

Practical Aspects of Vulnerability Assessment and Penetration Testing

by Joel Lanz

Failure to manage security, improper configuration of technology assets, excessive trust or privileges, and insufficient monitoring activities are the main culprits that allow unauthorized penetration of data. Joel Lanz examines the relative strengths of vulnerability assessment tests and penetration tests.

The enactment of the Sarbanes-Oxley Act of 2002 requires that CEOs and CFOs be responsible for establishing and maintaining internal controls to ensure they are notified of material information. To ensure compliance with both traditional and recently enacted regulations, many banks are reviewing their information integrity and data protection strategies as well as their processes. The *penetration test*, the traditional favorite of executive management and board members, is an independent test used to simulate the probable actions of unauthorized users (both external and internal to the bank) to infiltrate technology systems and the confidential data they hold.

Many executives, however,

are challenged by the concepts of vulnerability assessments and penetration tests. The terms not only are confusing to those not familiar with the technology aspects of each, but also are frequently used interchangeably by consultants performing the testing. It's difficult to appropriately supervise the external testers to ensure minimal productivity disruptions from high-risk penetration activities and to prevent the testers from gaining access to privileged information. Adding to the confusion is the lack of generally accepted penetration testing standards, which can cause decision makers to rely on poor or incorrect testing procedures. The buyer and user of these services also can be challenged by incorrect assumptions relating to the pur-

pose and use of vulnerability assessments and penetration tests.

Common Exposures Provide Unauthorized Access Opportunities

A jointly issued report from the FBI and the SANS Institute (Top 20 List)¹ identified the most commonly exploited vulnerabilities in two popular technology environments—UNIX and Windows. The report found that “the majority of the successful attacks on operating systems come from only a few software vulnerabilities. . . [and are] attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools.”² Analysis

© 2003 by RMA. Joel Lanz leads a technology assurance and advisory CPA practice; he is the leader of the New York State Society of CPAs Technology Assurance Committee Task Force on Security and Privacy; and he is an adjunct faculty member at Pace University.

of the causes of items appearing in the Top 20 List, as well as prominent security texts and studies,³ identify four conditions that facilitate successful attacks.

1. Failure to manage security. In his classic text on management, Peter Drucker identified five basics for managers: setting objectives, organization, communication, measurement, and development of people.⁴ Unfortunately, when it comes to managing security, many managers do not adhere to Drucker's advice.

While some organizations implement a combination of policies, procedures, and guidelines, these are typically generic and do not assign accountability to departments and individuals. This results in the failure to effectively communicate security responsibilities to individuals and to hold them accountable for their actions. A classic example of this failure is the security exposure that exists with transferred or terminated employees. Most corporate policies are specific as to who may approve access privileges for specific individuals, but these same policies do not address the manager's responsibility to adjust a subordinate's access privileges as the latter's job responsibilities change. Seldom are these managers punished for subjecting the organization to the increased risk.

Weak, easily guessed passwords are another symptom of poor management involvement with security. Many managers do not leverage readily available software features to enforce an appropriate password policy nor do they educate subordinates on the

importance of using passwords⁵ that minimize invasion opportunities or the ability to guess the word. The general public can access a number of password-cracking programs, such as L0pht-crack and Crack, to easily identify passwords in a relatively short time. In addressing the subject of poor passwords, a well-known white-hat hacker⁶ claims, "I've watched Crack chew through a 10,000-entry password file and spit out nearly 1,000 valid logins in less than an hour."⁷ These claims do not include the most dangerous passwords—default passwords that ship with software or hardware and that should be changed during implementation. Typically, these passwords are powerful and well known in the general technology community.

Information leaks give attackers just enough information to convince an authorized user that the former can be trusted with sensitive information. As in the western movies where a bank robber would "case the joint" before committing the crime, the unauthorized individual "cases" available information—whether from the Internet, overheard conversations in public places, press releases on software purchases, trash, or any other means. Gathering this information is the first step toward developing the appropriate reconnaissance needed to gain access to sensitive computer privileges and data.

2. Improper configuration of technology assets. To facilitate customer implementation and use of their products, technology vendors ship their products with

the least restrictive security. To achieve adequate levels of control, the customer must configure the asset for the desired security level. With deadlines and various pressures to prepare for systems conversions or implementations, this "hardening" requirement is postponed until after the implementation and then frequently forgotten. This issue affects the vendor as well. Recent headlines, such as the formation of a \$30-million effort to improve software reliability, has focused attention on how poorly developed software results in U.S. companies spending \$175 billion to repair damages caused by software defects.⁸

Unpatched or outdated software has always been a frequent target of attacks. Typically, a vendor is forced to issue a patch if there is something wrong with its software. The vendor also corrects various defects as it releases newer versions of software. By attempting to identify organizations that have not patched or updated its software, the attacker is identifying organizations that continue to have defects that can be exploited. Frequently, the exploitation strategy for a particular defect is readily available after the defect has been publicized by distribution of a patch or other means.

Improperly configured firewalls and routers can have damaging security effects too. A firewall (including a router for the purposes of this article) acts as a border guard. Many organizations maintain a false sense of security, believing that because they have purchased and installed a firewall they are protected from malicious attack. Similar to the border

guard's initial training, the firewall needs to be properly configured to enforce the organization's security policies. Since the world constantly changes, border guards receive continuous training to ensure that the latest risks can be identified, and the same applies to a firewall. The configuration of firewalls and routers needs to be constantly tested to ensure that they are protecting the enterprise.

With the advent of customer-interfacing systems such as Web banking, Web servers are another example of a technology resource that needs to be properly configured. Patch management and the judicious use of services available on the server are two strategies to limit the risk of unauthorized Web exploitation.

3. Excessive trust or privileges. Users of computers or other technology resources must earn the trust to initiate and process actions. Once appropriately earned, access privileges are no longer questioned. This is like a flight with a layover or change of planes in a hub airport; passengers don't need to go through a second security check at the hub as long as they remain in the secured area. Also like airport security, certain programs or users, based on the function performed, have privileges that enable them to bypass detailed security checks.

Given that *a majority of unauthorized access attempts originate with internal users*, it is no surprise that user accounts with excessive privileges are a primary example of this exposure. Typically, users have access privileges in excess of their job requirements. Again, this could

result from management failure to adjust privileges as job responsibilities change. It could also result from ignorance in not assigning privileges on a need-to-have basis.

Programs, directories, and files also may have excessive privileges. Many organizations have implemented systems that require unrestricted access to system resources for vendor applications. Another variation is trusted programs, such as those from the operating system vendor, that bypass security checks. Running excessive services or services not needed, although shipped with the product, further complicates the administration of security privileges. Finally, trusting one computer system or another (either the same company or a trusted vendor) can lead to exploitable conditions if the partners have not ensured that they each provide similar diligence over security practices.

4. Insufficient monitoring activities. Despite the technological complexity, the rules of basic risk management apply in promoting effective security. If an enterprise cannot prevent an activity, it should be able to detect the activity and evaluate its appropriateness by implementing monitoring tools. Most systems come with these tools, but they are frequently disabled because they might have a negative effect on systems performance and resource use. Even if they are not disabled, the commitment of resources to review and follow up on these activities can be a burden. Remote access, privileged user activity, changes to critical system resources, and potential intrusion activities are

examples of issues that should be monitored.

The Risk Manager Strikes Back

It's easy to understand the need for greater concern over system confidentiality, integrity, and availability. Fortunately, there is much material available and freely shared in the security community, including the actual tools used by attackers along with the guidance to effectively interpret the results. As written in the introduction to a leading text on defending against attacks, "To create an effective defense, we must understand the offensive tools used by our adversaries. By seeing how the tools truly work and understanding what they can do, not only can we better see the needs for good defenses, but also we can better understand how to apply the appropriate defensive techniques."⁹ Here is where vulnerability assessments and penetration testing enter the picture.

The bad news is that a generally acceptable standard for these tools does not exist. Many buyers and users are at the mercy of a book on hacking devices or an external service provider's opinion as to what constitutes an assessment or a test. Interestingly, the diversity of fees for performing these tests demonstrates the wide scope, practices, and opinions relating to what each are and what the providers believe are within the scope.

A single standard is currently being considered. The Information Technology Laboratory at the National Institute of Standards and Technology (NIST)¹⁰ has recently released a

Practical Aspects of Vulnerability Assessment and Penetration Testing

draft document that can help risk managers appropriately scope their vulnerability assessment and penetration testing activities while serving as a benchmark for comparing the testing services offered by various consultants—*Draft Special Publication 800-42, Guideline on Network Security*

Testing. This document describes a methodology for using network-based tools for testing systems for vulnerabilities. The primary aim of the document is to help administrators and managers get started with a program for testing on a routine basis. The methodology recommends focusing first on

those systems that are accessible externally—firewalls, Web servers, and so forth—and then moving on to other systems as resources permit. The document includes many pointers to various testing applications and contains more detailed descriptions of several of the more popular test tools.

Figure 1

Comparison of Vulnerability Assessments and Penetration Testing

	Vulnerability Assessments	Penetration Testing
General Description	Identify vulnerabilities automatically through use of software rather than relying on human skills.	Test to determine if an outside party can penetrate existing organizational defenses both from a technological and social perspective.
Strengths	Runs easily and quickly, enabling ongoing monitoring. Freeware or inexpensive tools available, some of which provide advice on how to fix the identified vulnerability. Excellent method for identifying basic issues.	Simulates actual hacker process to the extent possible. Demonstrates the practical risk of identified vulnerabilities by exploiting the latter to gain entry. Assess effectiveness of user security awareness and training by leveraging social engineering.
Weaknesses	Can create significant amounts of network traffic, slowing overall performance. Easily detected by technology staff. Susceptible to high false positive rate. Often misses new vulnerabilities.	Can result in false positives due to lack of generally accepted testing standards. Requires great expertise. Need to consider legal and regulatory impacts, especially if technology resources are outsourced. Provides a sample and is not intended to identify all vulnerabilities.
Why Perform	Obtain understanding on what's connected to the organization's network. Facilitates the identification of software that is outdated or needs patching. Can identify the most common security threats resulting from configuration management.	Excellent tool to use if organization is trying to determine the effectiveness of security given various levels of efforts by unauthorized individuals (considering that any system can be penetrated with unlimited resources). Serves as a "wake-up" call for organizations that have not taken security seriously.
Representative Action Steps	Identify what's on the network, including hosts and open ports. Update assessment tool for technology resources used and latest developments. Scan for compliance with policies and version/patch management issues.	Define and confirm rules of engagement. Identify relevant information through footprinting, scanning, and enumeration. Leverage info gathered to make an informed attempt at the target. After gaining basic access, attempt more significant privileges or rights. Gain access to privileged and sensitive data. Document evidence of access as appropriate.
Typical Findings	Inventory of vulnerabilities. Patch or upgrade systems as required. Tighten configuration management program. Ongoing monitoring of vulnerability alerts and mailing lists to identify evolving threats. Modify security policies as needed.	Poor security monitoring by technology group. Ignorance of user security awareness and responsibilities. Access to privileged and confidential information. Specific vulnerability exploited and how. Poor incident response procedures.
Frequency	Every one to three months, depending on the environment.	Annually.
Popular Tools Used	Nessus, ISS Internet Scanner, CyberCop Scanner, SAINT, and SARA.	Anything needed to gain access, including war dialers, Nmap, Nessus, L0phtcrack, John the Ripper, Dsniff, Hunt, Netcat, RootKit, and many others.

Practical Aspects of Vulnerability Assessment and Penetration Testing

The NIST document identifies and describes a number of popular network security testing techniques¹¹, including vulnerability assessments and penetration testing. The NIST defines the two tests as follows:

1. **Vulnerability Assessment (Scanning)**¹²—Provides system and network administrators with descriptions of various tools that can be used to proactively identify vulnerabilities before an adversary can. Scanning helps identify out-of-date software versions, vulnerabilities, and applicable patches or system upgrades, while validating compliance with, or deviations from, the organization's security policy.
2. **Penetration Testing**¹³—A security test in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques developed by hackers. Basically, vulnerability assessments are used to identify and inventory various exposures within the organization's systems. Penetration testing attempts to exploit any one of the vulnerabilities to gain unauthorized access. It is important to note that penetration testing does not provide a complete inventory of exposures, but does identify those exposures exploited to gain access. Without a generally acceptable standard, at best, the penetration test can only be evaluated against a given level

of effort—typically, hours of effort based on the tester's fees. The two test techniques are further compared in Figure 1.

Basic Lessons

No matter which test is employed, risk managers can derive a number of lessons from vulnerability assessments and penetration testing to help them significantly improve their security environments (as well as enhance test results from external audits) and avoid embarrassment.

Identify all doors. Many executives take a simplistic view of security. The typical perspective is that there is only one access point to guard. But with the advent of Web-enabled and client/server technologies, there are many doors. In identifying access points, multiple combinations of data transmission layers and servers need to be assessed and protected.

Monitor security-related advisories and updates. Well-respected, security-related organizations, such as CERT and SANS, distribute free newsletters providing guidance on recent and projected security threats. The risk manager needs to monitor these and, based on the severity of the issues identified, take necessary actions.

Use available assessment tools. By periodically running freeware tools, such as the Top 20 List, risk managers can mitigate the risk resulting from popular vulnerabilities. Additionally, benchmarking tools provided by the Center for Internet Security,

an organization sponsored by key audit and security groups, will help ensure that technical platforms have been sufficiently hardened to reduce external threats.

Apply security patches in a timely basis. Finding the low-hanging fruit should always be the top priority—mainly because it is the attacker's first priority. Devastating Web vulnerabilities still exist after years of being publicly known. If a security vulnerability is announced and a patch released, risk managers can be quite confident that unauthorized users will attempt to test the vulnerability. Establishing a reasonable patch management process will significantly reduce the chance of successful attacks.

Change factory default settings. Factory default settings, such as supervisory passwords, are well known in the technology community. Anyone who knows how to do basic research using the Internet can get these lists. Changing these default passwords to confidential passwords is just good business practice.

Enforce need-to-have access. With the majority of unauthorized system break-ins resulting from internal sources, it is imperative that risk managers restrict access on a need-to-have basis. Not doing so is a primary contributor to internal fraud and facilitates the circumvention of management-designed controls. Recent privacy regulations and expectations further require that need-to-have and confidential access be enforced.

Practical Aspects of Vulnerability Assessment and Penetration Testing

Conclusion

No system is impenetrable. Given unlimited resources, a dedicated attacker can succeed. The challenge, then, is to leverage risk management techniques to defend against the most likely and harmful attacks. Security is a team sport that doesn't necessarily require the most fancy equipment to win—but does require mastering the fundamentals of the game. Organizations must constantly give their best efforts to win the fight against attackers. By leveraging the ideas presented here, organizations can more effectively manage the results and expectations of their investments in security testing and significantly protect against attacks. □

ContactLanz at
jlanz@itriskmgmt.com

Notes

1 FBI/SANS Institute, *The Twenty Most Critical Internet Security Vulnerabilities—The Experts' Consensus*, Version 2.6, October 1, 2002.

2 Ibid, p. 1.

3 For example, McClure, Scambray and Kurtz, *Hacking Exposed*, 2001, p. 702.

4 Peter F. Drucker, *Management*, Harper & Row Publishers, 1974, p. 400.

5 Typically, appropriate passwords are more difficult to guess, are greater than six characters, and

contain a combination of regular (a), capital (A), numeric (1) and special characters (@).

6 A white-hat hacker is someone who points out and secures against security holes rather than someone who tries to gain unauthorized access, generally referred to as a black-hat hacker.

7 Dr-K, *A Complete Hacker's Handbook*, Carlton Books, 2000, p. 49.

8 "Tech Consortium Formed to Improve Software Reliability," *Computerworld*, May 20, 2002.

9 Ed Skoudis, *Counter Hack*, Prentice-Hall, 2002, p. 4.

10 Founded in 1901, NIST is a nonregulatory federal agency within the U.S. Commerce

Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

11 Other testing techniques include network mapping, security testing and evaluation, password cracking, log reviews, file integrity checkers, virus detectors, and war dialing.

12 NIST, Draft Special Publication 800-42, p. 13.

13 Ibid., p. 16.

Additional Resources

CERT. Provides practical advice on managing security from both a business and vulnerability perspective. Vendor management and vulnerability trend analysis are especially helpful. (www.cert.org)

Center for Internet Security. Sponsored by the major audit and security organizations, develops consensus benchmarks and automated tools to harden technical resources. (www.cisecurity.org)

NIST. Great reference and thought leadership studies on various security issues, including how-to guides for a number of technology environments. (csrc.nist.gov)

New York State Society of CPAs Technology Assurance Committee Homepage. Provides executive-level presentations and white papers addressing IT governance issues. (www.nysscpa.org)

IT Governance Institute. Excellent collection of papers and presentations from a senior management perspective. (www.itgovernance.org)

SANS Institute. "Knowledge through sharing" is the motto here, with the reading room providing peer-reviewed papers on many security management topics. (www.sans.org)