Chapter 8 – Desktop and Server OS Vulnerabilities

Notes

Overview

This chapter examines how security testing is used to analyze operating system vulnerabilities and correct them. It reviews how to discover and fix these vulnerabilities on Windows, as well as Linux operating systems. You will learn about the available assessment tools, in addition to several countermeasures for making these operating systems less vulnerable to common problems.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Describe vulnerabilities of the Windows and Linux operating systems
- Identify specific vulnerabilities and explain ways to fix them
- Explain techniques to harden Windows and Linux systems

Tips

Windows OS Vulnerabilities

1. This section describes several tools used to discover vulnerabilities on Windows systems. Using several tools collectively is advisable because they help you pinpoint problems more accurately.
2. You can check the CVE and CERT Web sites to determine vulnerabilities for any OS.
3. See Table 8-1 for the Windows Server 2012 vulnerabilities found at CVE.
4. Exploits against these vulnerabilities should only be used in specific cases, as a security tester and with prior approval.
5. Tools like Nessus and OpenVAS will help to automate some of the process of identifying vulnerabilities. You should understand the results that the tool provides by doing further research.

Windows File Systems

1. The purpose of a file system is to store and manage information.
2. The File Allocation Table is the original Microsoft file system. It is supported by nearly all desktop and server OSs.
3. The New Technology File System (NTFS) was first released as a high-end file system in Windows NT 3.1 and NT 3.51, it added support for larger files, disk volumes, and ACL file security. Subsequent Windows versions have included several upgrades.

Remote Procedure Call (RPC)

1. RPC is an interprocess communication mechanism that allows a program running on one host to run code on a remote host. The Conficker worm is an example of an attack related to RPC issues.
2. Use MBSA to determine if a system is vulnerable to an RPC-related issue.

Tip	Read http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx and http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx for more examples of RPC-related issues.

NetBIOS

1. NetBIOS has already been introduced in Chapter 6. NetBIOS is software loaded into memory that enables a computer program to interact with a network resource or device. NetBIOS is not a protocol, but an interface to a network protocol.
2. NetBEUI is a fast, efficient network protocol that allows NetBIOS packets to be transmitted over TCP/IP.
3. Systems running newer Windows OSs can share files and resources without using NetBIOS; however, NetBIOS is still used for backward compatibility, which is important when corporate budgets don't allow upgrading every computer on the network or when customer expectations must be met.

Server Message Block

1. Server Message Block (SMB) is used to share files and usually runs on top of NetBIOS, NetBEUI, or TCP/IP.
2. Hacking tools for SMB include L0phtcrack's SMB Packet Capture utility and SMBRelay.
3. Microsoft introduced SMB2 in Windows Vista. This version has several new features, is faster, and more efficient.

Common Internet File System (CIFS)

1. The Common Internet File System (CIFS) is an enhanced version of SMB used by Windows 2000 Server and later. It is a remote file system protocol that enables computers to share network resources over the Internet.
2. The main characteristics of CIFS are explained in this chapter. Understand how CIFS works and the enhancements offered by CIFS over SMB. SMB is used only for backward compatibility.
3. The two methods for server security an administrator can select:
    a. Share-level security
    b. User-level security

Null Sessions

1. Null sessions is anonymous connections established without credentials.
2. Using null sessions might pose a security risk to your organization.

Web Services

1. Understand the main problems of having a Web server installed on your network and some recommendations to better secure it.
2. Windows 2000 Server has IIS 5.0 installed by default. Many network administrators are not aware of this until a problem occurs.

3. Although IIS 6.0 (Windows Server 2003) through IIS 10.0 (Windows Server 2016) are installed in a "secure by default" mode, previous versions left crucial holes that made it possible for attackers to sneak into a network.

4. Regardless of the IIS version a system runs, keeping systems patched is important.

MS SQL Server

1. The most common critical SQL vulnerability is the null SA password.

Tip	Visit http://www.sqlsecurity.com/, to explore Microsoft SQL Server security issues.

Buffer Overflows

1. Understand the various buffer overflow problems. A buffer overflow occurs when data is written to a buffer (temporary memory space) and, because of insufficient bounds checking, corrupts data in memory next to the allocated buffer.

Passwords and Authentication

1. A comprehensive password policy is critical.

2. Examples of aspects that a password policy should include:
    a. Change password regularly
    b. Require passwords length of at least six characters
    c. Require a minimum password length of at least eight characters
    d. Require complex passwords
    e. No common words
    f. Passwords must not be identified with a particular user
    g. Never write a password down or store it online or on the local system
    h. Do not reveal a password over the phone
    i. Use caution when logging on
    j. Limit reuse of old passwords

3. Recommendations about configuring domain controllers. A good security or network administrator should enforce password age, length, and complexity at the domain controller. Also, the administrator should specify the account lockout threshold and duration.

Tip	Read http://www.techrepublic.com/article/lock-it-down-make-a-password-policy-part-of-your-security-plan/ for an article on how to create a password policy.

Tools for Identifying Vulnerabilities in Windows

1. Many tools are available for discovering Windows vulnerabilities. Using more than one tool for analysis is advisable, so learning a variety of methods and tools is beneficial.

Built-in Windows Tools

1. See Figure 8-1 for the checks available in Microsoft Baseline Security Analyzer (MBSA).

2. See Table 8-2 for MBSA's scanning capabilities.

3. See the minimum system requirements for MBSA in Table 8-3.

Tip	Visit https://www.petri.com/hfnetchk, for more information on HFNetChk scanner.

Best Practices for Hardening Windows Systems

1. Understand the difference between a penetration tester and a security tester.

Patching Systems

1. Understand the advantages of having the latest patch installed on your system and the options for patch management for both small and large networks. These options include:
    a. Accessing Windows Update manually
    b. Automatic Updates
    c. Systems Management Server (SMS)
    d. Windows Software Update Service (WSUS)
    e. Windows System Center Configuration Manager (SCCM)
    f. Third party management solutions

Antivirus Solutions

1. Understand the advantages of having an up-to-date antivirus program installed on your system and the options network administrators have for both small and large networks.

Enable Logging and Review Logs Regularly

1. Logging is essential for monitoring crucial areas. Understand the advantages and disadvantages of logging and the options available for reviewing logs.

2. Commands like ipconfig /all, netstat –r, net view, gpresult, especially when grouped together, could be seen as suspicious.

Disable Unused Services and Filtering Ports

1. It makes sense to disable unneeded services and delete unnecessary applications or scripts, since they are an open invitation for attacks.

2. Filtering out unnecessary ports can protect systems from attack. Explore some of the ports frequently subject to attack.

Other Security Best Practices

1. Other security best practices include the following steps:
    a. Minimize the number of users with administrative rights
    b. Implement software to prevent sensitive data from leaving the network
    c. Use network segmentation
    d. Restrict number of applications allowed to execute
    e. Delete unused scripts and sample applications
    f. Delete default hidden shares and unnecessary shares
    g. Be careful of default permissions
    h. Use appropriate packet-filtering technologies
    i. Use available tools to assess system security
    j. Use a file-integrity checker to monitor unauthorized file system modifications
    k. Disable the Guest account
    l. Disable the default Administrator account
    m. Make sure there are no accounts with blank passwords
    n. Use Windows group policies
    o. Develop a comprehensive security awareness program
    p. Keep up with emerging threats

Linux OS Vulnerabilities

1. Like any OS, Linux can be made more secure if users are aware of its vulnerabilities and keep current on new releases and fixes.
2. A typical Linux distribution has thousands of packages developed by many contributors around the world. With such diverse sources of code, it's inevitable that flaws will happen.

Tip	Visit http://www.linuxsecurity.com for recent news topics and articles regarding Linux security.

Samba

1. Samba is an open-source implementation of CIFS. It was created in 1992 by a group of programmers to allow sharing network resources over multiple OSs. By using Samba, you can have Windows systems using *nix resources and vice-versa.
2. Samba "tricks" Microsoft systems into believing the *nix resources are Microsoft resources.
3. Understand how to configure and use Samba in mixed Windows and *nix environments to allow both OSs to share files and printers.

Tip	For more information, visit http://www.samba.org, the official Samba Web site.

Tools for Identifying Linux Vulnerabilities

1. Visiting the CVE Web site is a good first step in discovering possible avenues attackers might take to break into a Linux system.
2. See Table 8-4 for the Linux vulnerabilities found at CVE.
3. A security tester using enumeration tools can:
    a. Identify a computer on the network by using port scanning and zone transfers
    b. Identify the OS the computer is using by conducting port scanning and enumeration
    c. Identify via enumeration any logon accounts and passwords configured on the computer
    d. Learn the names of shared folders by using enumeration
    e. Identify services running on the computer
4. For how to use OpenVAS see Figures 8-4 through 8-12.
5. Understand how Trojan programs are used to carry out attacks. Most Trojan programs perform one or more of the following functions:
    a. Allow remote administration of the attacked system.
    b. Create a file server on the attacked computer so that files can be loaded and downloaded without the user's knowledge.
    c. Steal passwords from the attacked system and e-mail them to the attacker.
    d. Log all keystrokes a user enters and e-mail the results to the attacker or store them in a hidden file the attacker can access remotely.
    e. Encrypt all of the user's files and hold them ransom
    f. Destroy all of the data on a victim system
6. Mention that even more dangerous are rootkits containing Trojan binary programs ready to be installed by an intruder who has gained root access to a system.

Tip	See http://nvd.nist.gov/nvd.cfm?cvename=CVE-2004-0075 for an example of a Linux vulnerability.

More Countermeasures Against Linux Attacks

1. The most critical tasks for protecting against attacks include:
    a. User awareness training
    b. Keeping current
    c. Secure configuration

Tip	The following link contains a quick reference guide for Linux security: http://tldp.org/REF/ls_quickref/QuickRefCard.pdf.

Additional Resources

1. Windows Server 2012 Security articles:
   http://www.windowsecurity.com/articles-tutorials/Windows_Server_2012_Security/

2. Microsoft Baseline Security Analyzer:
   http://technet.microsoft.com/en-us/security/cc184924.aspx

3. SANS Institute CIS Critical Security Controls:
   https://www.sans.org/critical-security-controls/?ref=top20

4. NIST Guide to General Server Security:
   http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

5. Extended Stored Procedures: Intro And 10 Cool Examples:
   http://www.devarticles.com/c/a/SQL-Server/Extended-Stored-Procedures-Intro-And-10-Cool-Examples/

6. FIRST Best Practice Guide Library (BPGL):
   http://www.first.org/resources/guides/

Key Terms

- **attack surface**
- **Common Internet File System (CIFS)**
- **domain controller**
- **Mandatory Access Control (MAC)**
- **NetBIOS Extended User Interface (NetBEUI)**
- **Remote Procedure Call (RPC)**
- **Samba**
- **Server Message Block (SMB)**
- **System Center Configuration Manager**
- **Systems Management Server (SMS)**
- **Windows Software Update Service**s