FORTRA™

DATASHEET (OFFENSIVE SECURITY)

Advanced Red Team Bundle – Core Impact, Cobalt Strike, and Outflank Security Tooling (OST)

Core Impact, Cobalt Strike, and Outflank Security Tooling (OST) are three powerful security solutions that use the same techniques as today's threat actors in order to safely evaluate organizational infrastructures and provide guidance on closing security gaps, enhancing defenses, and creating more resilient security strategies.

Core Impact is an automated penetration testing tool, typically used for exploitation and lateral movements in various environments. Cobalt Strike replicates the tactics of a long-term embedded actor, using a post-exploitation agent and covert channels to emulate advanced threats. OST covers every step in the attacker kill chain with a curated set of offensive security tools for red teams.

Core Impact, Cobalt Strike, and OST can be bundled together for a reduced price, enabling organizations to rapidly mature their security assessments with complementary solutions that interoperate with one another. This overview provides details on the key functionalities of each of these solutions and how they can be used together to amplify your testing efforts.

Core Impact

Core Impact is a versatile penetration testing tool that targets vulnerabilities in different vectors across an IT infrastructure, including networks, people, web applications, endpoints, Wi-Fi, and SCADA environments. Newer pen testers can get up to speed with automated testing capabilities, while advanced testers can increase efficiency and output by automating routine and repetitive tasks. Key features include:

Rapid Multi-Vector Tests

Step-by-step Rapid Penetration Tests (RPTs) exploit vulnerabilities with network, web application, and client-side tests. Defensive controls are put to the test to effectively prioritize the risks that most endanger mission-critical systems and assets.

Core Certified Exploits

The certified exploit library is carefully maintained by experts who develop and thoroughly test exploits, regularly making updates and additions of new exploits for different platforms, operating systems, and applications.

Self-Terminating Agents

Core Agents enable testers to maintain full control while simplifying interaction. These binary implants are injected into the memory or file system of a targeted or compromised remote host and come equipped with self-destruct capabilities so no lingering agents remain, ensuring no backdoors are left behind after an engagement ends.

Remediation Validation

Previous testing sessions are stored, allowing testers to recreate the same attack path and redeploy the same agents in order to confirm whether patches or compensating controls were effectively implemented.

Reporting

Testing activity is carefully tracked and logged and data can be populated into intuitive reporting templates to help provide guidance for remediation and prove adherence to industry requirements and government regulations.

Cobalt Strike

Cobalt Strike is a threat emulation tool that can be used to replicate scenarios in which a highly skilled attacker is embedded in an IT infrastructure. With a powerful post-exploitation agent and a flexible command and control framework, Cobalt Strike can be extended and tailored to suit the needs of any red team engagement. Key features include:

Post-Exploitation Agent

Beacon is Cobalt Strike's signature post-exploitation payload that can be used to perform the same tactics as an advanced actor in order to move laterally, escalate privileges, exfiltrate data, achieve persistence, and more. Actions include execution of PowerShell scripts, keystroke logging, taking screenshots, downloading files, and spawning other payloads.

Covert Communication

Beacon uses an asynchronous "low and slow" communication pattern to attract minimal attention during engagements. Additionally, Beacon's adaptable Command and Control language, Malleable C2, can be used to alter network indicators to blend in with normal traffic or cloak its activities by emulating different types of malware.

Attack Packages

Attacks can be designed using one of Cobalt Strike's numerous packages, like web drive-by attacks with java applets or website clones. Modify a benign file into a trojan horse using Microsoft Office Macros or Windows Executables. Get around two-factor authentication and target sites using a man-in-the-browser attack that will hijack a compromised user's authenticated web sessions with a proxy server to inherit cookies, authenticated HTTP sessions, and client SSL certificates

Flexible Framework

Cobalt Strike can be easily extended in numerous ways. Users can use Aggressor Script to modify or write their own built-in scripts, create their own Beacon Object File (BOF) to expand Beacon's post-exploitation capabilities, or make and use tools from the Community Kit, a central repository for projects from the user community.

OST

OST is a toolkit for red teamers by red teamers, built for performing in mature and sensitive target environments to efficiently simulate evasive techniques currently used by APTs and other cyber attackers. Key features include:

Evasive Movement

OST tools focus on avoiding detection, using the most up-to-date research and technology to bypassing defensive measures and solutions like EDR and antivirus. For example, tools like Sharpfuscator utilize obfuscation to compile C# repositories, Payload Generator deploys anti-forensic features to help evade antivirus and EDR solutions, and KernelKatz abusees vulnerable kernel drivers to gather credentials information straight from the LSASS memory. To maximize red team engagements, OST tools utilize unique techniques and capabilities unseen in any other solutions or services.

Tools for Every Attack Stage

OST addresses every aspect of an attack with multiple tools, providing shortcuts and simplifying even initial access, EDR evasion and OPSEC-safe lateral movement. For example, breaching an environment can be achieved by with the Office Intrusion Pack, which allows teams to phish with MS Office documents by utilizing high quality offensive macros. Teams can then move laterally with Lateral Pack, extract credentials with Credential Pack, or escalate privileges with DLL Hijack Library. HiddenDesktop is ideal for post-exploitation actions, as it grants stealthy yet fully interactive interaction on a target desktop including client applications, active cookies of the target user and connected hardware tokens.

Continuous Evolution

The OST toolkit is constantly expanding, with highly experienced security professionals regularly adding new tools that incorporate the latest offensive techniques. In addition to expert research and development, the OST team also creates and manages extensive documentation to ensure easy and efficient implementation.

Knowledge Sharing and Community

Exclusive access to the OST community provides a forum for likeminded red teaming professionals to discuss the latest research and strategize approaches for red teaming attacks. Knowledge sharing sessions are regularly held to explore and expand on relevant topics such as EDR evasion.

Layering Security: Integration and Interoperability

Not only do these tools work well individually, together they build on one another to create a holistic security testing methodology that can proactively reduce risk. They also provide countless opportunities for interoperability and integration.

All three of these tools can interact with one another during engagements using session passing and tunneling capabilities. For example, initial access may be achieved in Core Impact with Beacon then spawned to continue post-exploitation in Cobalt Strike. Alternately, OST's Stage 1 implant can be used to disable defensive systems, then passed to Cobalt Strike to escalate privileges, download files, and more.

Core Impact and Cobalt Strike can share resources, including modules and extensions like Beacon Object Files (BOFs). Cobalt Strike and OST are also closely aligned, with many features that extend the reach of both tools. For example, those with the Advanced Red Team Bundle can enrich the evasiveness of their Cobalt Strike payloads using Payload Generator's obfuscation methods. OST was explicitly developed to work in tandem with Cobalt Strike, with multiple tools integrating seamlessly into the C2 framework through Beacon Object Files (BOFs) and reflective DLL loading techniques.

The Advanced Red Team Bundle also provides the advantage of having a single point of contact for a robust portfolio of offensive solutions. It is especially advantageous to choose multiple solutions under a single umbrella like Fortra. You can not only benefit from the centralization and reduced console fatigue these integration and interoperability features provide, you will also enjoy the efficiency of having the same best-in-class sales and technical support across solutions.

Ready to Combine Core Impact, Cobalt Strike, and OST?

Reach out to one of our experts for pricing information and to find out more about how our Advanced Red Team bundle offering will benefit your organization.

REQUEST A QUOTE

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.