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
- Passwords and identities
- Mobile devices
- Wireless networks
- Web applications and services
- Network systems and devices

Backed by 15+ years of leading-edge security research and commercial-grade development, Core 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 assets.

- Surveillance camera vulnerability testing
- Web services testing for web and mobile applications

WHAT-IF ATTACK ANALYSIS

Demonstrate and document the severity of exposures by replicating how an attacker would compromise and interact with vulnerable systems, and revealing at-risk data.

COMMERCIAL-GRADE EXPLOITS

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.

Core Security partners with ExCraft Labs to deliver enhanced SCADA exploits for Core Impact Pro. The SCADA pack by ExCraft Labs targets over 50 exploits in various SCADA Systems that are deployed across many industries. This enhanced pack is updated with about 10 new exploits on average a month.

TEAMING

Multiple security testers now have the capability to interact in the same workplace against the same environment across multiple copies of Core Impact Pro. This capability provides a common view of discovered and compromised network targets.

REPORTING

Core Impact offers comprehensive reporting capabilities.

- Confirm exploitable vulnerabilities to plan remediation efforts
- View metrics that illustrate the efficacy of layered defenses
- Validate compliance with government and industry regulations
- Remediation validation reporting capabilities

EXCRAFT SCADA PACK ADD-ON PRODUCT

“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

“Typical Core quality. We have used this product extensively and never been disappointed. Best Buy.”

SC Magazine, review of Core Impact Pro
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 and validate results from web vulnerability scanners to confirm exploitability and prioritize remediation
- Pivot attacks to the web server and backend network
- Web services testing for web and mobile applications

MOBILE DEVICE PENETRATION TESTING
- Identify critical exposures posed by mobile devices on your network
- Evaluate the security of new mobile devices and related web services prior to deployment
- Access call and text logs, GPS data, and contact entries
- Embeddable Android Agent for Android devices

VULNERABILITY SCAN VALIDATION
Core Impact Pro can import and validate the exploitability of results from the following network and web vulnerability scanners:
- Acunetix® Web Security Scanner
- eEye Retina® Network Security Scanner
- GFI LANguard®
- HP WebInspect®
- IBM AppScan®
- IBM Internet Scanner®
- Lumension® Scan
- McAfee® Vulnerability Manager
- TripWire IP360™
- NTO Spider®
- Qualys QualysGuard®
- SAINTscanner®
- Tenable Nessus®
- Tenable Security Scanner®
- Cenzic Enterprise®

* A vulnerability scanner is not required to use Core Impact Pro

NETWORK PENETRATION TESTING
- Gather network information and build system profiles
- Identify and exploit critical OS, device, service, and application vulnerabilities
- Replicate an attacker’s attempts to access and manipulate data
- Leverage compromised systems as beachheads to attack other network resources through VPN and proxy pivots
- Test defensive technologies’ ability to identify and stop attacks

CLIENT-SIDE TESTING OF END USERS AND ENDPOINTS
- Crawl sites, search engines, etc. for potential target information
- Leverage a variety of templates or create custom phishing emails
- Use client-side exploits to test endpoint system security, assess defenses, and pivot to network tests
- Test security awareness with or without exploiting systems

IDENTITY DISCOVERY & PASSWORD CRACKING
- Discover Windows NTLM hashes and attempt to determine plaintext passwords for those hashes
- Discover identities: usernames, passwords, SSH keys, and cookies
- Utilize learned identities as part of multi-vector tests
- Automatically take control of systems via weak authentication manually or with the rapid penetration test wizard (RPT)

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

SURVEILLANCE CAMERA ATTACKS
- Testing teams can identify whether a host on their network is a camera and then test it for vulnerabilities
- Ability to prove camera vulnerabilities by taking a still shot of the video feed, or accessing the camera’s administration interface
- Testing video cameras using can be done manually or with the RPT wizard

THINK LIKE AN ATTACKER™
Enterprises and security professionals can focus on the most likely threats to their critical business assets by modeling, simulating and testing what an actual attacker would do.

CORE SOLUTIONS
Core Security helps more than 1,400 customers worldwide identify the most vulnerable areas of their IT environments to improve the effectiveness of remediation efforts and ultimately secure the business.

EXPERIENCE
Our patented, proven, award-winning enterprise products and solutions are backed by more than 15 years of applied expertise from Core Labs research and Core Security Consulting Services.