

Lab 2 Packet Sniffing

Description: In this lab, you will set up a Telnet session with one of the servers and login as the administrator. You will then use Wireshark in an attempt to capture the username and password from the target system.

Requirement: You will need access to the Cybrary lab environment to complete this lab.

Step 1: Log into the Cybrary website

Step 2: In the search box, search for “ **Certified Ethical Hacker (CEH)** ” by Practice Labs.

Step 3: Click the Launch button

Note: You may receive a message that the lab needs to be launched in a separate window. If you receive this message, please click the “Launch Item” button to launch the lab. It may take 1-2 minutes to launch the lab.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

Step 4: You will then see the lab environment open and will see several labs listed on the left-side.

Step 5: Click on the “ **Packet Sniffing** ” lab and then click the Start button.

Step 6: Next, turn on all of the virtual machines by hovering your mouse cursor over them and selecting the “Power on” option.

Step 7: Next, click on **PLABDM01**

Step 8: If the Server manager window opens, just close it by clicking the “x” at the top.

Step 9: Next, launch the Wireshark application by clicking the blue-colored shark’s fin on the bottom menu bar.

Step 10: Double-click on “ **Ethernet 3** ”

Step 11: Next, click on the **PLABWIN10** machine.

Step 12: On the Windows 10 desktop, double-click the **putty** shortcut icon.

Step 13: Click the **Telnet** radio button

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

Step 14: In the Host Name box, type the IP address for PLABDC01: **192.168.0.1**

Step 15: Next, click the Open button at the bottom.

Question 1: Do you see any error messages?

Note: An error message could indicate that the Telnet service might be running or that it may not be listening on port 23.

Step 16: Next, we will try our other server machine (PLABDM01) to see if Telnet is responding.

Step 17: Close putty and re-open it by double-clicking again on the putty shortcut icon on the desktop.

Step 18: Select the Telnet radio button again.

Step 19: Type this IP address (PLABDM01) in the Host Name field.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

192.168.0.2

Step 20: Click the Open button

Note: This should establish a connection with the server.

Step 21: Enter the following login information and press Enter.

login: **Administrator**

password: **Passw0rd**

Question 2: Were you able to get access?

Step 22: Next, click back on **PLABDM01** and stop the Wireshark packet capture by clicking on the red-colored square at the top of the Wireshark window.

Step 23: In the “Apply a display filter” box at the top, type in the following and then click on the blue-colored arrow. Note: The lab might be a little slow in responding to your actions.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

telnet

Step 24: Next, right-click on any packet and select Follow, then TCP Stream.

Question 3: Do you see any usernames or passwords? If no, keep repeating steps 23 and 24, until you find a username and/or password listed in the output. Once you find a username and/or password, enter them here

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*