

TESTING & ANALYSIS TO HELP YOU MAKE PURCHASING DECISIONS

PRODUCT **Reviews**

**HotPick**  
INFORMATION SECURITY®

**INFORMATION SECURITY**

SECURITY TESTING

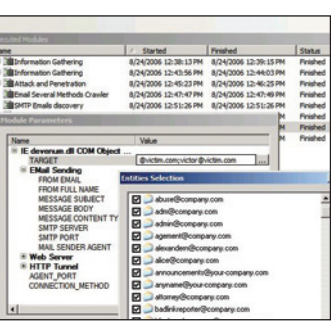
# Core Impact 6.0

REVIEWED BY MIKE POOR

**Core Security Technologies**

[www.coresecurity.com](http://www.coresecurity.com)

Price: **\$25,000** for annual subscription



Prior to Core Impact, the vast majority of security penetration testers would use “off-the-Web” exploit code, after scouring an application code for backdoors and covert channels. Core Impact changed the security landscape by providing stable, tested and trustworthy exploits for ethical hacking.

The latest release of this automated, commercial-grade penetration-testing software platform is an invaluable tool for professional penetration testers and corporate security engineers.

## Configuration/Management **A**

Installing Core Impact 6.0 was a breeze—download, double-click and enter the long string to decrypt the installation executable.

There are two main workflows: The rapid penetration test guides the user through the phases of reconnaissance, exploitation and reporting via a series of menu-driven wizards. You can choose the type of exploits to test, as well as the levels of risk to take (e.g., whether or not to run exploits that might crash or DoS the service).

The second workflow is conducted via modules. In this more granular mode, you choose from this version’s plethora of available exploits.

## Effectiveness **A**

We were able to run multiple exploits, test and compromise machines in minutes, giving the attacker complete command and control over our target systems and arming us with detailed information.

**Testing methodology:** We used VMware virtualization software to install a fully patched Windows XP Pro system to host Core Impact; and a Windows 2000 Advanced Server system with a few service packs missing to play the victim.

We first ran a rapid penetration test in which Core Impact walks you through a simple set of questions to identify the target systems. It scanned the network and identified live hosts, listening ports and OS versions, allowing us to choose the exploit modules most likely to compromise the target.

We chose remote exploits first, attacking the Microsoft Windows Plug and Play services umpnpgm-gr.dll vulnerability (Microsoft bulletin MS05-039). One click brings up a quick description of the exploit and the vulnerability, including links to patches and remediation information.

We then tested client-side exploits, switching to the “Modules View” to select individual attacks. We ran the IE IFRAME buffer-overflow exploit—which automatically sets up a Web server on the attack system, with a Web page serving up the exploit—and browsed the attack site to compromise our target system. Compromising a target using remote and client-side exploits demonstrates the need to patch the vulnerable software. One of the biggest benefits of running exploits against real systems is gaining insight into how credible the threat posed by vulnerabilities is in our environment.

At the end, Core Impact removes all the agents from the target system, a step often neglected by inexperienced penetration testers. Test activity is logged for review.

## Reporting **B**

Core Impact comes with a number of report generation options, from a simple executive summary to a detailed vulnerability report. The reports are simple and straightforward. The vulnerability report includes the number of systems compromised, along with detailed information regarding the vulnerabilities exploited. Administrators could use this report to remediate the exposures by following the remediation information and links to patches.

Core Impact uses Crystal Reports, with an XML-based generation system that can be altered and customized to meet your requirements. To take advantage of this feature, however, you have to get under the hood and change the XML templates.

## Verdict

Core Impact 6.0 is an amazing tool to validate your security posture. We highly recommend it to security engineers to verify the vulnerability of their networks, or confirm test results from third-party consultants.

Reprinted with permission from Information Security Magazine, January 2007.  
© 2007 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144



41 Farnsworth Street | Boston, MA 02210 | USA  
Ph: (617) 399-6980 | Fax: (617) 399-6987  
[www.coresecurity.com](http://www.coresecurity.com)