



Hands-On Ethical Hacking and Network Defense, Edition 4

Chapter 8: Desktop and Server OS Vulnerabilities

Module Objectives

- By the end of this module, you should 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

Windows OS Vulnerabilities (1 of 2)

- Many Windows OSs have serious vulnerabilities
 - Windows 2000 and earlier
 - Administrators had to disable, reconfigure, or uninstall services and features
 - Later versions of Windows
 - Disabled most services and features by default to improve security
- To find vulnerabilities for any OS, you can check the [CVE](#) and [CERT](#) vulnerabilities websites

Windows Server Vulnerabilities Found at CVE

CVE ID	Description
CVE-2021-34527	Windows 10, Server 2019, Server 2016, Server 2012, Server 2008, Windows 8.1, and Windows 7 have a flaw in the Printer Spooler subsystem that can allow attackers to remotely execute code. This flaw is so severe that Microsoft issued fixes for operating systems that are no longer officially supported (such as Windows 7).
CVE-2021-33740	Windows 10, Server 2019, and Server 2016 have a flaw in the Windows Media subsystem that could allow an attacker to remotely execute code on the vulnerable system.
CVE-2021-33773	Windows 10, Server 2019, Server 2016, Server 2012, and Windows 8.1 have a flaw by which users with remote access connections could elevate their permissions to give them administrative access.
CVE-2021-33756	Windows 10, Server 2019, Server 2016, Server 2012, Server 2008, Windows 8.1, and Windows 7 have a flaw whereby the Windows DNS Snap-in can be exploited to allow Remote Code Execution.

Windows OS Vulnerabilities (2 of 2)

- Many explanations on the CVE website are complex
 - Important that you're able to research a vulnerability relevant to the security test you're conducting
- Security testers can use information from the CVE site to test a Windows computer
 - Make sure it's been patched with updates from Microsoft that address known vulnerabilities

Windows File Systems

- Purpose of any file system
 - Stores and manages information that users create
 - Organized OS files needed to boot the system
- File system is the most vital part of any OS
 - Can be a vulnerability in some cases

File Allocation Table

- Original Microsoft file system
 - Supported by nearly all desktop and server OSs from 1981 to now
 - Later versions provide for larger file and disk sizes
 - F A T32
 - The standard file system for most removable media other than CDs and DVDs
- Most serious shortcoming
 - Doesn't support file-level access control lists (ACLs)
 - ACLs are necessary for setting permissions on files
 - Multiuser environment results in a critical vulnerability

NTFS

- New Technology File System (NTFS)
 - First released as a high-end file system in Windows NT 3.1 and in Windows NT 3.51
 - Added support for larger files, disk volumes, and ACL file security
- Subsequent Windows versions
 - Included several upgrades
- Some inherent vulnerabilities
 - Alternate data streams (ADSs)
 - Can “stream” (hide) information behind existing files
 - Without affecting their function, size, or other information
 - Makes it possible for system intruders to hide exploitation tools and other malicious files
 - Several detection methods exist

Remote Procedure Call

- An interprocess communication mechanism
 - Allows a program running on one host to run code on a remote host
- The Conficker worm exploited RPC by taking an advantage of a vulnerability in RPC
 - Ran arbitrary code on susceptible hosts
- Nessus
 - Excellent tool for determining whether a system is vulnerable due to an RPC-related issue and for many other configuration and patching items as well

NetBIOS (1 of 2)

- Software loaded into memory
 - Enables computer program to interact with network resource or device
- NetBIOS isn't a protocol
 - It is an interface to a network protocol that enables a program to access a network resource
- **NetBios Extended User Interface (NetBEUI)**
 - Fast, efficient network protocol
 - Requires little configuration
 - Allows NetBIOS packets to be transmitted over TCP/IP and various topologies
 - NetBIOS over TCP/IP is disabled by default on current versions of Windows

NetBIOS (2 of 2)

- Systems running newer Windows OSs can share files and resources without using NetBIOS
 - NetBIOS is still used for backward compatibility
 - Important when organizational budgets don't allow upgrading
 - Customer expectations must be met

Server Message Block (1 of 2)

- Used to share files
 - Usually runs on top of:
 - NetBIOS
 - NetBEUI
 - TCP/IP
- Several hacking tools target SMB
 - Well-known tools are L0phtcrack's SMB Packet Capture utility and SMBRelay
 - It took Microsoft seven years to patch the vulnerability that these tools exploited

Server Message Block (2 of 2)

- Microsoft introduced SMB2 in Windows Vista, SMB3 in Windows 8, and SMB3.1.1 in Windows 10
 - Fixed security issues
 - Added several new features
- SMB vulnerabilities are a common attack vector exploited by malware

Common Internet File System (1 of 3)

- **Common Internet File System (CIFS)**
 - A standardized protocol that replaced SMB for Windows 2000 Server
 - SMB is still used for backward compatibility
- CIFS is a remote file system protocol
 - Enables sharing of network resources over the Internet
- Relies on other protocols to handle service announcements
 - Notifies users of available resources

Common Internet File System (2 of 3)

- Offers many enhancements
 - Locking features
 - Caching and read-ahead/write-behind capability
 - Support for fault tolerance
 - Capability to run more efficiently over slow dial-up lines
 - Support for anonymous and authenticated access
- Two methods for server security
 - Share-level security
 - User-level security

Common Internet File System (3 of 3)

- Newer versions of Windows Server listen on most of the same ports as older versions
- Most attackers look for servers designated as **domain controllers**
 - Servers that handle authentication
- Windows domain controllers are usually global catalog servers
 - Global catalog servers are used to locate resources in a domain containing thousands or even millions of objects

Null Sessions

- A null session is an anonymous connection established without credentials
 - Used to display information about users, groups, shares, and password policies
 - Necessary only if networks need to support older Windows versions
- To enumerate NetBIOS vulnerabilities:
 - Use `Nbtstat`, `Net view`, `Netstat`, `Ping`, `Pathping`, and `Telnet` commands

Web Services

- Older versions of Web services and IIS would install with critical security vulnerabilities
 - Microsoft developed the IIS Lockdown Wizard
 - Locks down IIS versions 4.0 and 5.0
- IIS 5.0
 - Installed by default in Windows 2000 Server
 - A Windows 2000 server is also a web server using the default configuration, a setup many administrators aren't aware of until a problem occurs
- IIS 6.0 through IIS 10.0
 - Installs with a "secure by default" mode
 - Previous versions left crucial security holes
- Keeping a system patched is important
- Configuring only needed services and applications is a wise move

MS SQL Server

- Older versions of SQL Server have many potential vulnerabilities
 - Null System Administrator (SA) password
 - Most common critical SQL vulnerability
 - Allows remote users to gain System Administrator (SA) access through the SA account on the server
 - May occur in all versions before SQL Server 2005
- SQL Server 2000
 - An SA account with a blank password is created, and this account can't be disabled
 - Gives attackers administrative access to the database and the database server

Buffer Overflows

- Data is written to a buffer and corrupts data in memory next to allocated buffer
 - Normally, this problem occurs when dangerous functions use input that has not been properly validated
- Because of design flaws, functions don't verify text fits
 - Attackers can run shell code
- C and C++
 - Lack built-in protection against overwriting data in memory

Passwords and Authentication (1 of 3)

- Authorized users are the weakest security link in any network
 - Most difficult to secure
 - Relies on people who might not realize that their actions could expose their organization to a major security breach
- Companies should take steps to address this vulnerability
 - A comprehensive password policy is critical

Passwords and Authentication (2 of 3)

- A comprehensive password policy should include the following:
 - Change passwords regularly (quarterly)
 - Require at least eight characters
 - Require complex passwords
 - Passwords can't be common words, dictionary words, slang, jargon, or dialect
 - Passwords must not be identified with a particular user
 - Never write it down or store it online or in a file
 - Do not reveal it to anyone
 - Use caution when logging on and limit reuse

Passwords and Authentication (3 of 3)

- Configure domain controllers to enforce password age, length, and complexity
- Password policy aspects that can be enforced:
 - Account lockout threshold
 - Set the number of failed attempts before an account is disabled temporarily
 - Account lockout duration
 - Set the period of time an account is locked out after failed logon attempts
- Windows Server 2008 and newer domain controllers
 - Multiple password policies can be enforced

Knowledge Check Activity 8-1

Windows OSs are vulnerable to the Conficker worm because of which of the following?

- a. Arbitrary code
- b. SQL buffer overflow
- c. Blank password
- d. RPC vulnerability

Knowledge Check Activity 8-1: Answer

Windows OSs are vulnerable to the Conficker worm because of which of the following?

Answer: d. RPC vulnerability

Remote Procedure Call (RPC) is an interprocess communication mechanism that allows a program running on one host to run code on a remote host. Windows OSs are vulnerable as the Conficker worm takes advantage of a vulnerability in RPC to run arbitrary code on susceptible hosts.

Polling Activity 8-1

Which of the following is a well-known SMB hacking tool? (Choose all that apply.)

- a. SMBRelay
- b. SMBsnag
- c. L0phtcrack's SMB Packet Capture utility
- d. NTPass

Polling Activity 8-1: Answer

Which of the following is a well-known SMB hacking tool?

Answer: a. and c. SMBRelay and L0phtcrack's SMB Packet Capture utility

The two well-known SMB hacking tools are L0phtcrack's SMB Packet Capture utility and SMBRelay, which intercept SMB traffic and collect usernames and password hashes.

Polling Activity 8-2

Applications written in which programming language are especially vulnerable to buffer overflow attacks? (Choose all that apply.)

- a. C
- b. Perl
- c. C++
- d. Java

Polling Activity 8-2: Answer

Applications written in which programming language are especially vulnerable to buffer overflow attacks?

Answer: a. and c. C and C++

Both C and C++ lack built-in protection against overwriting data in memory, so applications written in these languages are vulnerable to buffer overflow attacks.

Tools for Identifying Vulnerabilities in Windows

- Many tools are available
 - Using more than one is advisable
- Using several tools helps pinpoint problems more accurately
- Some popular OS vulnerability scanners:
 - Tripwire IP360, Tenable Nessus, Nexpose, and OpenVAS

Scanning Windows Using Nessus Essentials

- Many security attacks can be avoided with careful system analysis and maintenance
- When Microsoft learns of problems or vulnerabilities in its software, it publishes:
 - Patches
 - Security updates
 - Service packs
 - Hotfixes

Common Windows Server Configuration and Security Issues (1 of 4)

Type of issue	Details to check for
Security updates missing	<p>Missing Windows, IIS, and SQL Server security updates</p> <p>Missing Exchange Server security updates</p> <p>Missing IE security updates</p> <p>Missing Windows Media Player and Office security updates</p> <p>Missing Microsoft Virtual Machine (VM) and Microsoft Data Access Components (MDAC) security updates</p> <p>Missing MSXML and Content Management Server security updates</p>
Windows configuration	<p>Account password expirations left at default settings, not matching company policy (30 days, etc.). This should be changed to match company policy.</p> <p>Blank or simple passwords are used for local user accounts. This should be changed to match company password policy.</p> <p>File system type on hard drives is insecure. F A T being used when NTFS should be used to provide ACLs. Change to NTFS if possible.</p> <p>Auto Logon feature is enabled. Disable if this feature is not required.</p>

Common Windows Server Configuration and Security Issues (2 of 4)

Type of issue	Details to check for
Windows configuration	<p>Number of local Administrator accounts should be 1 or 2 at most.</p> <p>Is the Guest account enabled? Disable this account if it is not required.</p> <p>Restrict Anonymous Registry key setting should be set to not allow anonymous access if not a business requirement.</p> <p>List shares on the computer and any unnecessary services running. Make sure shares are credential secured and stop unnecessary services.</p> <p>Windows version and whether Windows auditing is enabled. Is the Windows version supported by updates? Auditing creates log entries to track file access. Is this set to meet company policy?</p> <p>Firewall status and Automatic Updates status. Is the firewall enabled and configured to match company policy or left at defaults? Are automatic updates configured to match company policy?</p>
IIS (Internet Information Service)	<p>Is the IIS Lockdown tool running? If the server version is older than 2003, IIS Lockdown needs to be running.</p> <p>Are IIS sample applications and the IIS Admin virtual folder installed? These are default installation items and should be removed or secured.</p> <p>Are IIS parent paths enabled? If enabled, this default setting may need to be evaluated or disabled.</p>

Common Windows Server Configuration and Security Issues (3 of 4)

Type of issue	Details to check for
IIS (Internet Information Service)	<p>MSADC and Scripts virtual directories are installed by default and should be removed or disabled.</p> <p>IIS logging should be enabled.</p> <p>IIS should not be running on a domain controller.</p> <p>Does the Administrators group belong in the Sysadmin role? This setting may be a default configuration. If not intended, remove the Administrators group.</p> <p>Make sure the CmdExec role is restricted to Sysadmin only.</p> <p>SQL Server should not be running on a domain controller.</p> <p>The SA account password should not be default or blank, and the Guest account should not have database access.</p> <p>Access permissions to SQL Server installation folders should not be left at default settings.</p> <p>The Everyone group should not have access to SQL Server Registry keys.</p> <p>SQL Server service accounts should not be members of the local Administrators group. If compromised, hackers will have admin access.</p> <p>SQL Server accounts should not have blank or simple passwords.</p>

Common Windows Server Configuration and Security Issues (4 of 4)

Type of issue	Details to check for
SQL configuration	Check SQL Server authentication mode type to make sure it matches security requirements. The number of Sysadmin role members should be at the minimum.
Desktop application configuration	<p>IE security zone settings for each local user should match company policy.</p> <p>Is IE Enhanced Security Configuration enabled for Administrator accounts and is it configured to be secure? Administrator accounts should avoid browsing the Internet, and sessions need to be highly secured.</p> <p>Is IE Enhanced Security Configuration enabled for non-Administrator accounts? This setting must be configured to match company policy and not accidentally left at default settings.</p> <p>What are the Microsoft Office security zone settings for each local user?</p> <p>These should be set to match company policy and not accidentally left at default settings.</p>

Using Nessus Essentials

- If you have access to a Windows server that you have permission to scan, then use that as your target to see what vulnerabilities Nessus Essentials might discover

The screenshot displays the Nessus Essentials web interface. The top navigation bar includes the 'nessus Essentials' logo, 'Scans', and 'Settings' tabs. On the right of the top bar, there is a notification bell, the user name 'rob', and a profile icon. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules). The main content area is titled 'My Scans' and features buttons for 'Import', 'New Folder', and '+ New Scan'. Below these is a search bar labeled 'Search Scans:' with a magnifying glass icon and a count of '2 Scans'. A table lists the scans with columns for 'Name', 'Schedule', and 'Last Modified'. The table contains two entries: 'My Basic Network Scan' and 'My Host Discovery Scan', both with a schedule of 'On Demand' and a status of 'Completed' (indicated by a checkmark). The 'Last Modified' column shows the completion times: 'July 17 at 12:52 PM' and 'July 17 at 12:42 PM'. Each row has a checkbox on the left and a play button on the right.

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	My Basic Network Scan	On Demand	✓ July 17 at 12:52 PM	▶	✕
<input type="checkbox"/>	My Host Discovery Scan	On Demand	✓ July 17 at 12:42 PM	▶	✕

Source: Tenable

Best Practices for Hardening Windows Systems

- Penetration tester finds and reports vulnerabilities as defined in their contract
- Security tester:
 - Finds vulnerabilities
 - Gives recommendations for correcting vulnerabilities

Patching Systems (1 of 2)

- Best way to keep systems secure
 - Keep them up to date
 - Attackers take advantage of known vulnerabilities that has a patch available
 - Options for few computers (10 or fewer)
 - Accessing Windows Update manually
 - Time-consuming
 - Configure Automatic Updates on each machine depending on the Windows version
 - Options for large networks
 - **Systems Management Server (SMS)**
 - From 1994 to 2005, SMS was the standard for managing Windows security patches
 - Assessed machines in a defined domain and could be configured to manage patch deployment

Patching Systems (2 of 2)

- **Windows Software Update Service (WSUS)**
 - Downloads patches and publishes them internally to servers and desktop systems
 - The administrator has control over which updates are deployed
- Windows **System Center Configuration Manager (SCCM)**
 - Includes a suite of tools to help administrators deploy and manage servers alongside updated patch-management functionality
- Third-party patch-management solutions
 - BigFix, Tanium, and BladeLogic

Antivirus Solutions

- Antivirus solution is essential for:
 - Small networks
 - Desktop antivirus tools with automatic updates might be enough
 - Large networks
 - Require corporate-level solution
- Antivirus tools
 - Must be planned, installed, and configured correctly to ensure the best protection
 - Almost useless if not updated regularly

Enable Logging and Review Logs Regularly

- Logging is a crucial function for monitoring system security
 - Carefully record only useful statistics
- Review logs regularly for signs of intrusion or other problems
 - Use log-monitoring tool
- Build prevention and detection by considering what attackers might do if they compromised your network
- Commands like `ipconfig /all`, `netstat -r`, `net view`, and `gpresult`, especially when grouped together, could be seen as suspicious

Disable Unused Services and Filtering Ports

- Disable unneeded services
- Delete unnecessary applications or scripts
 - Unused applications are invitations for attacks
- Reducing the **attack surface**
 - Open only what needs to be open, and close everything else
- Filter out unnecessary ports
 - Make sure perimeter routers filter out ports 137 to 139 and 445
 - Protects against external null session attacks

Other Security Best Practices (1 of 2)

- Other practices include the following:
 - Minimize the number of administrative users
 - Implement software preventing data from leaving
 - Use network segmentation
 - Restrict the number of applications allowed to execute on a computer connected to the network
 - Delete unused scripts and sample applications
 - Delete default hidden shares
 - Use unique naming scheme and passwords
 - Ensure password length/complexity are sufficient

Other Security Best Practices (2 of 2)

- Other practices include the following (continued):
 - Be careful of default permissions
 - Use appropriate packet-filtering techniques
 - Use open-source or commercial tools to assess system security
 - Use a file-integrity checker
 - Disable the Guest account
 - Disable the local Administrator account
 - Disable accounts of users no longer with the company
 - Make sure there are no accounts with blank passwords
 - Use Windows group policies to enforce security configurations on large networks efficiently and consistently
 - Develop a comprehensive security awareness program
 - Keep up with emerging threats

Linux OS Vulnerabilities

- Linux can be made more secure if users are:
 - Aware of its vulnerabilities
 - Keep current on new releases and fixes
- Many versions are available
 - Differences range from slight to major
- It's important to understand basics
 - Run control and service configuration
 - Directory structure and file system
 - Basic shell commands and scripting
 - Package management

Samba

- Created as an open-source implementation of CIFS in 1992
 - To address the issue of interoperability
- Allows *nix servers to share resources with Windows clients
 - Security professionals should have a basic knowledge of SMB and Samba because many companies have a mixed environment of Windows and *nix systems
- Often used on networks that require *nix computers to access Windows resources
 - Designed to “trick” Windows services into believing *nix resources are Windows resources
 - *nix clients can connect to Windows shared printer and vice versa when Samba is configured on the *nix computer

Tools for Identifying Linux Vulnerabilities (1 of 5)

- CVE website
 - Source for discovering possible attacker avenues

CVE/CAN	Description
CVE-2021-36148	A buffer overflow in the function <code>dmар_free_irte</code> in the file <code>hypervisor/arch/x86/vtd.c</code> allows the attacker to corrupt memory.
CVE-2021-35039	A vulnerability was found in Linux Kernel up to 5.12.13 affecting the function <code>init_module</code> of the file <code>kernel/module.c</code> . The manipulation with an unknown input leads to a weak authentication vulnerability.
CVE-2019-14896	A heap-based buffer overflow vulnerability was found in the Linux kernel, version kernel-2.6.32, in Marvell WiFi chip driver. A remote attacker could cause a denial of service (system crash) or possibly execute arbitrary code when the <code>lbs_ibss_join_existing</code> function is called after a STA connects to an AP.

Tools for Identifying Linux Vulnerabilities (2 of 5)

- CVE information can be used for testing Linux computers for known vulnerabilities
- OpenVAS can enumerate multiple OSs
 - Security tester using enumeration tools can:
 - Identify a computer on the network by using port scanning and zone transfers
 - Identify the OS by conducting port scanning and enumeration
 - Identify via enumeration any logon accounts and passwords
 - Learn names of shared folders by using enumeration
 - Identify services running on the computer

Tools for Identifying Linux Vulnerabilities (3 of 5)

The screenshot displays the Greenbone Security Manager web interface. At the top, the header shows the Greenbone logo, the text 'Greenbone Security Manager', and the user 'Admin' logged in. Below the header is a navigation bar with tabs: Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area shows details for a host with IP 192.168.2.144. It includes fields for Comment, Hostname, IP, OS (Canonical Ubuntu Linux), Route, and Severity (10.0 (High)). Below this is a section titled 'Latest Identifiers' containing a table with columns: Name, Value, Created, Source, and Actions.

Name	Value	Created	Source	Actions
OS	cpe:/o:canonical:ubuntu_linux:8.04	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.105586)	
ssh-key	22 ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+j17FWx...	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.100259)	
MAC	00:15:5D:C8:94:03	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.103585)	
OS	cpe:/o:debian:debian_linux	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.102011)	
ssh-key	22 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBQZvO3WTEjP4TudjgWkI...	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.100259)	
OS	cpe:/o:canonical:ubuntu_linux	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.111067)	
OS	cpe:/o:canonical:ubuntu_linux:8.04	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.111069)	
OS	cpe:/o:linux:kernel	Mon Jun 14 2021	Report fca8c59d-13eb-41c8-94b4-00657e146320 (NVT 1.3.6.1.4.1.25623.1.0.105355)	

Source: GNU General Public License

Figure 8-6 OpenVAS has determined the target system is running Ubuntu Linux

Tools for Identifying Linux Vulnerabilities (4 of 5)

Greenbone Security Manager Logged in as: Admin **admin** | Logout
Sun Jul 18 20:15:19 2021 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: Anonymous X... autofs=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort=reverse=severity levels=html min_qod=70


Report: Results (59 of 389) ID: eebf462c-baf2-4fb-62b8-bd556a7238ef
Modified: Sun Jul 18 19:46:58 2021
Created: Sun Jul 18 19:07:48 2021
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.2.144	80/tcp	
OS End Of Life Detection	10.0 (High)	80%	192.168.2.144	general/tcp	
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	80%	192.168.2.144	512/tcp	
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.2.144	1524/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.2.144	8787/tcp	
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.2.144	1099/tcp	
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.2.144	3632/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.2.144	5432/tcp	
VNC Brute Force Login	9.0 (High)	95%	192.168.2.144	5900/tcp	
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.2.144	3306/tcp	
rlogin Passwordless / Unencrypted Cleartext Login	7.5 (High)	70%	192.168.2.144	513/tcp	
phpinfo() output Reporting	7.5 (High)	80%	192.168.2.144	80/tcp	
rsh Unencrypted Cleartext Login	7.5 (High)	80%	192.168.2.144	514/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.2.144	80/tcp	
Check for Backdoor in UnrealIRCd	7.5 (High)	70%	192.168.2.144	6667/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	192.168.2.144	80/tcp	
Test HTTP dangerous methods	7.5 (High)	99%	192.168.2.144	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.2.144	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.2.144	21/tcp	
UnrealIRCd Authentication Spoofing Vulnerability	6.8 (Medium)	80%	192.168.2.144	6667/tcp	

Source: GNU General Public License


Figure 8-8 Report of OpenVAS scan of 192.168.2.144

Tools for Identifying Linux Vulnerabilities (5 of 5)

**Greenbone**
Security Manager



Logged in as Admin **admin** | Logout
Sun Jul 18 20:21:46 2021 UTC

DashboardScansAssetsSecInfoConfigurationExtrasAdministrationHelp



Result: Possible Backdoor: Ingreslock

ID: ee4078c4-5ae1-474c-9de5-e528219a4c84
Created: Mon Jun 14 14:40:45 2021
Modified: Mon Jun 14 14:40:45 2021
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.2.144	1524/tcp	 
Summary A backdoor is installed on the remote host					
Vulnerability Detection Result The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)					
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.					
Vulnerability Detection Method Details: Possible Backdoor: Ingreslock (OID: 1.3.6.1.4.1.25623.1.0.103549) Version used: \$Revision: 11327 \$					

Source: GNU General Public License

Figure 8-9 Possible Backdoor: Ingreslock vulnerability found

Checking for Trojans (1 of 2)

- Trojan programs perform one or more of the following:
 - Allow remote administration of attacked system
 - Create a hidden file server on the attacked computer
 - Files can be uploaded and downloaded
 - Steal passwords from the attacked system
 - Email them to attacker
 - Log all keystrokes a user enters
 - Email the results or store them in a hidden file that the attacker can access remotely

Checking for Trojans (2 of 2)

- Linux Trojan programs
 - Sometimes disguised as legitimate programs
 - Contain program code that can wipe out file systems
 - More difficult to detect today
 - Protecting Linux computers against identified Trojan programs is easier
- Rootkits containing Trojan binary programs
 - More dangerous
 - Attackers hide tools
 - Perform further attacks
 - Have access to backdoor programs

More Countermeasures against Linux Attacks

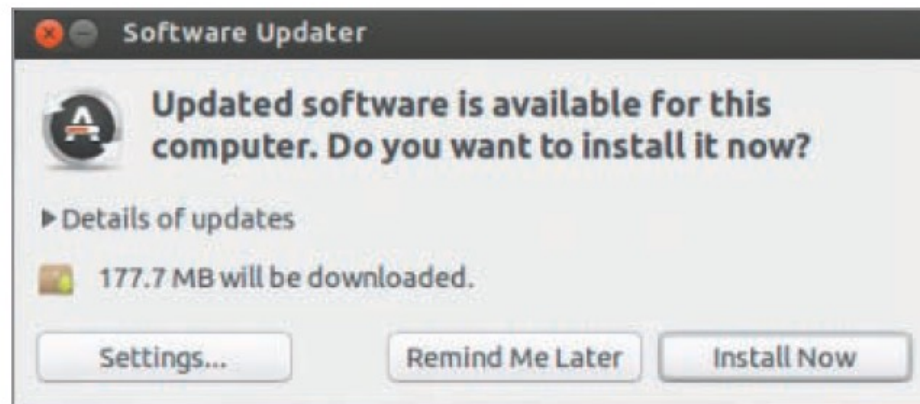
- Most critical tasks:
 - Training users
 - Keeping up on kernel releases and security updates
 - Configuring systems to improve security

User Awareness Training

- Make it difficult for social engineers to get information from employees
- Include all employees in the training
- No information should be given to outsiders
 - Knowing the OS that the company is running makes attacks easier to select an exploit
- Teach users to be suspicious of people asking questions about the systems they are using
 - Verify whom they are talking to
 - Ask for a phone number to call them back

Keeping Current

- As soon as a vulnerability is discovered and posted, OS vendors notify customers of upgrades and patches
 - Installing fixes promptly is essential to protect your system
- Linux distributions
 - Most display warnings to inform users when they are running outdated versions



Source: Ubuntu

Secure Configuration

- Many methods and tools can be used to configure a Linux system to help prevent intrusions
 - Vulnerability scanners
 - Built-in Linux tools
 - Security Enhanced Linux (SELinux)
 - Uses **Mandatory Access Control (MAC)**, an OS security mechanism that enforces access rules based on privileges for interactions between processes, files, and users
 - Free benchmark PDFs and tools provided by the Center for Internet Security (CIS)
 - OS Lockdown
 - A commercial tool (formerly known as Security Blanket)
 - Used to secure system quickly and save *nix system administrators from hours of manual configuration work

Knowledge Check Activity 8-2

For a Windows computer to be able to access a *nix resource, CIFS must be enabled on at least one of the systems. True or false?

- a. True
- b. False

Knowledge Check Activity 8-2: Answer

For a Windows computer to be able to access a *nix resource, CIFS must be enabled on at least one of the systems. True or false?

Answer: False.

To access a *nix resource from a Windows computer, CIFS must be enabled on both systems.

Discussion Activity 8-1

Discuss the measures that you can take for protecting systems on any network. Make a list of these measures and compare your answers with that of your classmates.

Discussion Activity 8-1: Answer

Discuss the measures that you can take for protecting systems on any network.

Answer: The measures for protecting systems on any network include having user awareness training programs, running antivirus tools, disabling unneeded services, filtering out unnecessary ports, installing security updates and patches, securing configurations, application whitelisting, and reviewing logs.

Self-Assessment

Recall the methods for improving security on tested systems.

Describe how the risks posed by vulnerabilities on embedded operating systems can be minimized.

Summary

- Now that the lesson has ended, you should 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