FORTRA

DATASHEET *(Cybersecurity)*

Offensive Security-Advanced Bundle

Core Impact and Cobalt Strike

Core Impact and Cobalt Strike are two powerful tools that help organizations assess the security of their environments. Though they share the same goal of providing insights to help bolster security efforts, they are otherwise distinct tools with unique features.

Core Impact is a penetration testing tool, primarily used for exploitation and lateral movements in various environments. Cobalt Strike, on the other hand, is threat emulation software, primarily used to simulate adversarial post-exploitation scenarios, and to support Red Team operations.

While these tools have clear differences, they are still both tools used for evaluating cybersecurity, so there are understandably a few key features that overlap. However, even these overlapping features have their own distinctions within each tool. This document provides an overview of the key functionalities of each of these tools, their similarities, and how they can be used together to amplify your security testing efforts.

Core Impact

Exploitation of Multiple Vectors:

Core Impact is an easy-to-use penetration testing tool that exploits security weaknesses associated with networks, people, web applications, endpoints, Wi-Fi, and SCADA environments. It expands the capabilities and productivity of pen testers, and automates repetitive and time consuming exploitation tasks.

Core Certified Exploits:

Core Security experts carefully develop and thoroughly test exploits, regularly updating and adding new exploits to Core Impact for different platforms, operating systems, and applications. In order to create the most comprehensive and trustworthy exploit library on the market, we work with third-party cybersecurity vendors to provide specialized exploit packs for various environments. Users can also import their own exploits.

Powerful Encryption:

Core Impact utilizes robust cryptography to fully encrypt the keys used to protect the command and control communicationsbetween agents and/or workspaces.

Watermarked, Self-Terminating Agents:

Each build of Core Impact is unique and includes a watermark to aid in the identification of each distribution, and all agents deployed from it. This watermark provides forensic confirmation that these are legitimate testing agents and not from a malicious source. Additionally, all agents deployed from Core Impact are set to self-terminate, ensuring that no potential backdoors are left behind.

Remediation Validation:

Core Impact stores previous testing sessions, which can be quickly and easily rerun in order to validate that remediation efforts, such as new compensating controls, are effective.

Integrations:

Core Impact users can import third-party scanner data, and automatically validate vulnerabilities identified within those scans to provide a prioritized list of potential targets to test. Integrations with other pen testing tools like Metasploit, PowerShell Empire, and Plextrac further centralize testing environments.

Cobalt Strike

Reconnaissance for Client-Side Attacks:

Cobalt Strike's system profiler maps a target's client-side interface your target uses, gathering a list of applications and plugins it discovers through the user's browser, as well as Internal IP address of users who are behind a proxy server.

Post-Exploitation:

Beacon is Cobalt Strike's post-exploitation payload to model an advanced actor. Beacon executes PowerShell scripts, logs keystrokes, takes screenshots, downloads files, and spawns other payloads.

Covert Communication:

Beacon's network indicators are malleable, using asynchronous "low and slow" communication pattern. Load a C2 profile to look like another actor. Use HTTP, HTTPS, and DNS to egress a network and resist blocking. Use named pipes to control Beacons, peer-topeer, over the SMB protocol.

Attack Packages:

Use Cobalt Strike to host a web drive-by attack using java applets or website clones. Transform an innocent file into a trojan horse using Microsoft Office Macros, or Windows Executables.

Browser Pivoting:

Use a browser pivot to go around two-factor authentication and access sites as your target. This man-in-the-browser attack will hijack a compromised user's authenticated web sessions with a proxy server that injects into 32-bit and 64-bit Internet Explorer. Use the proxy server to inherit cookies, authenticated HTTP sessions, and client SSL certificates.

Core Impact and Cobalt Strike Similarities

Real Time Collaboration:

With Core Impact, multiple security testers have the capability to interact in the same session, giving teams the ability to securely share data and delegate testing tasks. These shared workspaces provide a common view of discovered and compromised network targets for optimal collaboration.

Cobalt Strike users can connect to a team server to share data, communicate in realtime, and control systems compromised during the engagement.

Ransomware & Phishing Simulations:

Core Impact's social engineering capabilities can be used with its ransomware simulator to assess security awareness, identifying who is susceptible to such attacks. Using a phishing campaign for deployment, the behavior of multiple ransomware families can be imitated to, harvest credentials, encrypt data, and exfiltrate files.

Cobalt Strike allows you to import an existing email or write your own to create a targeted phishing template. It will then strip attachments, deal with encoding issues, and rewrite each template for each phishing attack. Cobalt Strike will then send the email and track who clicks.

Comprehensive Reporting:

Core Impact tracks and logs all actions taken during a testing session, including actions taken on remote hosts. Users can then leverage the simple and intuitive reporting templates to auto-populate pertinent data from the logs.

Cobalt Strike logs all of its activity on the team server. Reports can then be generated to provide a timeline and a list of indicators of compromise determined from red team activity.

Interoperability

Those with both tools can take advantage of session passing and tunneling capabilities between Core Impact and Cobalt Strike. This interoperability can streamline pen testing efforts even further. For example, users can start their engagement, getting initial access from Core Impact. From there, they can continue with post-exploitation activities by spawning a Cobalt Strike Beacon.

These tools can share resources, such as .NET assembly tools and other modules. Core Impact also fully supports the Cobalt Strike BOF API, allowing Core Impact users to also be able to benefit from Community Kit extensions. Additionally, any of Core Impact's library of certified exploits can be launched directly through Beacon.

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.