Integrated Network Vulnerability Scanning and Penetration Testing

www.saintcorporation.com

Introduction

While network vulnerability scanning is an important tool in proactive network security, penetration testing is the next step. This paper describes the various types of vulnerabilities that can threaten computer networks; explains network vulnerability scanning and penetration testing; and shows the benefits of the integrated SAINT® solution.

What are Vulnerabilities?

A vulnerability is anything running on a computer that could directly or indirectly lead to the compromise or breach of confidentiality, integrity, or availability of information or services anywhere on the network:

- Confidentiality breach – unauthorized read access
- Integrity breach – unauthorized creation, modification, or deletion of files
- Availability breach – denial of service

Types of Vulnerabilities

General types of vulnerabilities include the following:

- Passwords that are missing or easily guessed.
- Insecure file sharing resulting from NFS and SMB protocols which have been set up incorrectly.
- Excessive trust which results from .rhost or hosts.equiv files that have been configured incorrectly.

Buffer overflows are a more sophisticated vulnerability, usually caused by fixed-length strings in program code. A user-supplied parameter is copied into the fixed-length string. However, a specially crafted string could overflow the buffer and overwrite stack pointers causing a redirect of the program flow to arbitrary code being placed on the stack, or a denial-of-service.

Missing format strings are another sophisticated type of vulnerability. Some function calls require format strings (for example, two strings separated by a space: `"%s %s"`). If the format string is missing, the user can sometimes provide his or her own. Format specifiers such as %n can be used to overwrite key memory pointers.

Web application vulnerabilities can also cause breaches in network security:

- Lack of parameter checks can result in a network breach if special characters are input into CGI programs such as the following:
  - ../ could allow escape from the Web root
  - | or ; could allow shell commands

For example: http://host/cgi-bin/program?file=../../../../etc/passwd

- Cross-site scripting caused by Web servers or applications which echo <SCRIPT> tags or JavaScript references could be used by a malicious Web site to trick users into executing arbitrary scripts in the security context of the vulnerable site. (*For example:* http://host/search?query=<script>alert()</script>)

- PHP Remote File Include – PHP programs "include" or "require" code from other files. Some programs can be tricked into including code from a remote Web site. An attacker could host malicious code on his or her own Web site and cause it to be executed by the victim.
- SQL Injection is caused by database applications which place user input directly into SQL queries. `SELECT a FROM table WHERE id='$id'` could allow unauthorized database access. (*For example:* http://host/search?id=1'+UNION+SELECT+password+FROM+table+WHERE+id=id)

Malicious content vulnerabilities are client-side vulnerabilities allowing command execution. Web browsers, media players, virus scanners, or instant messaging clients can all be used to to trick a user into opening a malicious Web page or file. For instance, "Click here to get rich now!" Since the action is initiated by the user, the exploit is not blocked by the firewall.

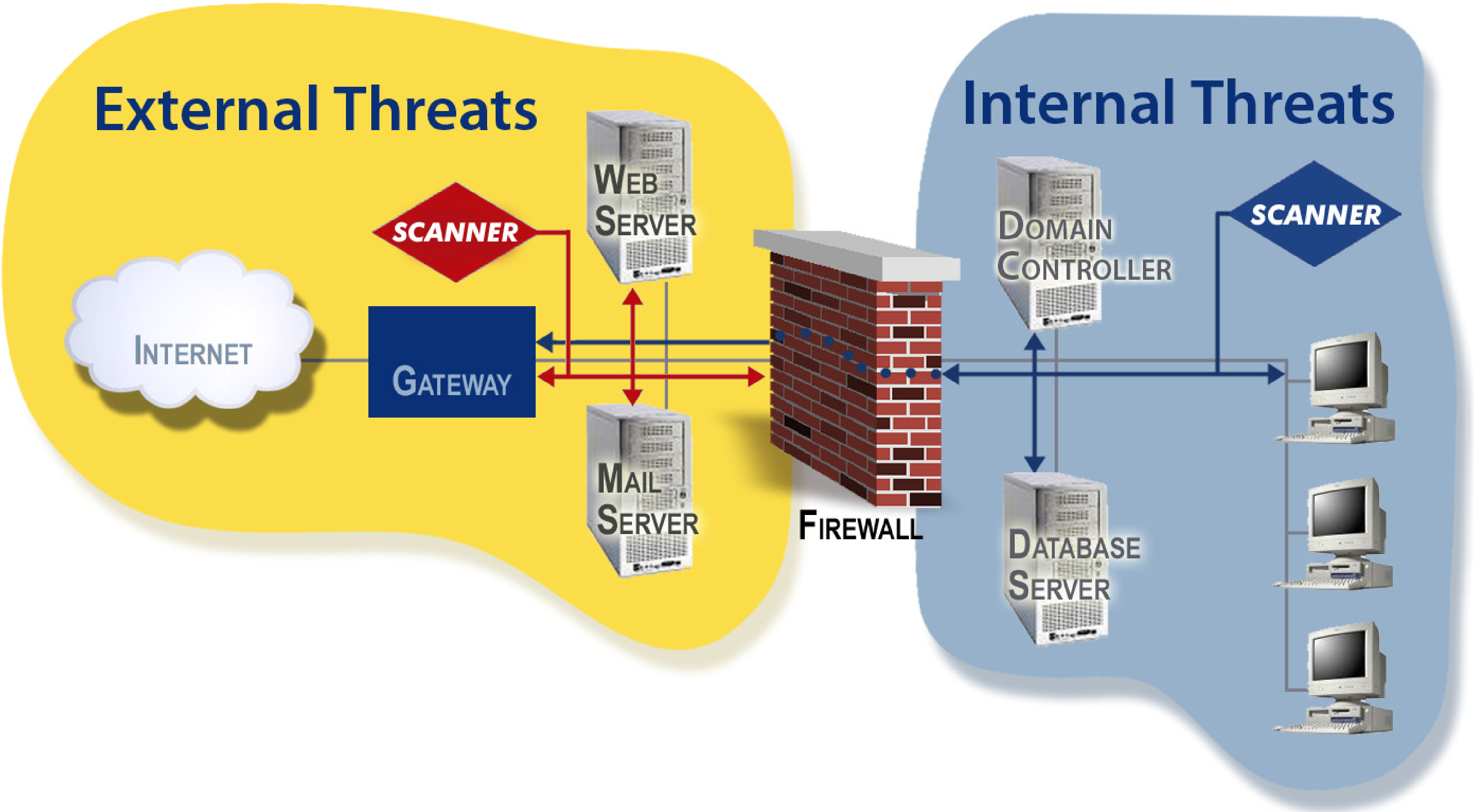
Network Vulnerability Scanning

Proactive network security means finding the holes in your network before the attackers do. Vulnerability scanning helps to protect against both external threats like attackers and worms, and internal threats such as malicious users within the network.

A network scanner detects vulnerabilities which are or might be present. The results of the scan will depend on the placement of the scanning machine. A vulnerability can only be detected if the scanning host has access to the vulnerable service. Since scanning through a router or firewall could hide internal vulnerabilities, it is best to place the scanner inside the firewall so it can scan for both internal and external vulnerabilities as shown in the placement of the blue scanner in the diagram below. The red scanner in the diagram can only scan for external vulnerabilities because it is placed outside of the firewall.

Vulnerability Scan Results

Vulnerability scan results serve multiple purposes. They provide an overview of the security of the network as well as a description of all vulnerabilities and potential problems, and how to fix them. Scan results also provide other useful information such as network services offered, operating system types, and host and NetBIOS names.

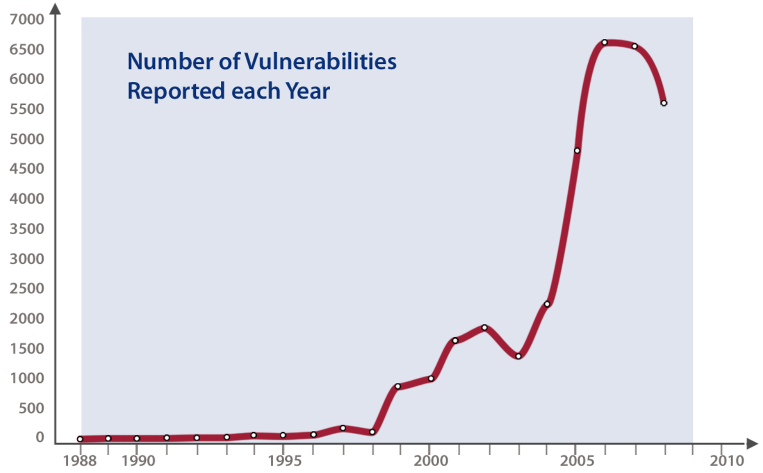

External Threats
Internal Threats
SCANNER
WEB SERVER
INTERNET
GATEWAY
MAIL SERVER
FIREWALL
DOMAIN CONTROLLER
SCANNER
DATABASE SERVER

Vulnerability Scanning Cycle

Networks should be scanned periodically to –

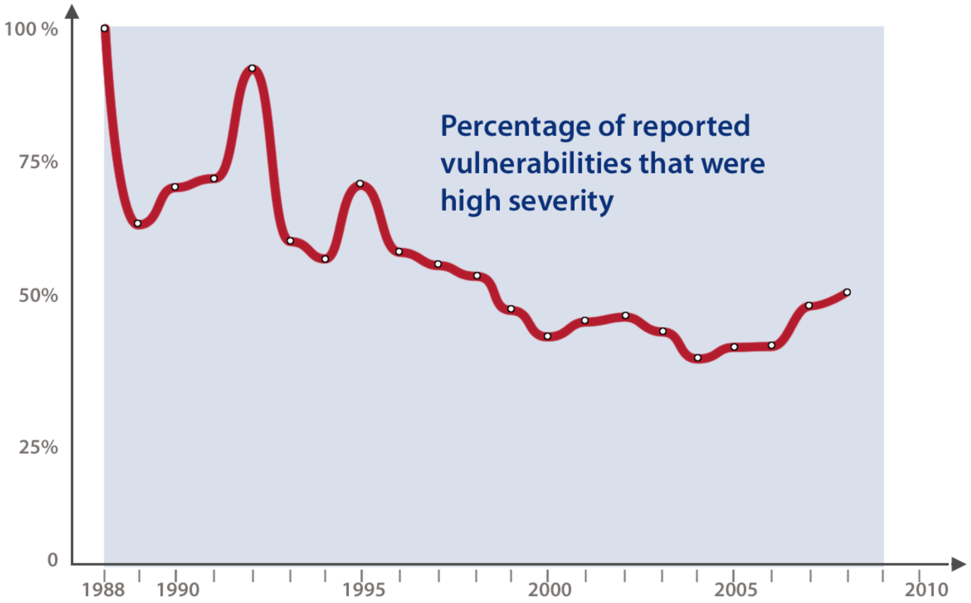
- Check that old vulnerabilities have been fixed.
- Check for new vulnerabilities created as a result of new hosts, upgrades of existing hosts, or new services on existing hosts.
- Check for newly announced vulnerabilities that were previously unknown; use the latest version of the scanner software.

The number of vulnerabilities reported each year has grown tremendously in the recent past as shown in the graph below. There are four times as many vulnerabilities reported today as there were five years ago and 88 times as many vulnerabilities reported today as ten years ago.



Reference: nvd.nist.

While the number of reported vulnerabilities has increased, fewer and fewer of the reported vulnerabilities are high severity, as shown in the following graph.



(High = CVSS Base Score 7.0-10.0)

Reference: nvd.nist.gov

Challenges

The existence of thousands of known vulnerabilities has resulted in longer vulnerability scan reports and made it difficult for administrators to assess the true impact and determine what an attacker could really gain. It is difficult for administrators to prioritize this multitude of vulnerabilities and know where to begin remediation efforts.

The Next Step – Penetration Testing

Penetration testing is the next step in proactive network security. It can help overcome the challenges mentioned above by assessing the real impact of vulnerabilities on a network and by prioritizing remediation. Vulnerability assessment and penetration testing go hand-in-hand. Vulnerability assessment results can be used as a starting point for a penetration test.

What is Penetration Testing?

Penetration testing is the act of assessing the security of your network by attempting to penetrate it by simulating the actions of an attacker. Penetration testing is authorized and scheduled, and will probably be detected by an IDS. Penetration testing is done with either manual or automated tools, such as SAINTexploit™. The penetration test can gather evidence of a vulnerability including reading and writing files, executing commands, or taking screen shots.

Benefits of Penetration Testing

A successful penetration test provides indisputable evidence of the problem as well as a starting point for prioritizing remediation. Penetration testing focuses on high-severity vulnerabilities and there are no false positives.

Drawbacks of Penetration Testing

Penetration testing focuses on vulnerabilities that allow command execution. Most command-execution vulnerabilities are buffer overflows, which inherently run the risk of crashing computers or services. However, automated penetration tests schedule the exploits from least to most dangerous. Another drawback is false negatives because buffer overflow exploits require precision within varying memory states. In addition, penetration testing only detects vulnerabilities which lead to penetration; this excludes cross-site scripting, denial of service, information gathering, etc.

Exploits

An exploit is a program designed to demonstrate the presence of a specific vulnerability usually by executing commands on the target. Penetration testing works by running a series of exploits that are chosen based on the target's operating system and running services.

There are three types of exploits:

- Remote – an initial break-in; exploitable by a remote user through a network service
- Local – privilege elevation; exploitable by an attacker who is already on the system
- Client – exploitable when a user is tricked into loading an attacker-supplied file

Advantages of Integrated Vulnerability Scanning and Penetration Testing

Because vulnerability scanning and penetration testing go hand-in-hand, an integrated solution with a single graphical user interface makes it easy to take network security to a higher level. With an integrated solution, such as SAINT, the results from the vulnerability scan link directly to the exploit.

The SAINT® solution

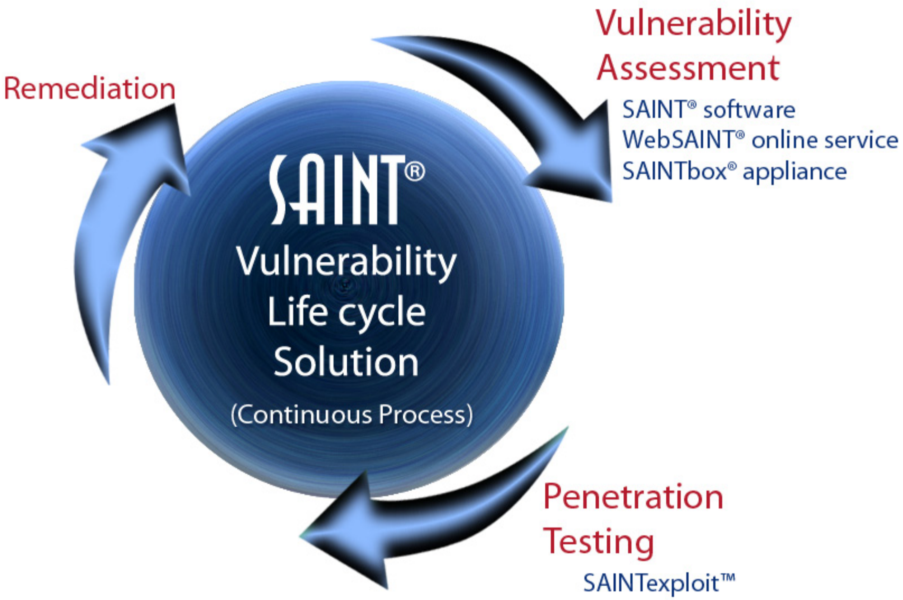
SAINT Corporation is the first developer of integrated vulnerability scanning and automated penetration testing software. The SAINTexploit™ penetration test tool examines potentially vulnerable services discovered by the SAINT network vulnerability scanner, and exploits the vulnerability to prove its existence without a doubt. The file browsing, command execution, and screen capture capabilities resulting from a successful exploit provide undeniable evidence of a network vulnerability. SAINT's integrated interface is easy to use with tabs for both vulnerability scanning and penetration testing.

SAINT updates are automatic and frequent. SAINT's reports range from executive summary to technical detail including a trend analysis option that allows you to quantitatively analyze your remediation program. Each report has configurable options with colorful graphs and tables to help you quickly identify problem areas.

Summary

Vulnerability scanning is only the first step in proactive network security. Penetration testing is the next step because it focuses on the high-severity vulnerabilities and provides a starting point for prioritizing remediation.

Vulnerability scanning and penetration testing provide a snapshot of the network's security at a specific point in time. As depicted in the SAINT VulnerabilityLife Cycle Solution diagram, network security requires a **continuous process** of scanning and testing because as soon as the tests are complete, any application or system change can result in new vulnerabilities.


Remediation
SAINT®
Vulnerability
Life cycle
Solution
(Continuous Process)
Vulnerability Assessment
SAINT® software
WebSAINT® online service
SAINTbox® appliance
Penetration Testing
SAINTexploit™