

Vulnerability Scanning vs. Penetration Testing

By

Joey Rachid, CISSP, CISM
Director, Product Marketing
Digital Defense, Inc.

INTRODUCTION

Information Technology (IT) threats are on the rise. According to the Computer Emergency Response Team Coordination Center (CERT/CC), the number of IT vulnerabilities reported annually has grown from approximately 2,400 in 2001 to more than 8,000 in 2006.¹ That is an increase of approximately 333% over the course of the last five years. That amounts to well over 650 newly identified and reported vulnerabilities every month, challenging even the most sophisticated and well-staffed IT security department to react adequately. Consequently, the days of *reacting* to IT security vulnerabilities are over. Today's IT security world demands a *proactive* approach to vulnerability and risk management.

Stay ahead of IT vulnerabilities by performing proactive network security assessments to paint a *true* and *actionable* picture of your network's security posture.

VULNERABILITY SCANNING

Identification and remediation of network vulnerabilities is the most effective way to minimize the risk of network compromises and potential threats to critical information systems. By performing regularly scheduled internal and external vulnerability assessments, you gain an understanding of your networks' vulnerabilities, and can take action to prevent compromises.

A well-conducted vulnerability scan will: assess the entire network (i.e., internal and external enterprise network assets), provide easy-to-use and accurate vulnerability reporting, facilitate IT asset prioritization according to criticality (i.e., Confidentiality, Integrity and Availability), and enable vulnerability remediation and workflow management

A comprehensive scan will enable you to proactively analyze your networks' vulnerabilities, identify the specific assets affected, and analyze the *true* risk they pose to your business.

Vulnerability scanning supports informed and actionable decisions regarding your network security vulnerabilities, ensuring your ability to identify IT vulnerabilities, take appropriate action, and ultimately reduce network security risks.

PENETRATION TESTING

Penetration testing is an analysis in which you authorize and coordinate with a third party to use known vulnerabilities and methods to attempt to hack into your network systems (external and/or internal). Penetration testing constructs a hacker's view of your network security posture. A penetration test reveals the security holes in your network environment, which can allow a hacker to gain access to critical network resources. A well-conducted penetration test is an independent, third party review of your network vulnerabilities, and provides awareness of the specific methods and exploits used to gain access to your network.

A penetration test generates a *real world* perspective of IT security controls, network infrastructure and network technologies implementation. A penetration test can also identify

weaknesses in IT technologies and applications, which a vulnerability scan will miss. A penetration test also allows you to test IT staff (and employee) reaction to an actual network attack.

Penetration testing validates the efficacy of your network protection. You gain a thorough understanding of weaknesses and mitigation steps to prevent a real network compromise.

WHAT IS THE DIFFERENCE?

Vulnerability scanning identifies network weaknesses that can be exploited by attackers. Penetration testing goes a step further, revealing the consequences of a skilled attacker exploiting identified weaknesses. Implementing a combination of recurrent network vulnerability scans and penetration tests is an excellent way to stay ahead of ever expanding IT vulnerabilities.

A network vulnerability scan generates a proactive assessment and comprehensive view of the current network security posture, empowering you to prioritize, perform, and track risk mitigation efforts. Additionally, a penetration test evaluates network security and identifies methods and areas still vulnerable to attack. A combination of vulnerability scanning and penetration testing provides the ultimate litmus test of your network security posture.

WHY ARE THEY NECESSARY?

In addition to complying with applicable regulatory requirements for recurrent vulnerability scanning and/or penetration testing, these assessments provide a proactive approach to managing network vulnerabilities. Considering that a network compromise costs American businesses an average of \$200 per compromised record (not to mention negative media attention – i.e.: TJ Max), vulnerability scanning and penetration testing are a cost effective method of preventing network compromises.^{II}

WHO SHOULD CONDUCT THEM?

Vulnerability scanning is most commonly performed by internal IT personnel, or by an outside IT security provider. In either case, the person conducting vulnerability scans must possess a technical understanding of your network infrastructure. If you decide to implement a 3rd party vulnerability-scanning product, or choose a vendor to conduct your vulnerability scanning, ensure regulatory compliance authority (i.e., PCI) certification. This establishes the third party vendor is a reputable company offering a reliable scanning solution.

An independent third party should always perform penetration testing. Use of a third party ensures regulatory compliance and provides an outsider's perspective of your network. When looking for a third party to conduct penetration testing, ensure they have successful experience relating to your specific business model. Take the time to understand their penetration testing methodology and the safeguards used to ensure they will not cripple your network while conducting their tests. Always ensure the third party penetration testing team understands the parameters of the engagement; limiting them to conducting only specified types of testing on specified hosts, during specified timelines, etc.

HOW OFTEN?

Conduct vulnerability scanning and penetration testing on a regular basis. Generally, the best practice for conducting vulnerability scanning of critical assets (e.g., web servers, critical databases, routers/firewalls) is daily or weekly, and monthly or quarterly for other assets (e.g., workstations). If your organization does not have the resources to conduct vulnerability scanning at the recommended intervals, make it a budget item; doing something is better than doing nothing.

Conduct penetration testing at least annually. If you have the resources and/or business need, penetration testing can be effective on a more frequent basis. Penetration testing more than once a month, or more often than vulnerability scanning, is not recommended. This provides IT personnel enough time to conduct adequate remediation actions before the performance of another penetration test.

SUMMARY

Vulnerability scanning and penetration testing are proactive tools in today's world of IT vulnerabilities. There is no silver bullet when it comes to protecting your network from malicious compromise; however, implementing recurrent vulnerability scanning with remediation and penetration testing, protects your IT assets and strengthens your network.

As the saying goes, "You don't have to run faster than the bear, just faster than the slowest person." In other words, you do not necessarily need the most secure network, just more secure than the others'. When hackers see your network locked down, they move on to another.

In closing, note that an element of vulnerability scanning and penetration testing that warrants careful consideration is the type of vendor you choose. Experience and reliability are extremely important. An unreliable vendor can wreak havoc on your systems or steal from your organization, and you might not even immediately be aware of it for quite some time. A well-established, experienced vendor will provide you with the service and reliability you need.

^ICERT® Coordination Center (CERT/CC) <http://www.cert.org/stats/fullstats.html>

^{II} Khalid, K. Calculating the Cost of a Security Breach. Forrester.
April 10, 2007.