Core Impact 7.5
Core Impact is a powerful tool that delivers quick, accurate assessments of the security of a network. The latest version expands the scope with Web application security checks and refines the valuable e-mail phishing feature for assessing the security savvy of end-users. Core's smart dashboard, friendly UI, attack configuration wizards, and focused reports make penetration testing easier than ever to conduct and interpret.
With Version 7.5, the tried-and-true attack toolkit becomes easier to use, leverages the fallibility of users to gain access to host systems, and adds security checks for Web-based databases.

CORE IMPACT HAS LONG BEEN ONE OF OUR favorite tools for testing the effectiveness of security devices. Now that we’ve had a chance to see what the recently released Version 7.5 of the product can do, we like Core Impact even better. This latest version adds two important Web application testing techniques, polishes the e-mail phishing attack capabilities introduced in Version 6, and generally makes penetration testing easier than ever before.

In serious security geek circles, you may get picked on for using Core Impact because it is so simple, but then again you’re likely to have more free time to think of retorts. Whether you’re a seasoned penetration tester or a neophyte, the new reporting interface and idiot-proof attack wizards make it a breeze to discover and exploit the vulnerabilities remaining in both your silicon- and carbon-based infrastructures.

Unsocial engineering
In Version 6.0, Core Impact introduced valuable client-side attacks that tested the security awareness of end-users by sending Trojans embedded in a legitimate-looking e-mail. By using these types of phishing attacks, you can directly assess the security awareness of your end-users. Do they readily click Yes and turn over control of their machines to malicious software applications, or do they report a potentially infected attachment to the help desk as taught in their yearly security training?

Version 7.5 makes configuring e-mail phishing attacks much simpler. First off, this version allows you to harvest e-mail addresses via several methods and by integrating with search tools, including Google, Yahoo, AltaVista, MSN Live Search, and MetaCrawler. Impact is able to search the Internet for corporate e-mails that black hats and spammers are scavenging as you harvest DNS, Whois, and PGP key services and pull the trigger. The e-mail is sent to the victims on your list and sits in their inboxes with all of their other mail. When a user opens the attachment, the Trojan calls back to Core Impact, setting up an agent tunnel ready for exploitation and giving you a look at which of your users need additional training in Information Assurance.

There’s one shortcoming we spotted in this feature: Once a client Trojan is in place, it tries to connect to Core Impact only once; if Impact isn’t available when the exploit is first executed, the potential compromise is lost. We’d like to see a timer added to the exploit to allow it to continue trying (every 10 minutes, every hour, once a day) if it doesn’t connect the first time. Additionally, we’d like to see Impact itself able to run on a server as a service, especially since an e-mail with a Trojan payload may not be opened for several days. Having Impact available to receive the call at any time would make this feature much more effective.

Among the UI improvements in Impact 7.5 is the separation of the attack wizards and reports for human vulnerabilities from those for network holes. You can now get a report on your least savvy users independently from the missing patches on your networked devices, and you can view the two attack domains separately in the dashboard. With the new dashboard, you can easily sift through thousands of unique entry points into the network and their vulnerabilities, and drill down to the smallest client detail.

Reports on testing activity, hosts, end users, and their vulnerabilities are a snap to generate, and they deliver the relevant information needed in an aesthetically pleasing form that executives will appreciate, though an interface that allowed different users to get different views according to their areas of responsibility would be a welcome improvement.

Web attack!
Also noteworthy in the 7.5 upgrade are two new Web application checking techniques. The first exposes vulnerabilities in Web apps that allow for SQL injection attacks. This tool removes all the heavy lifting involved in exploiting databases with Web front ends, and it should help open the eyes of security-obstinate Web programmers.

Core Impact does a very thorough job of looking for proprietary SQL injection bugs, checking whether your database server is vulnerable to these types of attacks. Impact also provides information on other SQL databases linked to your database, identifying these potential targets.

In our testing, Impact was able to correctly fingerprint our (unsecured) ASP application and its Microsoft SQL Server back end, and it enabled us to successfully extract protected information from the database. Impact was even able to deploy an agent to our database server through SQL injection.

The second major new addition to Impact’s arsenal of exploits is the checking for RFI (Remote File Inclusion) on PHP applications. If you’re not familiar with this type of exploit, it occurs when an attacker passes his own custom PHP code to the Web server, along with a request to execute the code. Many PHP designers have unwittingly written code that easily allows this type of attack to work. In the test lab, Impact was able to give us a shell window after a successful RFI attack on our PHP site. We could install and run any PHP code on the server we wanted. Impact even allows you to take screen captures from the compromised host.

A couple of improvements that arrived with Version 7.0 are worth noting. First, the multiple client-side agents that facilitated different levels of attack in previous versions of Impact have been replaced by a single, do-everything agent. Still in-memory (on by default), the client agent can now use all network connections through a single listener port, providing a greater degree of flexibility to bypass firewalls and other security devices. The agent also now supports runtime plug-ins that open the door for customized, client-side actions such as patching, installing security software, and gathering forensic information.

Version 7.0 also added support for FreeBSD as a target OS, a long-overdue addition, as well as full pivoting from Vista machines — the ability to attack additional machines from compromised Vista targets.

Core Impact’s automated penetration testing is still quick and effective, and because Impact is not a network vulnerability scanner, its tests are 100 percent free of false positives, which is the primary reason we consider it an essential testing tool. Version 7.5’s redesigned attack wizards, enhanced user interface, upgraded agent, and Web application attacks are significant improvements to an already compelling product that can help you improve your organization’s security posture by compromising both the machines that reside on your network and the people that use those machines on a daily basis.

— Victor R. Garza & Charles D. Herring