|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: NISHCHAL SREEVATHSA |  |  |  |  |

Capturing and Analyzing the Network Traffic using a Sniffer

Ethical Hacking & Lab 3

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 2](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 9](#_Toc409378040)
2. [Conclusion & Wrap-Up 10](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | To set up the network interface so that the sniffer can record network traffic, use ifconfig.  Application Protocol: Create network traffic so that the sniffer can record real-time traffic. (A few Protocols are ftp, telnet, SMTP, POP3, Telnet etc).  A user can record network traffic or examine a capture file using the free and open-source protocol analyzer Wireshark. |

## Objectives

|  |  |
| --- | --- |
|  | Using a sniffer, we recorded and examined the traffic. In this lab, Wireshark is the sniffer in use. A sniffer is a passive network scanner that only listens and logs traffic. All traffic is sent to every machine on a network through a hub. It will be necessary to configure a SPAN port in order to view all of the traffic sent to all machines. |

# Lab Description Details

**Step 1:** Accessed the internal Kali Linux2 machine on the topology and entered **root** as username and **toor** as password.

A screenshot of a computer

Description automatically generated**Step 2:** Open the Linux terminal and use the command **ifconfig** to configure the network interface so that the sniffer, Wireshark, may capture traffic. Type **# ifconfig eth0 0.0.0.0 up** to prevent the system from having an IP address. Then type Wireshark in the terminal and the Wireshark application opens. Select Interfaces from Capture, then check the eth0 box and press Start. Packets show up in the packet list.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Step 3:** Next process is to generate the Traffic, Use a Windows computer on the same network with the IP address 192.168.1.20 to start the transmission. Run as Administrator is selected when you right-click the shortcut for the command prompt. Return to Root user using the command: **cd \.**

Use ftp to transmit traffic to the 192.168.1.10 Windows server. Command: **C:\> ftp 192.168.1.10.**

Enter ftp for the username and zombie as the password.

To list every file and folder, use the **ls command**.

Using the command: ftp>bin, change the mode to binary and download the image.

The command: **ftp>get 2008.jpg** can be used to download the jpeg picture from the Windows server.

FTP session can be ended using the command: **ftp>bye**.

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated**Step 4:** Repeat these procedures to obtain the second flag, which is **80212**, by opening the file explorer once you have viewed the 2008.jpg image and entered the sampleflag number that was presented.

**Step 5:** Make a telnet connection to the Windows server.

Command: **# telnet 192.168.1.10**.

Type administrator in login field and enter P@ssw0rd for password field and then Add a user to the Windows server creeper.

Command: **#** **net user creeper P@ssw0rd /add**

Then creeper must be added to the Enterprise Admins group.

Command: **#** **net group "domain admins" creeper /add**

Enterprise Admin permission was assigned to the user Creeper. After this end the session.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedAnother account called superman was added using the command: **net user superman**. Found the flag with number **999818** for superman account. Similarly added another account called **Aquaman** and found the flag number: **888221.**

**A screenshot of a computer

Description automatically generatedStep 6:** Opened the Opera Mini Mailbox on the system and composed and sent an email to [student@campus.edu](mailto:student@campus.edu), subject stating as Minecraft and details as You should buy Minecraft. Further cross verified whether the mail was sent or not in the Send section of email and was able to see the compose mail which was sent. Then exit the mail.

A screenshot of a computer

Description automatically generated

**Step 7:** Select the Kali Linux 2 machine and open Wireshark. Since FTP uses plain text, you can see the zombie user's password. To view the zombie's FTP password, enter **frame contains zombie** in the Wireshark Filter pane and click Apply.

A screenshot of a computer

Description automatically generated

**Step 8:** I then looked at email traffic. Since POP appears as plain text, you may see the student's password as P@ssw0rd. To view POP traffic, including the password for the student account, enter **pop** in the Wireshark Filter box and then click apply.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated**Step 9:** To see the phrase "buy" from the email you already sent, In the Wireshark Filter box, enter the **frame contains buy** and hit apply. Choose Follow TCP Stream by performing a right-click on the POP frame. Both email content and plain text communications can be seen.

A screenshot of a computer

Description automatically generated

**Step 10:** To view telnet traffic, enter the **telnet** command in the Wireshark Filter pane and then click apply. Choose Follow TCP Stream by performing a right-click on the first telnet frame in the list. Select the bottom option in the list after selecting entire discussion. See the command that creates the creeper account and adds it to the domain administrators. Click on close and stop the Wireshark.

A screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

In this laboratory, you set up and ran a sniffer, fetched network data using ftp, configured a telnet connection, and opened an Opera Mail account. You also ran an analysis of the network traffic via Wireshark.