

Offensive Security-Elite Bundle

Frontline VM, Core Impact, & Cobalt Strike

[Frontline Vulnerability Manager](#) (Frontline VM™), [Core Impact](#), and [Cobalt Strike](#) are three powerful security testing tools that evaluate the security of their environments in order to better identify security vulnerabilities and predict their potential impact. Though they all share the same goal of proactively assessing risk, they are still distinct tools with distinguishing features that establish their own unique position in a vulnerability management program.

Frontline VM is a SaaS vulnerability management solution, mostly used for performing intelligent network scanning. Core Impact is a penetration testing tool, typically used for exploitation and lateral movements in various environments. Lastly, Cobalt Strike is threat emulation software, primarily used to simulate adversarial post-exploitation scenarios, and to support Red Teams operations.

This document provides an overview of the key functionalities of each of these tools and how they can be used together to amplify your security testing efforts.

Frontline Vulnerability Manager

Frontline VM is a cloud-native, vulnerability management SaaS solution that can perform comprehensive network security assessments which include risk prioritization, tracking, and remediation guidance. Key features include:

Intelligent Scanning

With both external data and proprietary technology, you can use Frontline VM to perform automated scans for vulnerability discovery, identification, and remediation management. Get a full overview of your environment's health and track your progress using a dashboard created using data aggregated from different scans.

Compliance Auditing

Run the Center for Internet Security (CIS) Benchmark scan to help determine whether your organization is adhering to compliance regulations and best practices pertinent to your industry.

User Accountability

Maintain security best practices using role-based access control and data segmentation to only give users the access relevant to their position.

Reporting

Select a report type using the template library and use all the available filters to tailor and build a report that provides all the information you're looking for.

Core Impact

Core Impact is a 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. Key features include:

Rapid Pen Tests

Use step-by-step [Rapid Penetration Tests](#) (RPTs) to discover, test, and report all in one place, optimizing the use of your security resources.

Core Certified Exploits

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

Clean-Up

Use Core Agents, binary implants injected into the memory or file system of a targeted or compromised remote host, to maintain full control while simplifying interaction. With programmable self-destruct capabilities for agents, you can ensure no agent is left behind after testing to drain resources or be used as a potential backdoor for attackers.

Reporting

Generate consistent, thorough recording of engagements to plan and prioritize remediation efforts and prove compliance for regulations like [PCI DSS](#), GDPR, and HIPAA.

Cobalt Strike

Cobalt Strike is a threat emulation tool that provides a post-exploitation agent and covert channels, replicating the tactics and techniques of an advanced adversary in a network. Key features include:

Reconnaissance for Client-Side Attacks

With Cobalt Strike's system profiler, you can map a target's client-side interface and gather a list of relevant applications and plugins.

Post-Exploitation Agent

Use Beacon, Cobalt Strike's post-exploitation payload, to simulate the same actions as an advanced actor, including execution of PowerShell scripts, keystroke logging, taking screenshots, downloading files, and spawning other payloads.

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. Get around two-factor authentication and access sites as your target using a man-in-the-browser attack that can hijack a compromised user's authenticated web sessions with a proxy server.

Flexible Framework

Mold Cobalt Strike into a tool that suits your needs, with tailored scripts, adjustable attack kits, and the Community Kit with user-created extensions.

Layering Security: Integration and Interoperability

While these solutions are valuable individually, together these tools build on one another to create a mature vulnerability management program that provides full coverage to proactively reduce risk. Frontline VM gives the necessary context to dismiss innocuous vulnerabilities and focus on those that pose a real threat. Core Impact then further prioritizes risks and guides remediation by discerning how much access could be gained and what damage could result if a vulnerability is exploited. Finally, Cobalt Strike enables a full attacks simulation to put defenses and security operations to the test.

These three solutions not only work in tandem, they can also work together. Core Impact can directly import scan results from Frontline VM for use in information gathering and to validate vulnerabilities. Additionally, Core Impact and Cobalt Strike are interoperable. Users with both tools can take advantage of session passing and tunneling capabilities. They can also share resources, including modules and extensions.

Staying ahead of attackers involves taking a proactive approach to cybersecurity and assembling a layered portfolio of offensive solutions. It is especially advantageous to choose multiple solutions under a single umbrella like HelpSystems. 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.

digitaldefense
by HelpSystems

www.digitaldefense.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.