Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 7

Analyzing Network Traffic to Create a Baseline Definition

**Section 1: Hands-On Demonstration**

Part 1: Capture Network Traffic using TCPdump Utility

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

In the Connections folder, double-click the PuTTy-DVWA shortcut to open a PuTTY session to the Linux server hosting the DVWA tool.

At the command prompt, type man tcpdump and press Enter to open the onscreen manual for the TCPdump utility.

Text

Description automatically generated

This screen displays all of the command line options for the tool and descriptions for each. Press Enter to scroll through the manual and learn more about this tool. Press q to return to the command line prompt.

At the command prompt, type cd /etc/network and press Enter to change the current directory.

At the command prompt, type ls and press Enter to list the files in the current directory.

At the command prompt, type cat interfaces and press Enter to display the available Ethernet interfaces.

The system returns the list of Ethernet interfaces available. The iface eth0 inet static statement indicates that the physical Internet interface (eth0) is available. The IP address for this machine, 172.30.0.13, matches the IP address in the title bar of the PuTTY window.

At the command prompt, type cd and press Enter to return to the root directory.

At the command prompt, type tcpdump -i eth0 -n -w tcpdumpcapturefile and press Enter to start the data capture.

Text

Description automatically generated

This command also instructs the utility to save the results of the data capture to a file (tcpdumpcapturefile) instead of printing the results. The TCPdump utility is now configured to capture data on the eth0 interface.

Minimize the PuTTy-DVWA window.

From the Connections folder, double-click the Web-DVWA Internet shortcut to launch the DVWA tool in a new browser window.

The actions you take within this tool will be captured by tcpdump and stored in the tcpdumpcapturefile file, which you initiated in the PuTTY session.

At the DVWA log-in page, type the following credentials and click Login to continue.

Graphical user interface, application

Description automatically generated

Username: admin

Password: password

If prompted to store the password, click Not for this site to dismiss the pop-up.

On the DVWA Navigation menu, click the DVWA Security button.

From the Script Security drop-down menu, select low and click Submit to change the security level.

Graphical user interface, text, application, email

Description automatically generated

On the DVWA Navigation menu, click the XSS reflected button.

XSS vulnerabilities are generally found in web forms that send and retrieve data to databases via HTML.

In the What’s your name? box, type Simon and click Submit.

Graphical user interface, text, application

Description automatically generated with medium confidence

The web form will take the name you entered and repeat it back to you in a friendly welcome. If prompted to remember web form entries, click No to continue.

In the What’s your name? box, type <Simon> and click Submit.

Graphical user interface, text, application

Description automatically generated

Note: The greater and less-than arrows surrounding “Simon” are referred to as scripting tags in HTML. They are what allow you to add scripts to a Web page. By entering <Simon> into a form field you are entering a script that contains only the instruction Simon. The fact that you see a response, even just the word “Hello” from the form indicates that this form is vulnerable. The Web form does not complain and it fails to return the expected outcome. Now that you have found a possible vulnerability, you will need to test it further.

In the What’s your name? box, type <script>alert('this is a vulnerability');</script> and click Submit.

Graphical user interface, application

Description automatically generated

Note: In order to test the vulnerability, you need to enter a script that does something. The command “alert” is a scripting function that generates a pop-up alert window to the screen. The command is telling the form to run a script that generates a pop-up window with the message within the quotes. The fact that you see this result, proves that the form will allow scripts to run. Since this simple script was processed correctly, you know that there is a good chance that any type of malicious script can be run.

Click OK to close the alert window.

Close the browser window.

Restore the PuTTy-DVWA window.

In the PuTTy-DVWA window, press CTRL+C to stop the data capture and return to the command prompt.

At the command prompt, type tcpdump -n -r tcpdumpcapturefile | less and press Enter to display the contents of the tcpdumpcapturefile file.

The pipe less command ( | less ) enables the user to use the arrow keys to cycle through the tcpdumpcapturefile log in smaller sections, one line at a time. To generate a pipe (|) character, press shift + backslash (\).

In the PuTTy-DVWA window, press the down arrow key repeatedly to cycle through the entire contents of the file.

Notice that the communication in this output is between 172.30.0.2, the vWorkstation, and 172.30.0.13, the Linux server that hosts the DVWA tool. Notice too that the port used for this data stream is port 80 (172.30.0.13.80), which corresponds to HTTP, as you might expect from a web application.

Use the scrollbar to locate the alert script in the log file.

Make a screen capture showing the alert script within the tcpdumpcapturefile file and paste it into a Lab Report file.

Text

Description automatically generated

Close the PuTTy-DVWA window.

When prompted, click OK to close the window.

Part 2: Capture Network Traffic with Wireshark

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 to open the remote connection.

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.

On the TargetWindows02 taskbar, click the Wireshark icon to open the Wireshark application.

On the Welcome to Wireshark page, click the Student interface to select the network interface for this lab environment.

In the ...using the filter: box, type not port 3389 to filter out RDP traffic between TargetWindows02 and the vWorkstation, then press Enter to start the capture process.

Graphical user interface, text, application, email

Description automatically generated

Minimize the Wireshark window.

On the TargetWindows02 desktop, double-click the putty icon to launch the PuTTY application.

In the Host Name (or IP address) box of the PuTTY Configuration dialog box, type 172.16.8.5 (the IP address for LAN Switch 1), then select the Telnet radio button and click Open to open an unsecure Telnet connection.

Graphical user interface, application

Description automatically generated

At the login prompt, type the following credentials. Press Enter after each entry.

Login: cisco

Password: cisco

In the terminal console window, type show interface and press Enter to display the list of available interfaces.

Text

Description automatically generated

In the terminal console window, type show vlan and press Enter to display the VLANs on this machine.

Text

Description automatically generated

In the terminal console window, type quit and press Enter to close the terminal console session to LAN Switch 1.

Repeat steps 6-11 for each of the following IP addresses:

LAN Switch 2: 172.16.20.5

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Tampa 2811 router: 172.17.8.1

Graphical user interface, application

Description automatically generated

Text

Description automatically generated



The Tampa router will display an error on the show vlan command. This is normal behavior for a router.

On the TargetWindows02 desktop, double-click the putty icon to start the PuTTY application again.

In the Host Name (or IP address) box of the PuTTY Configuration dialog box, type 172.16.8.1 (the IP address for the Norfolk 2811 router), then select the SSH radio button and click Open to start a secure SSH connection.

Graphical user interface, application

Description automatically generated

If prompted with a security warning, click Yes to continue.

Graphical user interface, text, application

Description automatically generated

At the login prompt, type the following credentials. Press Enter after each entry.

Login: cisco

Password: cisco

In the terminal console window, type show interface and press Enter to display the list of available interfaces.

Text

Description automatically generated

In the terminal console window, type quit and press Enter to close the terminal console session to Norfolk 2811.

On the TargetWindows02 desktop, double-click the putty icon to start the PuTTY application again.

In the Host Name (or IP address) box of the PuTTY Configuration dialog box, type 172.30.0.13 (the IP address for the DVWA server), select the SSH radio button, then click Open to start a secure SSH connection.

If prompted with a security warning, click Yes to continue.

Graphical user interface, application

Description automatically generated

At the login prompt, type the following credentials. Press Enter after each entry.

Login: student

Password: student

In the terminal console window, type exit and press Enter to close the terminal console session to the DVWA server.

Text

Description automatically generated

Minimize the remote TargetWindows02 connection to return to the vWorkstation desktop.

Part 3: Transfer Files using Tftpd64 and FileZilla

On the vWorkstation desktop, close the Connections folder.

On the vWorkstation taskbar, click the FileZilla Client icon to open the FileZilla Client application.

If prompted, click OK to close the Welcome to FileZilla pop-up.

In the text boxes at the top of the FileZilla window, type the following login credentials to connect to the FileZilla Server on the TargetWindows02 desktop.

Host: 172.30.0.10

User name: student

Password: P@ssw0rd!

Port: 21

Click the Quickconnect button to complete the connection to the FileZilla Server.

Graphical user interface, text, application

Description automatically generated

If prompted to remember FileZilla passwords, click OK to continue.

In the Local site and Remote site panes, navigate to the following folders:

Local site: (C:\ISSA\_TOOLS\Documentation)

Remote site: (/)

Graphical user interface, application, Word

Description automatically generated

In the lower Local site pane, right-click the AnyConnect\_adminguide.pdf file and select Upload from the context menu to upload the file to the TargetWindows02 desktop.

Graphical user interface, text, application

Description automatically generated

Drag the Filename border to the right to see the entire filename and ensure that you are selecting the correct file. When the upload process is complete, FileZilla will display a pop-up message confirming the upload.

Close the FileZilla Client window.

Restore the remote TargetWindows02 connection.

Make a screen capture showing the AnyConnect\_adminguide.pdf on the TargetWindows02 desktop and paste it into your Lab Report file.

Graphical user interface, application

Description automatically generated

On the TargetWindows02 desktop, double-click the Tftpd64 icon to launch the Tftpd64 application

Minimize the remote TargetWindows02 connection to return to the vWorkstation desktop.

On the vWorkstation desktop, double-click the Tftpd64 icon to launch the Tftpd64 application.

The Tftpd64 application uses the TFTP (Trivial File Transfer Protocol) to send (put) or receive (get) files between computers.

In the Tftpd64 window, click the Browse button and select the Desktop folder (C:\Users\Administrator\Desktop), then click OK to change the Current Directory to the vWorkstation desktop.

Graphical user interface, application

Description automatically generated

In the Tftpd64 window, select 172.30.0.2 from the Server interfaces drop-down menu.

Restore the remote TargetWindows02 connection.

Table

Description automatically generated with medium confidence

In the Tfpd64 window, click the Tftp client tab, then type or select the following information and click the Put button.

Host: 172.30.0.2 (vWorkstation)

Port: 69

Local File: C:\Users\Administrator\Desktop\AnyConnect\_adminguide.pdf

Block Size: Default

This is the same file that you transferred using FileZilla earlier in this lab. A pop-up window will indicate whether or not the file transfer was successful.

Graphical user interface

Description automatically generated

Click OK to dismiss the pop-up indicating that the TFTP transfer is completed, then close the Tftpd64 application.

Minimize the remote TargetWindows02 connection to return to the vWorkstation desktop.

In the Tftpd64 window, click the Show Dir button to verify that the AnyConnect\_adminguide.pdf file was transferred to the vWorkstation.

Make a screen capture showing the transferred file in the Tftpd64 directory and paste it into the Lab Report file.

Graphical user interface, text, application

Description automatically generated

Close the Tftpd64:directory window.

Close the Tftpd64 application

Part 4: Analyze a Packet Capture with Wireshark

Restore the remote TargetWindows02 connection.

From the TargetWindows02 taskbar, restore the Wireshark application.

On the Wireshark toolbar, click the Stop capturing packets icon to stop the packet capture process.

Graphical user interface, text, application

Description automatically generated

From the Wireshark menu bar, select Statistics > Protocol Hierarchy to open the Protocol Hierarchy Statistics window.

Graphical user interface, text, application

Description automatically generated

Wireshark will open a new window that describes the different protocol types captured on the LAN segment; this provides a clear indication of what protocols are on the LAN segment and which ones are permitted to be on the LAN segment as part of the network’s overall baseline definition. If necessary, adjust the window size to view the entire report.

Make a screen capture showing the Protocol Hierarchy Statistics and paste it into your Lab Report file.

Graphical user interface

Description automatically generated

Close the Protocol Hierarchy Statistics window.

From the Wireshark menu bar, select Statistics > Packet Lengths to open the Packet Lengths window.

Graphical user interface, text, application

Description automatically generated

Wireshark will open a new window that describes the packet size distribution of the capture. It is important to know and understand what protocols and what size of Ethernet frames are being used for the transmission on the LAN segment. This is an important network traffic baseline definition.

Make a screen capture showing the Packet Lengths distribution and paste it into your Lab Report file.

Graphical user interface, application, table

Description automatically generated

Close the Packet Lengths window.

From the Wireshark menu bar, select File > Save As.

Graphical user interface, application, table

Description automatically generated

In the Save As dialog box, click the Desktop button, type yourname\_S1\_WiresharkCapture, replacing yourname with your own name, select Wireshark/tcpdump/…-pcap from the Save as type drop-down list, and click Save.

Graphical user interface, text, application, email

Description automatically generated

Close the Wireshark window.

Note: In the next steps, you will use the File Transfer folder to move the deliverable file from the TargetWindows02 machine to the vWorkstation. You will transfer the file to your local system at this 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\_WiresharkCapture.pcap

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.

Graphical user interface, application

Description automatically generated

Part 5: Analyze a Packet Capture File with NetWitness Investigator

Restore the remote TargetWindows02 connection.

On the TargetWindows02 taskbar, click the RSA icon to launch the NetWitness Investigator application.

From the NetWitness Investigator menu bar, click Collection, then select New Local Collection to create a new collection.

Application, table

Description automatically generated

In the New Local Connection window, type yourname Collection in the Collection Name box, replacing yourname with your own name, and click OK to name the new collection.

Graphical user interface, text, application

Description automatically generated

In the left pane, double-click the yourname Collection to activate it and change the status to Ready.

Graphical user interface, application

Description automatically generated

In the left pane, right-click the yourname Collection, then select Import Packets from the Context menu.

Graphical user interface, application

Description automatically generated

In the Open dialog box, navigate to the TargetWindows02 Desktop, select the yourname\_S1\_WiresharkCapture.pcap file you saved earlier in this lab, and click Open.

Graphical user interface, text, application, email

Description automatically generated

When the file has finished importing, double-click the yourname Collection to open it in NetWitness Investigator.

In the summary report, locate details about the PuTTY sessions and file transfers you performed in this lab. You should be able to identify the following:

The IP protocol (TCP or UDP) used for each transaction.

The IP addresses of the machines you interacted with in this lab.

The name of the files transferred.

The user accounts and passwords used in this lab.

Make a screen capture showing the password and filename used in the FTP transfer and paste it into your Lab Report file.

Graphical user interface

Description automatically generated with medium confidence

Make a screen capture showing the filename used in the TFTP file transfer and paste it into your Lab Report file.

Graphical user interface, text, application

Description automatically generated

Close the NetWitness Investigator window.

Close the remote TargetWindows02 connection to return to the vWorkstation.

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.

yourname\_S1\_WiresharkCapture.pcap