

Product Overview

Replicate Real-World Attacks and Reveal Critical Security Exposures

CORE Impact® Pro is the most comprehensive software solution for assessing and testing security vulnerabilities throughout your organization.

- endpoint systems & email users
- mobile devices
- network devices
- network systems
- web applications
- wireless networks

Backed by 15+ years of leading-edge security research and commercial-grade development, Impact Pro allows you to evaluate your security posture using the same techniques employed by today's cyber-criminals.

Multi-Threat Surface Investigation

CORE Impact Pro is the only solution that empowers you to replicate multi-staged attacks that pivot across systems, devices and applications, revealing how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and data.

What-If Attack Analysis

Impact Pro empowers you to demonstrate the severity of exposures by not only replicating how an attacker would compromise and interact with vulnerable systems, but also revealing exactly which data would be at risk.

Commercial-Grade Exploits

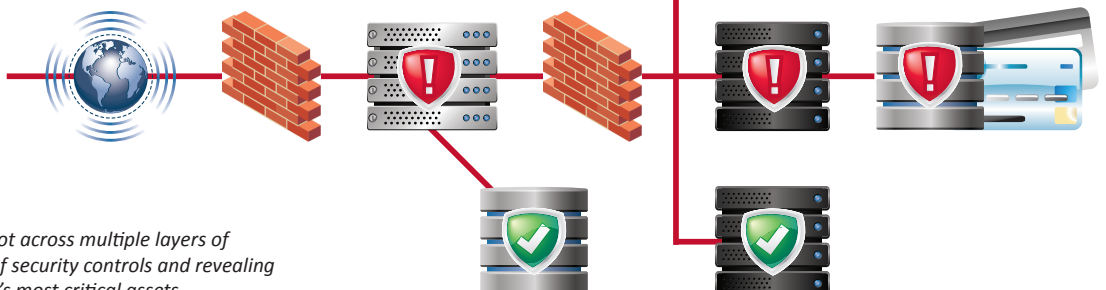
Only CORE Impact Pro offers a stable, up-to-date library of commercial-grade exploits and real-world testing capabilities. CORE routinely delivers 30+ new exploits and other updates each month – all professionally built and tested by in-house researchers and developers.

Actionable Results and Reports

Impact offers the industry's most comprehensive vulnerability reports.

- Confirm exploitable vulnerabilities to plan remediation efforts
- Gain metrics that illustrate the efficacy of layered defenses
- Validate compliance with government and industry regulations

CORE IMPACT™
PROFESSIONAL



CORE Impact replicates attacks that pivot across multiple layers of infrastructure, confirming the efficacy of security controls and revealing exposed pathways to your organization's most critical assets.

What They're Saying

"While it's nice to know that we're compliant with regulations, it's much more important for us to ensure IT security for our customers. CORE Impact helps us to both comply with the PCI Standard and honor our commitment to keep customer data safe."

- Chief Architect and Security Officer, *Online Retail*

"It would have taken someone three weeks of work every quarter to do what Impact did in a few hours."

- Security Specialist, *Health Care*

"With CORE Impact, we were able to find several weaknesses before they became issues. We were also able to verify which of our network defenses were performing up to expectations, and as a result our network is now significantly more resilient."

- Assistant Vice President, *Financial Services*

"In our view, Impact Professional still is top of the heap and we designate it SC Lab Approved again this year."

- SC Magazine, review of CORE Impact v12, February 2012



Network Penetration Testing

- Gather network information and build system profiles
- Identify & exploit critical OS, service & application vulnerabilities
- Replicate an attacker's attempts to access and manipulate data after the initial compromise
- Leverage compromised systems as beachheads to attack other network resources through VPN and proxy pivots

Client-Side Testing of End Users and Endpoints

- Crawl sites, search engines and other sources for potential attack targets and information useful for targeting attacks
- Leverage a variety of templates or create custom phishing emails
- Use client-side exploits to test endpoint system security
- Test security awareness with or without exploiting systems
- Replicate multistaged attacks by pivoting to backend networks

Network Device Penetration Testing

- Scan IP ranges for network devices and gather identifying information, such as manufacturer, model and OS
- Exploit configuration vulnerabilities and verify access through configuration retrieval, password cracking, access list piercing, and interface monitoring capabilities

Vulnerability Scan Validation

CORE Impact Pro can import and validate the exploitability of results from the following network and web vulnerability scanners:

- | | |
|---|---------------------------------|
| • eEye Retina® Network Security Scanner | • McAfee® Vulnerability Manager |
| • GFI LANguard™ | • nCircle IP360™ |
| • HP WebInspect® | • NTO Spider™ |
| • IBM AppScan® | • Qualys QualysGuard® |
| • IBM Internet Scanner® | • SAINTscanner® |
| • Lumension® Scan | • Tenable Nessus® |

A vulnerability scanner is not required to use Impact, since it can independently identify and profile servers, services, web pages, etc. to intelligently select exploits appropriate for your testing targets.

Web Application Penetration Testing

- Identify weaknesses in web applications, web servers and associated databases – with no false positives
- Test for all OWASP Top Ten web application vulnerabilities
- Dynamically generate exploits that can compromise security weaknesses in custom applications
- Import and validate results from web vulnerability scanners to confirm exploitability and prioritize remediation
- Pivot attacks to the web server and backend network

Mobile Device Penetration Testing

- Identify critical exposures posed by mobile devices on your network
- Evaluate the security of new mobile devices prior to deployment
- Get actionable data required to mitigate business risks
- Access call and text logs, GPS data, and contact entries

Wireless Network Penetration Testing

- Assess WEP, WPA-PSK and WPA2-PSK encrypted networks
- Conduct man-in-the-middle attacks, intercept wireless transmissions, and insert exploits into relayed traffic
- Impersonate access points to target Wi-Fi enabled systems
- Pivot to network, web application and client-side attacks

