coresecurity
by HelpSystems

DATASHEET *(Cybersecurity)*

CORE IMPACT

Simple enough for your first test, powerful enough for the rest

Core Impact is a comprehensive penetration testing platform that safely and efficiently replicates attacks and uncovers security weaknesses. Organizations can maximize their resources with certified exploits and guided automations, providing valuable insights that will help mitigate risk and protect critical assets.

Conduct pen tests in just a few simple steps

Core Impact streamlines testing by providing step-by-step wizards and rapid penetration tests so users can discover, test, and report in just a few simple steps.

Leverage a robust library of Core Certified exploits

Using a stable, up-to-date library of commercial-grade exploits, Core Impact reveals how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and assets.

Centralize your pen testing toolkit

Gather information, exploit systems, and generate reports, all in one place. Every phase of the penetration test process can be executed and managed from a single console. Users can choose a vector to test, select or create different modules, and view data obtained from agents deployed across multiple targets.

An intuitive dashboard allows users to easily open new workspaces and tests, view the latest available exploits, and launch remediation validations. Reports can also be created from the dashboard, including those on network hosts, discovered identities, and phishing simulation results, as well as full executive summaries.

PRODUCT SUMMARY

KEY FEATURES

- Intuitive wizards for deploying professional level tests
- Extensive and reliable library of certified exploits
- Multi-vector testing capabilities
- Teaming capabilities in a collaborative workspace
- Tailored reporting to build remediation plans
- Powerful integrations with other pen testing tools and more than 20 vulnerability scanners
- Robust safety features, including fully encrypted, self-destructing agents

PLATFORMS MONITORED

- Operating Systems including Windows, Linux, and Mac
- Cloud (Public, Private, Hybrid)
- Databases
- Web Services
- Network Appliances
- Software Applications
- Your Critical Data

SYSTEM REQUIREMENTS

- Windows 10 Enterprise 64 bit
- Windows 10 Pro 64 bit
- Windows Server 2016 Standard

Common Core Impact Use Cases

Core Impact offers diverse testing functionality in order to provide thorough coverage and security insights so organizations know who, how, and what is vulnerable in their IT environments.

Automate the Routine

Users can efficiently execute common tasks, saving time while providing a consistent, repeatable process for their testing infrastructure. Additionally, Core Impact allows you to quickly re-test exploited systems to verify that remediation measures or compensating controls are effective and working.

Proving Compliance with Industry Regulations

Multiple regulations require organizations have regular assessments of their security infrastructure to ensure sensitive data is properly protected. Core Impact provides an easy to follow and established automated framework that can support industry requirements and standards, including PCI-DSS, CMMC, GDPR, and NIST.

Conduct Network and Web Application Tests

Accurately identify and target internal information systems for network penetration testing. Core Impact can help exploit vulnerabilities in critical networks, systems, hosts, and devices by imitating an attacker's methods of access and manipulating data, as well as testing defensive technologies' ability to stop attacks.

Run web application penetration tests to find weaknesses through detailed web crawling, pivoting attacks to web servers, associated databases, and backend networks to confirm exploitability.

Conducting Phishing Simulations for Increased Security Awareness

Easily deploy phishing campaigns for client-side social engineering tests to discover which users are susceptible and what credentials can be harvested. Use the step-by-step process to create emails, select targets, and choose between browser redirects or web page clones. Challenge users with more sophisticated, tailored spear-phishing emails that are harder to identify as fake. Actual emails can be imported from mail clients to increase the authenticity of the attack.

Test Critical SCADA Systems

Core Security offers an add-on pack with additional SCADA and Industrial Control System exploits for Core Impact. The SCADA pack provides over 140 exploits in various SCADA and ICS that are deployed across many industries, on top of the SCADA and ICS exploits already shipped by default in Core Impact. This enhanced pack is updated with about four new exploits on average a month.

Validating Vulnerabilities Surfaced Through Scanners*

Core Impact's one-step test can quickly validate the results of over 20 different third-party scanners, including Nessus and BurpSuite. After you complete a scan against your environment, Core Impact can evaluate the scan's output and provide a prioritized validation of your infrastructure's weaknesses.

- Acunetix Web Vulnerability Scanner
- Burp Suite Professional
- Cenzic
- GFI LANguard
- HP WebInspect
- IBM Enterprise Scanner
- IBM Internet Scanner
- IBM Rational AppScan
- McAfee Vulnerability Manager (formerly McAfee Foundstone)
- Microsoft Baseline
- nCircle
- Nessus
- Nexpose
- Nmap
- NTOSpider
- Patchilnk VMS
- Qualys Guard
- Qualys Web Application Scanner
- Retine
- SAINT
- STAT Guardian
- Tenable Security Center
- Tripwire IP360

* A vulnerability scanner is not required to use Core Impact

coresecurity
by HelpSystems

www.coresecurity.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.