

WHITE PAPER

Automated Penetration Testing: Can IT Afford Not To?

Sponsored by: Core Security Technologies

Charles J. Kolodgy

Gerry Pintal

January 2007

IDC OPINION

Today's enormously complex enterprise IT infrastructures consist of hundreds and in some cases thousands of systems and subsystems. Each component of these infrastructures is meticulously configured and integrated into complex systems architecture.

Professional IT staffs responsible for securely establishing and maintaining these IT infrastructures are assessing, on an ongoing basis, the real risks presented by system vulnerabilities.

The task of correctly assessing the real security risks associated with a seemingly endless stream of vulnerability and patching reports is a critical and time-consuming activity for IT staffs. However IT professionals understand that despite their best efforts, vulnerabilities may still present significant security risks for their companies.

During research and in-depth interviews, IDC found compelling reasons why IT executives and team members must adopt penetration testing as an integral part of their security and vulnerability management (SVM) processes and programs. Penetration testing enables users to:

- ☒ **Intelligently manage vulnerabilities.** Penetration testing provides detailed information on actual, exploitable security threats. By performing a penetration test, an organization can identify which vulnerabilities are critical, which are insignificant, and which are false positives.
- ☒ **Avoid the cost of network downtime.** Recovering from a security breach can cost millions due to IT remediation efforts, lost employee productivity, and lost revenue. Penetration testing allows an organization to prevent this financial drain by identifying and addressing risks before security breaches occur.
- ☒ **Preserve corporate image and customer loyalty.** Even a single incident of compromised customer data can be costly. Penetration testing helps an organization avoid data incidents that put its goodwill and reputation at risk.
- ☒ **Justify security investments.** Penetration testing can both evaluate the effectiveness of existing security products and build the case for proposed investments.

IN THIS WHITE PAPER

In this white paper we provide an overview of penetration testing, discuss security vulnerabilities, and summarize the results and benefits of penetration testing realized by the IT executives interviewed. We also present the features and benefits of Core Security Technologies' CORE IMPACT, a leading product in the penetration testing space.

PENETRATION TESTING

Overview

Vulnerability scanning tools have been commercially available for close to a decade to assist IT professionals in collecting, tracking, and reporting the status of known vulnerabilities. However, these tools address only a portion of a comprehensive vulnerability management process and are known to produce many false positives. False positive reports are a huge time sink for IT staff, and they severely complicate IT's ability to accurately identify high-risk vulnerabilities pertinent to business and operations.

An IT security executive in the transportation industry explained, "The thing that really used to irk me is when I had someone come in, scan my network, and then tell me I had 15,000 medium-level vulnerabilities. I thought, in between all of the patching, updates, crashes, backups, and users, when am I supposed to look at these 15,000 vulnerabilities?"

To address some of the problems inherent in vulnerability assessment, enterprises have utilized penetration testing, which is the process of executing a real, but safe attack on an IT infrastructure or any of its systems and/or subsystems in an effort to uncover and demonstrate the existence of security risks presented by network or client (end-user) vulnerabilities. Until recently, penetration testing has been more of an art than a science or engineering practice. Most penetration testing activities are performed by outside consultants or a specialized team within the IT security organization. Both methods require considerable capital resources.

Recently though, software tools have hit the market that provide a cost-effective way to look at real risks, not just vulnerabilities. These commercial applications contain exploit testing engines that automate all of the steps of a proven penetration testing process.

"The thing that really used to irk me is when I had someone come in, scan my network, and then tell me I had 15,000 medium-level vulnerabilities. I thought, in between all of the patching, updates, crashes, backups, and users, when am I supposed to look at these 15,000 vulnerabilities?"

Why Penetration Testing?

Workload Issues

IT organizations are continually challenged with tight budgets and ever-increasing workloads. In some cases, they may regard penetration testing as "just another activity" to add to their already heavy workloads.

IDC explored this issue during interviews with IT executives. Although adding another tool to work with initially appears to add to IT's overall workloads, participants in this research conclusively found the opposite to be true.

As a direct result of their acquiring and incorporating CORE IMPACT into their arsenal of IT tools, they were emphatic in stating that their IT teams, in addition to improving their overall security posture, were able to accomplish more with less.

In the words of one participant, "CORE IMPACT is a 'force multiplier.'" By using an automated penetration testing tool, such as CORE IMPACT, the IT staff can immediately check to ensure that any changes to the IT infrastructure do not inadvertently create new vulnerabilities. This timeliness and the ability to quickly identify real vulnerabilities with the volumes of vulnerability reports free the IT staff to pursue other mission-critical assignments.

"CORE IMPACT is a 'force multiplier.'"

The Need for Proof

Generally, IT staffs are overwhelmed with tasks. They spend their day making sure their IT infrastructures provide valuable services. Because they are so involved in their work, they feel that their systems are unassailable. They can't imagine that anyone could get into *their* systems. When it comes to thinking about their systems being vulnerable, they take a "show me attitude." They will believe you when you can demonstrate that you can do what you say you can. Penetration testing is the only process and discipline that is capable of providing factual information about real vulnerabilities that may exist in an IT infrastructure. When penetration testing is executed, the infrastructure is subjected to rigorous tests that follow a sophisticated pattern or series of steps an attacker might take to leverage vulnerabilities. It allows people to see exactly what an attacker can do. There is no question about whether the vulnerabilities are real or false. When IT staffs see this capability, they generally agree that it is valuable to address specific problem areas instead of spending the day putting out the "fire of the day." They can address security needs quickly and spend the rest of their time providing valuable IT services.

If Enterprises Don't Adopt Penetration Testing... ?

The Cost of Breaches

Hackers and other individuals possessing the technical know-how and access to sophisticated hacking tools have joined forces with criminal elements to exploit vulnerabilities for financial gains. A single breach of a company's security can result in severe damage to a company's reputation and brand. The direct and indirect consequences of a single breach are significant and include the potential for loss of revenue, customers, and investor confidence as well as regulatory fines and possibly even litigation.

To properly address these classes of security threats, professional IT staffs need to avail themselves of the most sophisticated tools and technologies. These tools will enable them to probe their security infrastructures in the same way an external hacker or insider would. By utilizing penetration testing, IT professionals are able to conclusively establish that no "hidden" vulnerabilities exist in their infrastructures at the time the scan is executed.

Government Intervention

Federal, worldwide, and local governments have recognized the escalating number of criminal activities and thefts resulting from inadequate and, in some cases, nonexistent protection of confidential and personal data possessed by companies. As a consequence, governments have been passing legislative mandates that hold companies and their executives accountable for the protection of such data.

Existing and pending government regulations such as GLBA, HIPAA, and Sarbanes-Oxley (SOX) provide such mandates. Specifically, SOX requires public companies to undergo periodic audits of their security policies and procedures. These mandates clearly place the responsibility on senior company executives and board members to ensure that established security policies and their implementation offer maximum protection of customer, employee, and partner information. Companies and executives in violation of these regulations may be subject to criminal penalties and severe fines, and executives may face jail terms.

The problem with most of these mandates is that meeting the requirement doesn't necessarily make enterprises secure. In many cases, the compliance level is just the bare minimum. Also, with so many regulations to meet, there is the problem of overlapping conflict. However, all compliance standards have one thing in common — an audit trail. By implementing a strong penetration testing program, enterprises can provide the information they need to meet compliance data requirements, but most importantly they will be gathering invaluable information that will improve their real security posture.

Privacy regulations are also surfacing worldwide — in Europe (the European Union Data Protection Directive); Japan (the Japanese Personal Information Protection Act [JPIPA]); Hong Kong, SAR China; Taiwan; and New Zealand — and the trend shows no signs of abating.

VULNERABILITIES IN PERSPECTIVE

Historical Overview

Security vulnerabilities are discovered nearly every day. These vulnerabilities are likely to be found in the systems or subsystems contained within an IT infrastructure. Vulnerabilities in these components are the result of unintentional built-in defects in appliance microcode, server systems, application software, and even security hardware and software components, which are specifically designed and purpose-built for business and enterprise security. In addition, vulnerabilities exist because of end-user actions (e.g., launching attachments from unknown sources). Table 1 shows the unabated growth of reported system vulnerabilities since 1995.

TABLE 1

CERT/CC Statistics, 1995–2005

	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Number of system vulnerabilities reported	171	345	311	262	417	1,090	2,437	4,129	3,784	3,780	5,990

Source: CERT/CC, 2006

Vulnerability assessment is an ongoing IT task. The dynamics driving today's business environment force continual change in components or their configuration. New components are added, others are upgraded or patched, and some become obsolete and are removed. All changes must be analyzed and tested to evaluate how they impact known and unknown vulnerabilities. Ideally, an organization must test the infrastructure for vulnerabilities as often as changes are made to IT infrastructure components and/or their associated policies.

IDC believes that the only way an organization can know its true vulnerability risks is to take a "hacker's eye" approach to evaluating the effectiveness of its internal and external defenses. With an automated penetration testing product, such as CORE IMPACT, IT professionals learn what is possible and become key proponents of conclusively determining if there are any exposed internal or external vulnerabilities and proactively addressing them.

BENEFITS OF PENETRATION TESTING

To provide a broad perspective of the impact that penetration testing has had on enterprises that have incorporated Core Security Technologies' CORE IMPACT product into their SVM programs, this section outlines a summary of the strong impact and benefits of penetration testing from the business and IT perspectives.

Business Benefits

- Saves hundreds of thousands of dollars in remediation and notification costs by avoiding network downtime and/or averting a single breach
- Lowers the costs of security audits by providing comprehensive and detailed factual evidence of an enterprise's ability to detect and mitigate risks
- Creates a heightened awareness of security's importance at the CXO management level
- Provides unassailable information usable by audit teams gathering data for regulatory compliance
- Provides a strong basis for supporting approval of larger security budgets
- Provides support to evaluate the effectiveness of other security products, either deployed or under evaluation, to determine their ROI

IT/Technical Benefits

- ☒ Allows IT staff to quickly and accurately identify real and potential vulnerabilities without being overburdened with numerous false positive indicators
- ☒ Allows IT staff to fine-tune and test configuration changes or patches to proactively eliminate identified risks
- ☒ Assists IT in prioritizing the application of patches for reported known vulnerabilities
- ☒ Enhances the effectiveness of an enterprise's SVM program
- ☒ Provides vulnerability perspectives from both outside and within the enterprise
- ☒ Is a force multiplier when it comes to overall impact on IT resources and significantly enhances the knowledge and skill level of IT staff

As the preceding summary illustrates, enterprises that have adopted automated penetration testing as part of their overall SVM programs have clearly and significantly benefited in critical areas of their business and operations. In IDC's discussions with CORE IMPACT users, a vice president of information security in the communications industry stressed the following point: *"Penetration testing is one of the necessary tasks of an IT security group. It may be 5% to 10% of the overall workload, but it is a critical piece. Penetration testing internally and externally, with focus on the inside, has provided us the biggest way to remediate our risks."*

ADVANCES IN SECURITY ASSURANCE: CORE IMPACT

Since its inception in 1996, Core Security Technologies has been fully dedicated to information security, originally through its Security Consulting Services group and its CoreLabs research and development arm and later through its CORE IMPACT software. When Core Security Technologies was performing penetration testing as a service vendor, it realized that enterprises needed a comprehensive penetration testing tool that they could constantly use. With a tool that could accurately gather and report specific information about a company's potential security vulnerabilities, the practice of penetration testing could become more professional and scalable. Core Security Technologies took its penetration testing knowledge and released CORE IMPACT in 2002.

CORE IMPACT, the company's flagship product, eliminates the need for highly skilled penetration testing experts who are in short supply, making it practical and affordable for companies and enterprises to conduct necessary penetration testing in-house even when security budgets continue to be squeezed. When used effectively, CORE IMPACT virtually eliminates the ambiguities created by false positive and negative occurrences that result from generic vulnerability assessments. It also provides valuable information on the effectiveness of patching. With CORE IMPACT, it is possible to determine if the patch was successfully installed, if it creates a vulnerability (e.g., by changing a setting), or if it can help to prioritize patching efforts. A vice president of information security in the

communications industry said, *"Core single-handedly has been responsible for our patching practices improving 100% over the past three or four years since we have had that tool. As a result, our security internally on our network has improved quite significantly."*

"Core single-handedly has been responsible for our patching practices improving 100% over the past three or four years since we have had that tool. As a result, our security internally on our network has improved quite significantly."

The product provides a comprehensive software framework for IT personnel to perform penetration tests frequently. The methodology and tool set increase the productivity of testers by automating the penetration testing process. The product captures knowledge acquired by the testers by logging all methods and results, which ensures timeliness in eliminating exploits through real-time updating, and provides actionable results for management decision making.

CORE IMPACT consolidates in one application the ability to perform a penetration test without being reliant on highly sophisticated experts and various software tools or methodologies. To accomplish this, CORE IMPACT:

- Makes available valuable resources for important penetration testing phases:
 - High-level overview and analysis
 - Strategic attack planning
 - Results analysis
 - Recommendation formulation
- Encompasses all phases of a penetration test in a single framework
- Defines and standardizes the penetration test methodology for maximum efficiency and replication of effort
- Enforces the use of an organization's methodology and ensures quality results
- Improves the security of the penetration testing practice itself
- Simplifies and speeds execution of monotonous and time-consuming tasks
- Improves the information security of the organization in which it is implemented

Integrated into one application framework, CORE IMPACT consolidates the ability to perform a professional penetration test without being reliant on diverse software tools or varied manual means. CORE IMPACT provides a consistent methodology and broad set of tools to the penetration tester. Its architecture provides the efficiency and in-depth analysis required for scrupulous assessment of enterprise vulnerabilities. Additionally, CORE IMPACT has the following characteristics:

- User-friendly interface.** The CORE IMPACT console presents all phases of a penetration test in an intuitive graphical interface, including when running modules on different operating systems and architectures.

- ☒ **Commercial-grade exploit code.** CORE IMPACT provides the penetration tester with a range of up-to-date, professionally developed and maintained exploits for different platforms, operating systems, and applications, including multiple combinations of these elements. CORE IMPACT exploits allow the penetration tester to both audit for vulnerabilities and exploit the vulnerabilities to penetrate the target host or application.
- ☒ **Transparent attacking.** CORE IMPACT permits attacks to run from intermediate compromised hosts without modification (i.e., once a machine is successfully attacked, a new attack can be launched from the compromised machine). This powerful capability allows the tester to seamlessly stage or proxy attacks through intermediate hosts.
- ☒ **Information-gathering tools.** CORE IMPACT includes information-gathering modules ranging from network discovery and Nmap to port scanning and operating system stack fingerprinting. These modules can be run from any acquired system without modification. Integration with other common information-gathering packages, such as vulnerability scanners, is provided in the form of import modules.
- ☒ **Logging and storage of test data.** Information about the target network is accumulated during the penetration test, and all CORE IMPACT-initiated penetration testing activities are logged and stored in a structured format inside a CORE IMPACT database. This always up-to-date view of the target system aids the tester in conducting high-level strategic analysis of a current scenario, as well as in reporting results of the test at a later time.
- ☒ **Customizable framework.** CORE IMPACT provides a framework that is adaptive to the tester's definition and redefinition of methodologies and targets. CORE IMPACT lets users develop and customize new or existing tools quickly, thus maximizing IT efficiency by reusing knowledge and experience from successive penetration tests and different penetration testing teams. It also provides the framework for advanced users to design exploit code and scripts.

GOOD-ENOUGH OR REAL KNOWLEDGE

Cybercriminals are becoming more sophisticated and are making use of state-of-the-art tools to steal high-value data for profit. Many existing security solutions are not being used effectively enough to thwart dedicated attackers. However, many enterprises have a dilemma. They need to be secure, which requires considerable resources, but some enterprises must meet mandatory regulatory requirements or pass the scrutiny of an audit. If enterprises do just enough to pass an audit, they may be dealing with a requirement, but they will not be providing the necessary level of protection.

The real goal of security must be to protect enterprises from any serious breach, which inevitably will result in severe negative consequences for their business, clients, and executive management.

Enterprises that institute security measures and policies simply to meet regulatory mandates or to pass the scrutiny of an audit won't make the grade in providing maximized levels of protection from breaches. However, many enterprises just will not budget for the tools, such as penetration testing, that will inform them if their other security investments are meeting a specific security need.

The greatest challenge for a company such as Core Security Technologies is to make enterprise buyers understand that the money spent on penetration testing software isn't a pure expense, which is what many see, but instead is a value-add that provides real risk information and allows for the proper allocation of security resources. Core Security Technologies has been providing this information, and based on the input from its customers, CORE IMPACT is demonstrating its value.

CONCLUSION

Through interviews with IT executives in a diverse range of industries, IDC found that companies that have incorporated Core Security Technologies' CORE IMPACT product into their new or existing SVM programs have been highly successful in detecting, eliminating, and managing both known and unknown vulnerabilities.

CORE IMPACT is a highly efficient and cost-effective solution for conclusively determining and addressing the real and demonstrable security risks that enterprises will continue facing for the foreseeable future.

IDC believes that penetration testing must be a required component of an enterprise's SVM program.

METHODOLOGY

The results presented in this white paper are based on current and historical research undertaken by IDC. As part of this research effort, IDC also conducted in-depth interviews with senior enterprise IT executives who have incorporated automated penetration testing as part of their overall SVM programs. Summary comments of their experiences are also presented in this paper.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.