

I D C E X E C U T I V E B R I E F

Penetration Testing: Taking the Guesswork Out of Vulnerability Management

January 2007

Adapted from [Worldwide Vulnerability Assessment and Management 2004–2008 Forecast and 2003 Vendor Shares: Assessing Risk and Compliance](#), by Charles J. Kolodgy; IDC #32026

Executive Overview

Today, IT managers currently have limited capability to assess real risk, technically validate the effectiveness of security products they use, and make intelligent IT security investment decisions.

This Brief will discuss how penetration testing software can efficiently address these challenges. Penetration testing is an important addition to the vulnerability assessment and management (VA&M) portfolio in that it picks up where "scan and identify" products leave off, substantiating whether theoretical threats to network security are real or not. Penetration testing software provides the capability to test the overall IT security infrastructure and polices to ensure that an organization's security investments are actually working. This capability will become increasingly important as companies continue to spend more on solutions to protect their information assets and meet compliance requirements. Management will need to justify those investments by proving that they are indeed paying off.

Penetration testing is necessary for organizations to:

- Understand the actual risk to their business posed by specific vulnerabilities
- Test the security of their network
- Determine if their current security investments are actually detecting and preventing attacks

Penetration testing software represents the best option for doing so.

Introduction

The network security efforts of IT managers have so far been focused on keeping the bad guys at bay. Traditionally, this has been accomplished by trying to outsmart hackers by creating barriers or providing defensive mechanisms once a vulnerability was identified. As networks become more complex, however, it's impossible to protect everything. Instead, managers need to prioritize their security to protect the most critical assets and ensure the technology they have deployed is functioning as effectively as possible. Vulnerability scanners can help, but the list of potential vulnerabilities produced by a scanner can be dauntingly long and not wholly accurate.

Additionally, managers should probe deeper to understand the true threat to assets when specific vulnerabilities are exploited on their network. A new class of penetration-testing software products has emerged to do this. These products represent a potential solution for managers to test the security of a network, identify what resources are exposed, and determine if current security investments are actually detecting and preventing attacks. This Brief examines key trends in the vulnerability assessment and management (VA&M) market and identifies the value of penetration testing as part of a comprehensive security methodology.

The Need for Better Vulnerability Management

IT infrastructure is getting more complex, and wider access to internal networks is being granted to credentialed users located outside the firewall. Today, IT managers currently have limited capability to assess real risk, technically validate the effectiveness of security products they use, and make intelligent IT security investment decisions.

In addition, the following factors are driving demand for better vulnerability management solutions:

- **Organizations need something more than a status check and a laundry list of items to fix.** Scanners are good for detecting potential flaws, but companies need to know not only what vulnerabilities they have, but also a means of measuring policy compliance and risk management. Most organizations do attempt to patch known vulnerabilities, but patching everything is not a practical or necessary step in every case. Furthermore, enterprises need to understand their organization's true exposure in the event of a "real" security compromise.
- **Government requirements for security and privacy have become more demanding.** Organizations of all sizes have to be concerned about their ability to measure their compliance to security requirements. For example, regulations such as HIPAA, GLBA, FDIC, FISMA, and Sarbanes-Oxley mandate that organizations regularly test the security of their networks and provide audits of those findings. As companies expand their use

of additional security products and services, they are also seeking ways to measure their risk.

These factors are helping to drive the growth of the VA&M software market, which achieved \$435 million in vendor revenue in 2003. IDC expects the worldwide revenue for VA&M software to reach \$871 million in 2008, representing a compound annual growth rate (CAGR) of 15% from 2003 (see Table 1).

Table 1

Worldwide Network and Host Vulnerability Assessment & Management Software Revenue, 2003–2008 (\$M)

	2003	2004	2005	2006	2007	2008	2003–2008 CAGR (%)
Network	178.7	215.4	259.6	299.3	341.3	381.5	16.4
Growth (%)	18.2	20.6	20.5	15.3	14.0	11.8	
Share (%)	41.1	41.8	43.0	43.1	43.5	43.8	
Host	256.4	300.6	344.1	395.1	443.3	489.4	13.8
Growth (%)	15.1	17.2	14.5	14.8	12.2	10.4	
Share (%)	58.9	58.3	57.0	56.9	56.5	56.2	
Total	435.1	516.0	603.8	694.3	784.6	870.9	14.9
Growth (%)	16.4	18.6	17.0	15.0	13.0	11.0	

Source: IDC 2004

As the market grows, security technology is becoming more specialized, with vendors designing products to target specific pain points. One pain point is the need to measure security effectiveness, and vulnerability management products such as penetration testing software provide the security measurement that enterprises require.

Penetration testing is a localized, time-constrained, and authorized attempt to breach the security of a system using attacker techniques. During a penetration test, organizations actually try to replicate in a controlled manner the kinds of access an intruder or worm could achieve. With a penetration test, network managers can identify what resources are exposed and determine if their current security investments are detecting and preventing attacks.

It is necessary for organizations to understand the actual risk to their business posed by vulnerabilities, and a penetration test is the best option.

The Rise of Penetration Testing

IDC expects that proactive security, as embodied in penetration testing, will take a larger share of the market over time compared with passive security, as represented by vulnerability scanning. Penetration testing products attempt to exploit potential vulnerabilities that the vulnerability scanner identifies. In effect, penetration testing software discovers which theoretical threats are, in fact, actual threats, and prioritizes which are most critical in a network.

The software has essentially productized what used to be a costly and time-intensive professional service. Until recently, penetration testing had been a very complex manual process that could be performed only by a select few security specialists with years of experience. This software-replaces-services model is taking hold in many security markets.

In the absence of penetration-testing software, a company has the following two options:

- **Hire a consultant who uses proprietary and publicly available software.** The results, however, will not be consistent across all environments and, therefore, not repeatable and scalable. Also, effectiveness will depend on the skill of the tester, not the quality of the product.
- **Internally develop penetration-testing capabilities.** It's difficult to find security professionals with sufficient knowledge, and publicly available tools are not quality assured, which can sometimes backfire. The fact that this option requires a lot of time from a highly specialized team invariably makes it expensive.

Penetration testing offers the following benefits in two areas: business and IT.

Business Benefits

- Informs companies as to whether the security infrastructure (IPS, IDS, firewalls) they've bought so far is working and delivering the expected level of security.
- Tells companies whether critical business information is exposed.
- Helps companies comply with regulatory mandates around informational security and privacy. Penetration testing allows organizations to be better prepared for audits and to meet regular network testing requirements of HIPAA, FDIC, GLBA, FISMA, and Sarbanes-Oxley.
- Helps companies allocate IT security resources more efficiently and effectively.

IT Benefits

- Saves time by exposing vulnerabilities and subsequent network information or resources that are at risk. Network administrators are better able to prioritize the volumes of information received from a vulnerability scanner, saving days and weeks of time otherwise spent on finding a network's true weak points
- Helps IT managers conduct more comprehensive security audits. Penetration testing provides the ability to test for vulnerabilities as they relate to how network components work together
- Enables a proactive rather than reactive approach to making informed security decisions. Penetration testing lets network administrators view their network through the eyes of an attacker to prevent attack
- Allows IT managers to justify further security expenditures more convincingly

Market Drivers Supporting Penetration Testing

Risk Management

As networks become more complex, it is not possible to protect everything. Instead, managers need to prioritize their security to protect the most critical assets.

Vulnerability scanners can determine what is theoretically vulnerable, but that information needs to be overlaid with the value of the asset to operations. Without physically penetrating the host or network, there is no way to quantify and qualify an organization's true exposure in the event of a "real" security compromise. Many products in the VA&M space are designed to help managers make informed risk management decisions.

Vulnerability Remediation

The vast majority of attacks, including automated worms, are performed against known vulnerabilities that have patches available. However, ensuring that patches are up to date, properly applied, and that they effectively remediate the problem vulnerability is a difficult task.

Sometimes patching is not the best or only solution. Options can include segmenting the affected system from the network, inserting a firewall, reconfiguration, or other security solutions.

VA&M solutions are being asked to discover the existing patch level and to determine what vulnerabilities exist at that patch level. New vendors are emerging in this area, as well as existing vulnerability vendors that are partnering with patch and remediation companies to provide solutions tied to their vulnerability products.

Software Evaluation and Vulnerability Testing

Software security vulnerability products geared to software developers and quality assurance are growing in popularity. VA&M procedures can be valuable tools in making other security products better. By using the output from penetration testing, intrusion detection and intrusion prevention products can become more accurate.

VA&M Usage by SMB Market

Small- to medium-sized businesses need to be able to demonstrate that they are meeting government-mandated security requirements. These businesses must also comply with larger enterprises, which often require that a small business have an acceptable security-posture status prior to connecting into the larger company's systems.

These developments will increase the need for VA&M that can meet the specific needs of the small- and medium-business (SMB) market and the IT consultants that service them. Indeed, VA&M services delivered via the Web are becoming quite popular in this segment.

Considerations

Budgetary and staffing constraints will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure. Penetration-testing software products can simplify the complexity associated with managing multiple security solutions, while increasing the effectiveness of the protection.

Vulnerability management is essential. IDC believes that VM will eventually split into pure vulnerability scanners and vulnerability assessment management. In the latter category, penetration testing will bring the following to the process:

- Provide actionable items / prioritization / real results, tied to business assets
- Interoperate with other security products or devices, such as vulnerability scanners, firewalls, and intrusion detection and prevention, in order to improve risk management
- Assist in smart remediation of vulnerabilities beyond patch management, such as network segmentation, firewalling, and/or deploying intrusion detection and prevention
- Validate that applied remediation efforts are effective in plugging the found vulnerabilities
- Provide detailed audit reports for regulatory compliance

Vulnerabilities must be viewed as part of an overall security management infrastructure that takes into account security policy and compliance and risk management. VA&M solutions should be expected to inform IT managers why the vulnerability is a concern and how each specific vulnerability is ranked, so that remediation can be performed in a consistent prioritized manner instead of chaotically.

Network and systems administrators should consider implementing penetration testing under the following conditions:

- The organization has or is evaluating deployment of an IPS, IDS, and/or vulnerability scanner
- There is a need to manage vulnerabilities more efficiently
- There is a need to comply with regular testing aspects of Sarbanes-Oxley, GLBA, FDIC, FISMA, and/or HIPAA
- There is difficulty justifying additional security expenditures, or there is a need to improve decision-making processes

Conclusion

The growing reliance on IT for corporate operations and the increasing government and industry regulation are elevating security policy, adherence to best practices, and measurement to a critical component of corporate governance. To meet these needs, vulnerability assessment and management (VA&M) products are being released that can assist enterprises in handling policy creation, compliance measurements, increased efficiency, and audits as well as reporting.

Penetration testing software is an important addition to the VA&M portfolio to the extent that it picks up where "scan and identify" products leave off, revealing theoretical threats to network security as real or not. Penetration testing software provides the capability to test overall security architecture to ensure that an organization's security investments are actually working.

This capability will become increasingly important as companies continue to spend more on solutions to protect themselves. Management will need to justify those investments by proving that they are indeed paying off.

To assess real risk, technically validate the effectiveness of security products they use, and make intelligent IT security investment decisions, organizations should implement penetration testing software products.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2007 IDC. Reproduction is forbidden unless authorized.