FORTRA®

OFFENSIVE SECURITY

Red Team & Penetration Testing Tools

COBALT STRIKE

Cobalt Strike enables advanced adversary tactics for Red Team operations. Key Capabilities include advanced post-exploitation, flexible framework, community-driven extensions & team-based ops.

OUTFLANK (OST)

OST provides a broad arsenal for evasive attack simulation. Engineered by active practitioners, key features include advanced evasive movement, multi-phase tools, rapid expansion and more.

CORE IMPACT

Core Impact tests exploitation paths and lateral movement across networks, applications and endpoints with automated exploitation capabilities.

IMPACKET

Impacket is an open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.

Empower your team with interoperable tools that efficiently test defenses, validate exploitability, and emulate sophisticated attacks even in mature, high-security environments.

FORTRA'S OFFENSIVE SECURITY

Industry Leading Red Team and Penetration Testing Tools

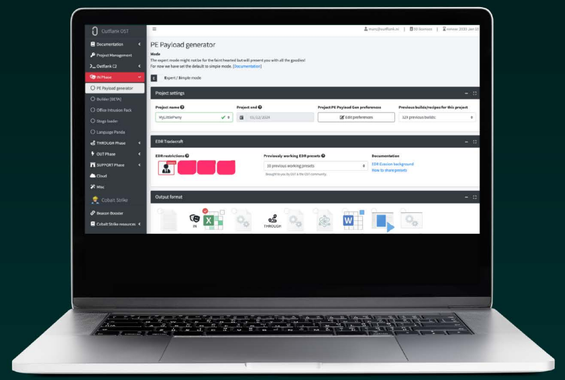
COBALT STRIKE

Advanced Post-Exploitation: Deploy Beacon, Cobalt Strike's signature payload, to gather information, execute commands, move laterally, elevate privileges, and more.

Flexible Framework: Customize operations using malleable C2 profiles, UDRLs, sleep masks, and tailored scripts to mimic advanced attackers.

Community-Driven Extensions: Leverage 100+ user-developed tools from a curated library, including custom BOFs, aggressor scripts, and post-exploitation modules.

Team-Based Operations: Coordinate red team activities through team servers with shared access to compromised systems and collected data.



OUTFLANK (OST)

Advanced Evasive Movement: Avoid detection using the most up-to-date research and technology for bypassing defensive measures and solutions like EDR and antivirus.

Multi-phase Tools: Accelerate operations through purpose built tools for access, evasion, and covert lateral movement.

Rapid Expansion: Take advantage of cutting-edge techniques, as OST continuously evolves through expert driven research and regular tool releases.

Tradecraft and Community: Get exclusive access to regular tradecraft sessions and a forum for OST users to discuss attack strategies and methodologies.

CORE IMPACT

Exclusive Crafted Exploits: Leverage an expert-validated exploit library that is regularly tested and updated for modern platforms and **applications.**

NTLM Relay Attacks: Trigger system authentication with Coercer module, then use NTLMrelayx to redirect connections for automated agent deployment, certificate generation, LDAP queries, and more.

Ransomware Simulation: Evaluate security controls by paring phishing capabilities with the ransomware simulator, which mimics multiple ransomware families to encrypt files.

Compliance Documentation: Generate detailed technical reports to help plan remediation and prove adherence to industry requirements and government regulations, like PCI DSS, GDPR, HIPAA.

IMPACKET

Protocol Library: Examples of python classes for low-level programmatic access to packets and for protocols like SMB, RDP, LDAP, and more.

Ready to use scripts: Pre-built scripts like psexec.py, wmiexec.py, and secretsdump.py can be used for common attack scenarios like remote execution.

Authentication Mechanisms: Test authentication scenarios with credential handling methods like Pass-the-Hash, Pass-the-Ticket, and relay attacks.

Extensible framework: Designed to be the base for unique tools for customized attack techniques that can be used for a broad range of offensive objectives.

fortra.com/offsec