VeriSign®
The Value of Trust℠

An Introduction to Network Vulnerability Testing

CONTENTS

Introduction

As electronic commerce, online business-to-business operations, and global connectivity have become vital components of a successful business strategy, enterprises have adopted security processes and practices to protect information assets. Most companies work diligently to maintain an efficient, effective security policy, implementing the latest products and services to prevent fraud, vandalism, sabotage, and denial of service attacks. However, many enterprises overlook a key ingredient of a successful security policy: They do not test the network and security systems to ensure that they are working as expected.

Network penetration testing—using tools and processes to scan the network environment for vulnerabilities—helps refine an enterprise's security policy, identify vulnerabilities, and ensure that the security implementation actually provides the protection that the enterprise requires and expects. Regularly performing penetration tests helps enterprises uncover network security weaknesses that can lead to data or equipment being compromised or destroyed by exploits (attacks on a network, usually by "exploiting" a vulnerability of the system), Trojans (viruses), denial of service attacks, and other intrusions. Testing also exposes vulnerabilities that may be introduced by patches and updates or by misconfigurations on servers, routers, and firewalls.

SecureTEST, a security scanning service of VeriSign Consulting, uses proven methodologies and tools to detect vulnerabilities in the enterprise's network, and to then recommend repairs or corrections if necessary. SecureTEST services can be tailored to an enterprise's specific needs and include three levels of assessment. As the industry leader in trust services, VeriSign has the expertise, experience, and technology to recognize and detect security vulnerabilities and to provide effective, enterprise-wide solutions for them.

Penetration Testing Overview

The overall objective of penetration testing is to discover areas of the enterprise network where an intruder can exploit security vulnerabilities. Different types of penetration testing are necessary for different types of network devices. For example, a penetration test of a firewall is different from a penetration test of a typical user's machine. Even a penetration test of devices in the DMZ (demilitarized zone) is different from performing a scan to see if network penetration is possible. The type of penetration test should be weighed against the value of the data on the machine being tested and the need for connectivity to a given service.

The penetration testing process has three primary components:

- Defining the scope
- Performing the penetration test
- Reporting and delivering results

Step 1: Defining the Scope

Before a penetration test can be launched, the enterprise must define the scope of the testing. This step includes determining the extent of testing, what will be tested, from where it will be tested, and by whom.

Full-Scale vs. Targeted Testing

An enterprise must decide whether to conduct a full-scale test of the entire network or to target specific devices, such as the firewall. It is usually best to do both in order to determine the level of exposure to the public infrastructure, as well as the security of individual targets. For example, firewall policies are often written to allow certain services to pass through them. The security for those services is placed on the device performing those services and not at the firewall. Therefore, it is necessary to test the security of those devices as well as the firewall. Some of the specific targets that should be considered for penetration testing are firewalls, routers, Web servers, mail servers, FTP servers, and DNS servers.

Devices, Systems, and Passwords

In defining the scope of the project, the enterprise must also decide on the range of testing. For example, is it looking only for vulnerabilities that could lead to a compromise of a device, or is it also looking for susceptibility to denial of service attacks? In addition, the enterprise must decide whether it will allow its password file to be hacked by the security team to test its users' choice of passwords, and whether it will subject its devices to password grinding across the network.

Remote vs. Local Testing

Next, the enterprise must decide whether the testing will be performed from a remote location across the Internet or onsite via the local network. This decision is dictated to a large degree by the targets that are selected for testing and by the current security implementations. For example, a remote test of a machine behind a firewall that hides network address translation for Internet access will fail if the firewall appropriately prevents access to the machine. However, testing the same firewall to see if it will protect users' computers from a remote scan will be successful.

In-House vs. Outsourced Testing

After the scope of the testing has been determined, the IT team must decide whether to use in-house resources to perform the testing or to hire outside consultants. In-house testing should be chosen only if an enterprise lacks the funds to hire outside consultants, or if the data is so sensitive that no one outside the company should view it. In all other cases, hiring outside consultants is recommended. Outside security consultants are highly trained and have worked with hundreds of different networks, bringing specific expertise and broad experience to the testing process. In addition, they help ensure an unbiased and complete testing procedure. Security consultants continuously research new vulnerabilities, invest in and understand the latest security testing hardware and software, recommend solutions for resolving problems, and provide additional personnel for the testing process. Enterprises can leverage the experience and resources of outside security consultants to help ensure thorough, properly executed penetration tests.

Step 2: Performing the Penetration Test

Proper methodology is essential to the success of the penetration test. It involves gathering information and then testing the target environment.

The testing process begins with gathering as much information as possible about the network architecture, topology, hardware, and software in order to find all security vulnerabilities. Researching public information such as Whois records, SEC filings, business news articles, patents, and trademarks not only provides security engineers with background information, but also gives insight into what information hackers can use to find vulnerabilities. Tools such as ping, traceroute, and nslookup can be used to retrieve information from the target environment and help determine network topology, Internet provider, and architecture. Tools such as port scanners, NMAP, SNMPC, and NAT help determine hardware, operating systems, patch levels, and services running on each target device.

Once information about all the targets has been assembled, the security engineers use it to configure commercial scanning tools such as ISS Internet Scanner, NAI's CyberCop Scanner, and freeware tools such as Nessus and Satan to search for vulnerabilities. The use of these commercial and freeware tools greatly speeds up the scanning process. After the vulnerability scanning has been completed, the output is examined for false positives and false negatives. Any vulnerability suspected of being false is re-examined or tested using other tools or custom scripts.

To test for new vulnerabilities that have not been updated into the commercial or freeware scanners, the security engineers perform additional tests and run recently released exploits. This is necessary because new exploits are released every day, and it may be several weeks or months before these vulnerabilities are included in the vulnerability databases of the automated scanning tools.

Once scanning has been performed, the security engineers can test for additional items defined in the scope of the penetration test, including password vulnerabilities and denial of service (DOS) attacks. To test for DOS attacks in a production environment, without risking device outage, an enterprise can create a duplicate image of the production device and then place the image on similar hardware for testing.

Step 3: Reporting and Delivering Results

After completing the penetration testing, security engineers analyze all information derived from the testing procedure. Then they list and prioritize vulnerabilities; categorize risks as high, medium, or low; and recommend repairs if vulnerabilities are found. They may also provide resources, such as Internet links, for finding additional information or obtaining patches to repair vulnerabilities.

The final report may include the following parts:

- An executive summary summarizes the penetration test findings and discloses information concerning both strong and weak aspects of the existing security system. Key points of the test findings are also included.
- A more technically detailed report of the findings lists information about each device's vulnerabilities; categorizes and prioritizes risks; and makes recommendations about repairs, including providing additional technical information on how to repair any vulnerability.
- Additional information, such as raw scanner output, Whois records, screenshots, and diagrams, as well as relevant RFCs and white papers, is included in an appendix.

VeriSign SecureTEST

With more than 20 years of experience in delivering robust, reliable security solutions, VeriSign Consulting can assist enterprises in every phase of network penetration testing. Its SecureTEST Vulnerability Assessment Service helps identify areas of the enterprise's network where an intruder can exploit security vulnerabilities to gain unauthorized information about internal networks, gain access to restricted information, maliciously modify or destroy information, or deny authorized users or customers access to the network's information resources.

To accommodate the unique needs of each enterprise, VeriSign's SecureTEST offers three levels of service:

Common Vulnerability Assessment (CVA)

The CVA is a remote security assessment that focuses on the services that are most commonly misconfigured by personnel and are most commonly exploited by intruders. It also focuses on the most probable means of unauthorized access. A professional security engineer not only interprets the scanner output but also creates an executive summary and recommendations report.

Secure Device Assessment (SDA)

The SDA is an on-location device configuration assessment that includes architectural review of device deployment, operating system configuration, and device and policy configuration. This assessment is similar to an audit, except that it includes scanning services, when necessary.

Secure Exploit Assessment (SEA)

This penetration study encompasses all aspects of the CVA and also includes the following features: additional vulnerability research, DNS auditing, full enumeration including NetBios and Windows NT- and Unix-specific issues, penetration attempts with multi-stage attacks, and custom attack methodologies. Additional options include "brute force" password cracking and grinding, blind scanning (attacker perspective), "war dialing," and testing for denial of service attacks and social engineering (manipulating users to obtain confidential information such as passwords).

Summary

Although most enterprises have invested heavily in security products and services to protect their networks and operating systems from malicious or accidental destruction and loss of services and information, many enterprises do not take the critical step of ensuring that these security measures are properly implemented and enforced. Penetration testing is a vital component of a comprehensive security program. By thoroughly scanning and testing the network environment, a properly executed penetration test helps identify vulnerabilities in the network and prevent the loss or compromising of sensitive data. VeriSign SecureTEST Vulnerability Scanning Assessments provide varying levels of penetration testing, depending on the needs of the enterprise. Using solid methodologies and a range of state-of-the-art tools and processes, the VeriSign assessment team leverages its experience and expertise to identify, analyze, and prioritize security vulnerabilities. Working with the enterprise's internal security team, the VeriSign team can develop long-range solutions to provide a comprehensive, scalable, and robust security solution.

Glossary

brute-force cracking – an attempt to guess a password by running every possible combination of letters or numbers

cracking – maliciously exploiting a computer network

denial of service attack – an extremely serious attack that completely overloads Web servers and prevents legitimate users from accessing the system

exploit – an attack on a network, usually by "exploiting" a vulnerability of the system; hackers frequently post discovered vulnerabilities and their exploits, increasing the importance of regular security scanning

NAT (NetBios Auditing Tool) – an auditing tool that enumerates all machines

NMAP (Network Mapping) – a scanning tool that locates devices on the network

nslookup – a utility that uses a host name to find out its corresponding IP address

password grinding – an attempt to log on to a network by repeatedly guessing passwords until a random guess succeeds

patch – a program that is written to fix a vulnerability in an application or system

ping – a utility that tests for network connectivity

port scanner – a program that knocks on every single port (65,535) to see which ones are open for access to a network

SNMPC (Simple Network Management Protocol on a PC) – a sniffer program that looks at SNMPC packets

traceroute – a utility that traces the route of data through the network

war dialing – the process of dialing analog phone lines in numeric succession, looking for modems, faxes, and other devices connected to a network

Whois – a utility that provides access to directories that contain personal contact information, such as names of companies or individuals