

HANDS-ON PENETRATION TESTING SERVICES FROM THE MAKERS OF CORE IMPACT

Today's IT threat environment obligates organizations to identify data security risks before attackers do. As attack techniques evolve and new vulnerabilities arise, cybercriminals continue to aggressively target sensitive data via multiple vectors, including web applications, network and end-user systems, and Wi-Fi networks.

While it's clear that proactive vulnerability management is essential to mitigating risks, many organizations find that traditional vulnerability scans provide volumes of information about potential risks – with little clear insight into actual, proven exposures.

Core Security Technologies' CORE IMPACT penetration testing services safely replicate real-world attacks against your IT systems, pinpointing your organization's critical information security weaknesses in the most proactive and realistic way possible.

- **Reveal complex paths of exposure to critical assets**
Service offerings can be combined to trace links between vulnerabilities and reveal attack paths extending from the network perimeter to backend resources.
- **Cut through data overload**
Traditional security solutions often provide a flood of information about potential threats. CORE IMPACT services deliver clear and concise information about proven exposures that pose imminent risks to your systems and data.
- **Go beyond vulnerability scanning**
CORE IMPACT penetration testing services replicate attacks against your environment, both identifying exploitable vulnerabilities and revealing the potential implications of a related breach.
- **Support compliance initiatives**
Assessment results can be leveraged during compliance initiatives for mandates requiring penetration testing and other proactive security controls.
- **Work with skilled security professionals**
CORE IMPACT penetration testing engagements are conducted by highly experienced, CISSP- and/or CEH-certified professionals.

CORE IMPACT Penetration Testing Services Offerings

The following CORE IMPACT services offerings can be conducted individually or combined to reveal how chains of vulnerabilities present paths of exposure throughout your environment.

Web Application Penetration Testing Services

Mitigating weaknesses in web applications can be costly since they often require re-coding to effectively remediate issues. CORE IMPACT Web Application Penetration Testing services pinpoint exploitable application weaknesses with no false positives, allowing development resources to focus on addressing critical exposures. Core Security engineers can assess your web applications for flaws cited by the Open Web Application Security Project (OWASP), such as:

- **A1: Injection Flaws** – assess applications against SQL injection and blind SQL injection attacks
- **A2: Cross-Site Scripting (XSS)** – test applications against URL-based XSS attacks
- **A4: Insecure Direct Object References + A7 Failure to Restrict URL Access** – uncover hidden, backup and old pages in applications + discover and analyze robots.txt files to reveal admin pages and other sensitive URLs



What you get with CORE IMPACT penetration testing services

- **Personalized recommendations**
A Core Security professional analyzes test findings and prepares a personalized summary of critical exposures and suggested next steps.
- **Visibility into critical risks**
CORE IMPACT services deliver proof of exploitable weaknesses that expose sensitive systems and data to attack.
- **Actionable data for efficient remediation**
You receive reports with details on exposed systems, compromised vulnerabilities and remediation recommendations.
- **Full audit trails**
After each engagement, you receive a detailed audit trail of all testing activities, including systems tested, exploits run, and more.



When it comes to pen testing, there is nothing that this tool either cannot or won't soon do for you.

SC Magazine, November 2009

*In reference to CORE IMPACT, the solution used for our penetration testing services.

Why CORE IMPACT services are safe for your environment

- **Rigorous quality assurance**
All exploits used during testing are developed in-house and undergo rigorous quality assurance to ensure that they leave your systems unaffected.
- **No exploit code installed**
Exploits are managed via CORE IMPACT's proxy agent, which replicates attacks without leaving anything behind on tested systems.
- **Optimized system stability**
While some exploits can interrupt processes due to the nature of the attacks they replicate, these can be omitted from tests to ensure system stability.
- **No backdoors**
IMPACT testing services are designed to never leave behind a path that could later expose your systems or data.
- **Independent validation from the field**
Included among the hundreds of organizations using CORE IMPACT software in-house are some of the world's largest corporations and government organizations.
- **No new vulnerabilities**
CORE IMPACT services find existing weaknesses without creating new vulnerabilities on assessed systems.

- **A10: Insufficient Transport Layer Protection** – identify where weak levels of encryption expose your HTTPS-secured sites
- **A6: Security Misconfiguration** – assess web server and network infrastructure to identify other security issues that undermine web application integrity (requires Network Penetration Testing service)

This service can be customized to address additional OWASP-ranked weaknesses and other web application exposures, such as remote file inclusion.

Network Penetration Testing Services

Your organization's servers and workstations make up the backbone of your IT infrastructure and house some of its most important data. CORE IMPACT Network Penetration Testing services replicate real-world attempts to exploit and traverse your network environment, providing visibility into:

- which systems are exposed if perimeter defenses are compromised
- what OS, service and application vulnerabilities pose real threats
- how privileges can be escalated on compromised systems
- what information could be accessed, altered or stolen
- how low-level network compromises can open paths to critical backend data

Client-Side Penetration Testing Services

Email-based attacks on employees and contractors pose one of the greatest threats to information security today. CORE IMPACT Client-Side Penetration Testing services assess end-user security awareness and reveal exploitable endpoint vulnerabilities using email-based phishing and spear phishing techniques to:

- identify end users who click on links in malicious emails
- test their systems for exploitable OS, service and application vulnerabilities
- demonstrate how compromised endpoints expose other, more sensitive systems on your network (requires Network Penetration Testing service)

Wireless Network Penetration Testing Services

Your organization's Wi-Fi networks provide a tempting point of exposure for criminals seeking access to protected backend databases and other critical resources. CORE IMPACT Wireless Network Penetration Testing services identify critical Wi-Fi weaknesses by:

- gathering information on network strength, security protocols and connected devices
- replicating attempts to crack networks encrypted with WEP, WPA-PSK and WPA2-PSK
- sniffing traffic to find streams of sensitive data
- attempting to join cracked networks and compromise backend systems
- pivoting from wireless to network testing in an attempt to access data on backend systems (requires Network Penetration Testing service)

Next Steps

To learn more about CORE IMPACT Penetration Testing Services, please contact Daniel Rheault at +1 (617) 695-1152 or drheault@coresecurity.com.