VeriSign®

WHITE PAPER

# An Introduction to Network-Vulnerability Testing

Where it all comes together.™

WHITE PAPER

## CONTENTS

Where it all comes together.™

# 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 (DoS) 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, Trojan horses, DoS attacks and other intrusions. (Definitions for many industry-related terms are provided in the glossary that follows.) Testing also exposes vulnerabilities that may be introduced by patches and updates or by misconfigurations on servers, routers and firewalls.

SecureTEST®, a VeriSign security-scanning service, uses proven methodologies and tools to detect vulnerabilities in the enterprise's network and then to 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 recognise and detect security vulnerabilities and 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 intruders can exploit security vulnerabilities. Various 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 (demilitarised zone) is different from performing a scan to see whether 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 who will test it.

### Full-Scale vs. Targeted Testing

An enterprise must decide whether to conduct a full-scale test of the entire network, target specific devices, such as the firewall or both. 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, File Transfer Protocol (FTP) servers and domain-name-system (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 searching for susceptibility to DOS attacks? In addition, the enterprise must decide whether it will allow the security team to hack its password file 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 on site via the local network. This decision is dictated to a large degree by targets selected for testing and by 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 whether 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 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 take advantage of the experience and resources of outside security consultants to help ensure thorough, properly executed penetration tests.

### + Step 2: Performing the Penetration Test

Proper methodology, involving gathering information and testing the target environment, is essential to the success of the penetration test. 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, U.S. Securities Exchange Commission (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 (Network Mapping), SNMPC (the Simple Network Management Protocol on a PC), and NAT (the NetBios Auditing Tool) 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 the Internet Security Systems®, Internet Scanner®, the McAfee® 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 re-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 latter step 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 DOS attacks. To test for such 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 penetration testing, security engineers analyse all information derived from the testing procedure. Then they list and prioritise vulnerabilities, categorise 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 summarising the penetration test findings and disclosing 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 listing information about each device's vulnerabilities, categorising and prioritising risks and making 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, included in an appendix.

## VeriSign SecureTEST

VeriSign, which has more than 20 years of experience in delivering robust, reliable security consulting solutions, can assist enterprises in every phase of network-penetration testing. The VeriSign® SecureTEST Vulnerability Assessment Service helps identify areas of the enterprise's network where intruders can exploit security vulnerabilities to gain unauthorised information about internal networks, gain access to restricted information, maliciously modify or destroy information or deny authorised users or customers access to the network's information resources.

To accommodate the unique needs of each enterprise, the VeriSign SecureTEST service offers three levels of service, described below.

### Common Vulnerability Assessment

The Common Vulnerability Assessment (CVA) is a remote security test that focuses on the services personnel most commonly misconfigure and intruders most commonly exploit. It also focuses on the most probable means of unauthorised access. A professional security engineer not only interprets the scanner output but also creates an executive summary and recommendations report.

### Secure Device Assessment

The Secure Device Assessment (SDA) is an on-location, device-configuration test that includes an 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

The Secure Exploit Assessment (SEA) is a penetration study that encompasses all aspects of the CVA and includes additional vulnerability research, DNS auditing, full enumeration including NetBios and Windows NT- and UNIX-specific issues, penetration attempts with multistage attacks and custom attack methodologies. Additional options include brute-force password cracking and grinding, blind scanning, war dialling and testing for DoS attacks and social engineering.

# 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 do not take the critical additional step of ensuring that these security measures are properly implemented and enforced.

Penetration testing is a vital component of a comprehensive security programme. By thoroughly scanning and testing the network environment, a properly executed penetration test helps identify vulnerabilities in the network and prevent 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 employs its experience and expertise to identify, analyse, and prioritise 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.

For more information about VeriSign Managed Security Service, please call 0800 032 2101 or email sales@verisign.co.uk.

**Visit www.verisign.co.uk for more information.**

# 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

**DMZ (demilitarised zone)**—The semi-secure region between a network's inner and outer firewalls

**denial-of-service (DoS) attack**—An extremely serious attack that 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 programme written to fix a vulnerability in an application or system

**ping**—A utility that tests for network connectivity

**port scanner**—A programme that 'knocks' on every single port (65,535 total) to see which ones are open for access to a network

**SNMPC (Simple Network Management Protocol on a PC)**—A sniffer programme that looks at SNMPC packets

**social engineering**—Manipulating users to obtain confidential information such as passwords

**traceroute**—A utility that traces the route of data through the network

**Trojan horse**—A programme that allows viruses onto a network

**war dialling**—The process of dialling analogue 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