporting
- Ethical boundaries: Operate within scope and avoid causing actual harm
- Continuous adaptation: Adjust tactics based on defensive responses

FORTRA®

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.