CS 3710 Introduction to Cybersecurity
Term: Spring 2022

Lab Exercise 3 – Sniffing

Due Date: February 18, 2022 11:59pm
Points Possible: 7 points

Name:

By submitting this assignment you are digitally signing the honor code, "On my honor, I pledge that I have neither given nor received help on this assignment."

1. Overview

In this exercise, you will be introduced to Wireshark, a very useful tool that covers a very important network monitoring, security, and forensic concept – reading and understanding networking traffic. Wireshark (software known as a packet analyzer) allows you to view pieces of data (called packets) in real-time as they go in and out of a system and can be saved as packet capture (pcap or cap) files. In this exercise, you will be analyzing packet capture files as well as capturing live network traffic in real-time.

2. Resources required

This exercise requires a Kali Linux VM running in the Cyber Range. Please log in at https://console.virginiacyberrange.net/.

3. Initial Setup

From your Virginia Cyber Range course, select the **Cyber Basics** environment. Click "start" to start your environment and "join" to get to your Linux desktop.

4. Tasks

Task 1: Analyzing a Wireshark capture file

Wireshark offers a variety of sample packet captures to analyze for learning about network traffic, attacks, and how to use the tool. You can find the whole list at: https://wiki.wireshark.org/SampleCaptures.

Go to SampleCaptures wireshark page and click on Telnet and then click on the **telnet-cooked.pcap** to download it. The file is located in the /home/student/Downloads folder. You can open the pcap file from within an open Wireshark GUI by going to File -> Open, or you can open the file from the command line by supplying Wireshark the path and file name.

Question #1: What is the username and password of the Telnet user? (.5 point)

Using the follow TCP stream command, the credentials are username: fake, password: user.

Question #2: What is the operating system and version of the server that the user logged into? (.5 point)
Using the TCP follow command, the operating system is found in the line, "Welcome to OpenBSD: The proactively secure Unix-like operating system." So the operating system is OpenBSD, which is a free security based Linux like operating system.

Question #3: Once the user was logged in what commands did they run? (.5 point)

There were four commands run in this order
/sbin/ping www.yahoo.com,
ls,
ls -a,
exit.

Next download an HTTP packet capture with several downloaded images here: https://wiki.wireshark.org/uploads/__moin_import__/attachments/SampleCaptures/http_with_jpegs.cap.gz

Question #4: Paste a screenshot of the last image that was downloaded. (.5 point)
Searching the TCP source port of 80, the following image was found to be downloaded.

Question #5: What is the date and time that the image was downloaded? (.5 point)

The image was downloaded at Date: Sat, 20 Nov 2004 10:21:17 GMT.

Now it's time to do some cyber forensics analysis on FTP. Download and open a new pcap file from http://artifacts.virginiacyberrange.net/gencyber/ftp_attack.pcap. This is a packet capture of a file transfer using FTP. FTP uses ports 21 and 20. Port 21 is the command port and port 20 is the data port. Open the file in Wireshark to begin your analysis.

The user logs in early on in the capture and downloads a file. Inspect this traffic and answer the following questions:

Question #6: What is the username and password of the FTP user? (.5 point)
Using follow tcp stream and the filter for tcp port 20 or 21, the username and password are:

USER anonymous
PASS h4x0r@evil.com

Question #7: What is the name and version of the FTP software on the server? (.5 point)

The name of the software is vsFTPd and the version is 2.2.2.

Question #8: What is the name of the file that was downloaded? (.5 point)

The name of the file that was downloaded file.txt.

Question #9: What is the content of the file downloaded? (.5 point)
The file content download was: "test file for download\n \n"

Later in the FTP capture the user tries to log in using another username. After many failed password guesses the user guesses the correct password and is authenticated to the FTP server. Inspect this traffic and answer the following questions:

Question #10: What is the new username and password of the FTP user that is successful? (.5 point)

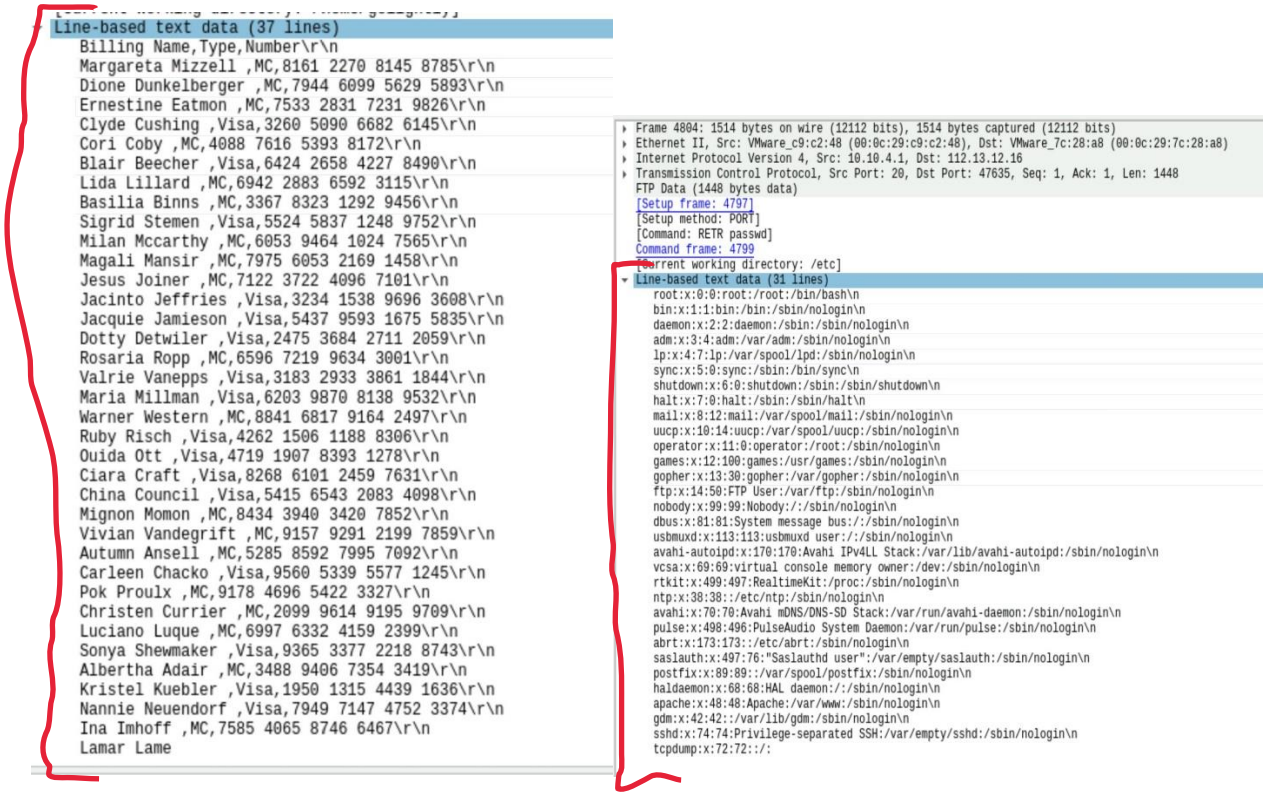
User: Golightly
Password: letmein

Question #11: What are the names of the 2 files that were downloaded while logged in as this new user? (.5 point)

The files were "CC_data.csv" and "passwd."

Question #12: Cut and paste a screenshot of the contents of the two files that were downloaded while logged in as this user. (.5 point)

This is the data from the files "CC_data.csv" on the left and "passwd" on the right.



Hints: *FTP filtering will help here. Also, HTTP files can be downloaded as an object, but FTP file transfers are embedded in the data channel.*

Task 2: Capturing traffic real-time using Wireshark

Now let's take a look at some real-time packet capturing. Make sure that you are running Wireshark as **root.**

Start a real-time capture in Wireshark and then open a Web Browser within the Cyber Range and go to the site dvwa.example.com. You will see a login screen. Log in using the username of **admin** and the password of **password**. You can exit out after you have logged in and then stop the Wireshark capture.

Filter your packet capture to show the HTTP POST where you entered your username and password.

Question #13: What filter did you use? (.5 point)
The filter that I used was http.request.method == "POST".

Question #14: Cut and paste a screenshot of your packet capture that shows the username and password. (.5 point)

```
POST /login.php HTTP/1.1
Host: dvwa.example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dvwa.example.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Connection: keep-alive
Cookie: PHPSESSID=0b40ruafu4tddqtqgqjbsiib16; security=low
Upgrade-Insecure-Requests: 1

username=jb9war&password=pasword_example&Login=Login&user_token=2d8ad07094f19ea7cf0a31c9135f6e91HTTP/1.1 302 Found
Date: Sun, 13 Feb 2022 18:34:15 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

NOTE: *We will be using dvwa.example.com in future labs, so feel free to look around.*

By submitting this assignment you are digitally signing the honor code, "I pledge that I have neither given nor received help on this assignment".

END OF EXERCISE

References

- Wireshark https://www.wireshark.org/