Core Impact

Product Overview

Core Impact simplifies testing for new users and allows advanced users to efficiently execute common tasks. This saves significant time versus manual testing, while providing a consistent, repeatable process for testing infrastructure.

Benefits of Web Application Testing with Core Impact:

- Exposed systems due to compromised perimeter defenses
- What OS and services vulnerabilities pose actual threats to your network
- How privileges can be escalated on compromised systems
- What information could be accessed, altered or stolen
- What systems are vulnerable to denial of service attacks
- How trust relationships could expose additional systems to local attacks

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

Multi-Threat Surface Investigation

Core Impact 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.

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

Teaming

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

Reporting

Core Impact offers comprehensive, customizable 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

Core Security partners with ExCraft Labs to deliver enhanced SCADA exploits for Core Impact. 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.

Network Penetration Testing

- Gather network information and build system profiles
- Identify and exploit critical OS, device, service, and application vulnerabilities
- Replicate attacker attempts to access and manipulate data
- Pause/resume attacks to meet SLA requirements
- 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 and Password Cracking

- Discover Windows NTLM hashes and attempt to determine plaintext passwords for those hashes
- Discover identities: usernames, passwords, Kerberos tickets/ e-keys, and SSH keys
- 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)

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
- 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

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

Vulnerability Scan Validation

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

- Acunetix® Web Security Scanner
- Retina® Network Security Scanner
- GFI LANguard™
- HP Web Inspect®
- IBM AppScan®
- IBM Internet Scanner®
- Lumension® Scan
- Portswigger Burp Suite
- McAfee® Vulnerability Manager
- TripWire IP360™
- Rapid7 AppSpider
- Rapid7 Nexpose
- Qualys QualysGuard®
- SAINTscanner®
- Tenable Nessus®
- Tenable Security Scanner®
- Tenable SecurityCenter™
- Trustwave App Scanner

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

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

ABOUT CORE SECURITY

Courion has rebranded the company, changing its name to Core Security, to reflect the company's strong commitment to providing enterprises with market-leading, threat-aware, identity, access and vulnerability management solutions that enable actionable intelligence and context needed to manage security risks across the enterprise. Core Security's analytics-driven approach to security enables customers to manage access and identify vulnerabilities, in order to minimize risks and maintain continuous compliance. Solutions include Multi-Factor Authentication, Provisioning, Identity Governance and Administration (IGA), Identity and Access Intelligence (IAI), and Vulnerability Management (VM). The combination of these solutions provides context and shared intelligence through analytics, giving customers a more comprehensive view of their security posture so they can make more informed, prioritized, and better security remediation decisions.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

CORE SECURITY