CORE SECURITY TECHNOLOGIES

STRATEGIC SECURITY FOR YOUR ORGANIZATION

The First Comprehensive Assessment of Your Security Risks

CORE IMPACT

CORE IMPACT™ is the first automated, comprehensive penetration testing product for assessing specific security threats to your organization's information assets. By using CORE IMPACT to safely exploit vulnerabilities in your network infrastructure, you can identify tangible information security risks while testing the effectiveness of your security investments.

ALSTOM

"We immediately saw a return on investment from the data gathered during our initial CORE IMPACT training session."

Continental Airlines

"Running a penetration test used to be very risky, but now, with CORE IMPACT, the testing process could not be safer. The product also made us much more efficient by reducing testing time from days to just a few minutes per week."

CORE IMPACT enables you to:

- identify real vulnerabilities and expose attack paths that put information assets at risk
- delineate actual threats from false positives with the latest Commercial-Grade exploits
- intelligently plan, prioritize and execute vulnerability remediation efforts
- evaluate, configure and test the effectiveness of security infrastructure, such as IPS and IDS
- justify budget requests for new security infrastructure
- identify exposure to social engineering attacks and monitor end-user security awareness programs
- collect information required for compliance with industry and government regulations

And because CORE IMPACT combines an intuitive interface with straightforward reporting, you don't have to be a security expert to identify risks and determine how to optimize your information security.

Place Your Trust in Our Commercial-Grade Exploits

A penetration test is only as effective as the exploits it runs against your network, and only CORE IMPACT offers Commercial-Grade Exploits. With CORE IMPACT, you have full control over the most comprehensive, stable and up-to-date library of exploits available. Created in-house by a dedicated team of experts, they are guaranteed to be current, effective and safe for your network.

CORE IMPACT's Commercial-Grade Exploits:

- perform penetration tests safely and securely
- test as many target OS configurations and attack vectors as possible
- minimize service disruptions
- are created in-house by dedicated exploit developers
- are developed and released on a regular basis
- undergo intensive quality assurance testing
- are updated as functionality and attack vectors evolve

Product Spotlight: Agents

When used for actual network attacks, exploits can execute payloads of malicious code that alter, destroy or expose information assets.

CORE IMPACT exploits deploy the industry's first benign payloads, known as "Agents." Agents preserve the integrity of compromised computers by running only in system memory.

A successfully deployed Agent provides indisputable evidence that a vulnerability is real by allowing you to interact with the compromised system, escalate privileges, and target other network resources.

With Agents, you can safely:
- validate the existence of vulnerabilities
- prove that vulnerabilities can be exploited
- assess the consequences of actual network intrusions
- return compromised computers to their pre-attack states

FCWCOM

After using IMPACT it seems obvious to us that manual penetration testing is obsolete.

"Put an End to Manual Penetration Testing," Federal Computer Week, May 15, 2006

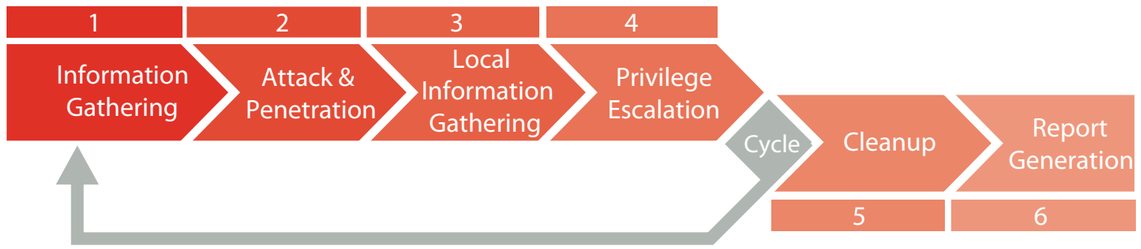
SC MAGAZINE LAB APPROVED

We rate CORE IMPACT as Lab Approved for its comprehensive capabilities, flexibility and ease of use...

"Group Test: Vulnerability Assessment" SC Magazine, January 2007

Put Your Network Security to the Test in Six Easy Steps

With CORE IMPACT, you systematically execute real-world network attacks to gain information about actual, exploitable security threats. The product's industry-first Rapid Penetration Test (RPT) provides an automated, six-step process that allows you to evaluate your entire network in a matter of minutes. What's more, you can quickly and cost-effectively repeat tests to prove the effectiveness of new security systems and vulnerability remediation efforts.



The CORE IMPACT Rapid Penetration Test empowers you to evaluate the security of your information assets - quickly, thoroughly and safely.

1. Information Gathering

Successful penetration testing relies on your ability to gather relevant information about the target network. CORE IMPACT automates information gathering to select the most relevant attacks for your network, saving time and ensuring testing efficiency.

- Identify the operating system and services running on targeted systems.
- Control the IP ranges you want to scan.
- Select from a variety of network discovery and port scanning methods, including TCP Connect, Fast SYN, UDP service discovery and ICMP.
- Eliminate the need to purchase supplemental tools to gather network information prior to testing.
- Gather valuable data to assist with remediation efforts.

2. Attack and Penetration

During Attack and Penetration, CORE IMPACT automatically selects and launches remote attacks leveraging data obtained in the Information Gathering step. You maintain full control over which computers are attacked and the order in which exploits are launched.

- Launch multiple, simultaneous attacks to speed the testing process.
- Interact with compromised systems via discrete agents that are installed only in memory, thereby preserving system integrity.
- Maintain control over which exploits are applied.

3. Local Information Gathering

The Local Information Gathering step collects information about computers that CORE IMPACT has successfully compromised. During this step, Agents (see "Product Spotlight: Agents") gather information about OS, network configuration, Agent privileges, users and installed applications.

- Browse file structures and view file contents on compromised systems.
- View rights obtained on compromised systems.
- Interact with compromised systems via shells.
- Gather information that can be used to attack other computers on the network.

4. Privilege Escalation

During the Privilege Escalation step, CORE IMPACT attempts to penetrate deeper into a compromised computer by running local exploits in an attempt to obtain administrative privileges. After Privilege Escalation, you can shift the source agent to one of the newly compromised systems and cycle back to the initial Information Gathering step, thereby establishing an outpost from which to run attacks deeper into the network.

- Run local exploits to gain administrative privileges on compromised systems.
- View the networks to which a compromised computer is connected.
- Pivot attacks from any compromised system to other computers on the same network, gaining access to systems with increasing levels of security.

5. Cleanup

The Cleanup step automatically uninstalls every connected agent. In addition, all agents are automatically uninstalled when closing the active workspace, regardless of whether the Cleanup step is executed or not.

- Run tests without installing modules or tools on compromised systems (or altering them in any way).
- Quickly and easily remove all agents from compromised systems, leaving them in their original states.

6. Report Generation

CORE IMPACT generates clear, informative reports that provide data about the targeted network and hosts, audits of all exploits performed, and details about proven vulnerabilities. You can view and print reports using Crystal Reports® or export them in popular formats such as HTML, PDF and Microsoft® Word.

- Obtain actionable information about exploited vulnerabilities and associated risks.
- Create activity audits to satisfy regulatory requirements.
- Export report content in popular formats that can be easily customized and shared.
- Meet the needs of different constituencies with tailored reports for management, network administrators, remediation staff and others.

Product Spotlight: Client-Side Exploits

Client-side exploits take advantage of vulnerabilities in client software including web browsers, email applications and media players. End-users are often lured into triggering these exploits through social engineering tactics.

CORE IMPACT client-side exploits are Commercial-Grade and take advantage of the product's automated capabilities to pinpoint vulnerabilities in client software throughout your organization.

A successful CORE IMPACT client-side exploit can leverage the compromised system to attack workstations or servers otherwise protected by perimeter defenses and accessible only via the internal network.

WINNER eWEEK Excellence Awards 6TH ANNUAL

"Vulnerability Assessment & Remediation" eWeek, June 19, 2006 CORE IMPACT 5.0

HOTPICK INFORMATION SECURITY®

CORE IMPACT 6.0 is an amazing tool to validate your security posture. We highly recommend it ...

"Group Test: Vulnerability Assessment" SC Magazine, January 2007

Get the Right Solution for Your Environment

CORE IMPACT is designed with the flexibility you need to meet your specific penetration testing requirements.

Lightweight

You can run CORE IMPACT on any Windows computer with the following minimum specifications:

- Intel® Pentium™ III 800 MHz or better
- 256 MB RAM (512MB recommended)
- 300 MB free hard disk space
- Internet Explorer 6.0 or 7.0
- a Windows®-compatible Ethernet networking card
- Windows 2000 Professional SP3 or greater
- Windows XP Home or Professional SP1 or greater

Cross-Platform

CORE IMPACT offers a comprehensive, up-to-date library of exploits for system services and applications running on the following target platforms:

- Windows 2003, XP, 2000, NT4
- Linux®
- Mac OS X®
- AIX®
- Sun Solaris™
- OpenBSD

Compatible

CORE IMPACT improves the productivity and effectiveness of your overall vulnerability management efforts by integrating with vulnerability scanners and patch management tools, including:

- Nessus™
- eEye Retina®
- GFI LANguard™
- Nmap Security Scanner
- Harris STAT Guardian™ Vulnerability Management Suite (VMS)
- Qualys QualysGuard®
- PatchLink Update™

In addition, CORE IMPACT's XML-based test results can be exported for use in third-party security management and reporting products.

Customizable

All CORE IMPACT exploits are developed using Python, allowing you to review, customize and extend them as desired. New exploits can easily be added to CORE IMPACT and executed in conjunction with the product's existing library of exploits.

Stay a Step Ahead of Growing Threats

With CORE IMPACT, you can stay on top of vulnerabilities by running penetration tests as often as necessary to:

- test existing or new network infrastructure
- ensure the integrity of security patches
- assess the impact of system upgrades or modifications
- generate periodic reports for compliance purposes

Since the product is updated frequently with new exploits, you can keep your defenses current by replicating attacks that take advantage of the latest vulnerabilities.

Product Spotlight: Traffic Masking

As network security technologies such as firewalls, IDS and IPS become more widespread, attackers develop increasingly sophisticated network circumvention methods – such as modifying network traffic to mask attacks.

CORE IMPACT's Traffic Masking capabilities include:

MSRPC fragmentation:
CORE IMPACT breaks attack traffic into small pieces to ensure that security investments provide the highest levels of protection against masked payloads.

MSRPC traffic encryption:
CORE IMPACT offers the first automated technology for testing networks with attacks that use MSRPC-supported encryption.

Get Started Today

To learn more about CORE IMPACT, please contact us at **+1 (617) 399-6980** or email **sales@coresecurity.com**

41 Farnsworth Street
Boston, MA 02210
Ph: +1 (617) 399-6980
Fax: +1 (617) 399-6987
www.coresecurity.com

© 2007 Core Security Technologies and CORE IMPACT are trademarks of CORE SDI, Inc. All other brands and products are trademarks of their respective holders.