

## Lab Exercise 3 – Sniffing

Due Date: September 23, 2022 11:59pm  
Points Possible: 7 points

Name: **Jingtao** Scott Hong jh4ctf

*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 an important network monitoring, security, and forensic concept – reading and understanding networking traffic. Wireshark (software known as a packet analyzer or sniffer) 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

**\*\*NOTE** – you can complete Task 1 of this lab on your own computer if you install Wireshark. Otherwise, use Wireshark on the Cyber Range, but make sure to use the range's web browser to download the pcap file to the range.

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. On the Cyber Range, the file will be downloaded to 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. You can also drag the file to an open Wireshark window to open it.

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

Username: fake Password: user

**Question #2:** What is the operating system and version of the server that the user logged into? (.5 point)

OS: OpenBSD/i386 (oof)

Version: 2.6-beta(oof)

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

```
$ /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\\_jpeg.cap.gz](https://wiki.wireshark.org/uploads/_moin_import/attachments/SampleCaptures/http_with_jpeg.cap.gz)

**Question #4:** Paste a screenshot of the last image that was downloaded. (.5 point)



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

Date: Sat, 20 Nov 2004 10:21:06 GMT\r\n

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](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)

User: anonymous  
Password: h4x0r@evil.com

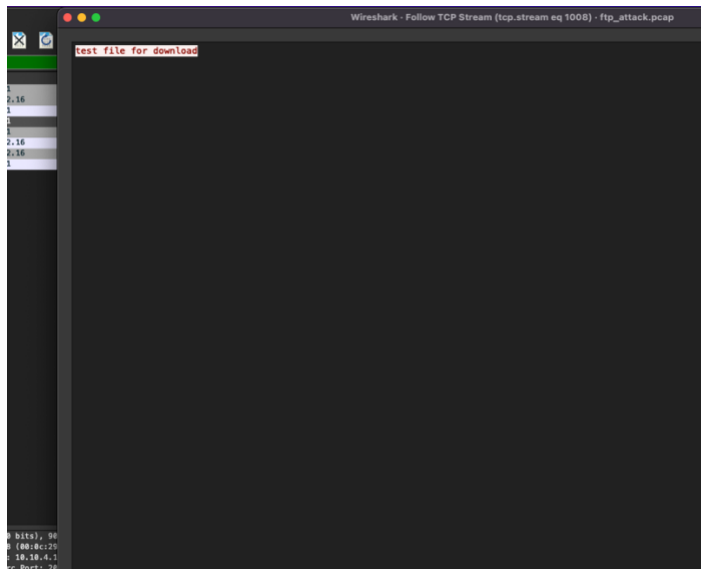
**Question #7:** What is the name and version of the FTP software on the server? (.5 point)

Name: vsFTPD  
Version: 2.2.2

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

file.txt

**Question #9:** What is the content of the file downloaded? (.5 point)



Test file for download

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 successfully authenticated? (.5 point)

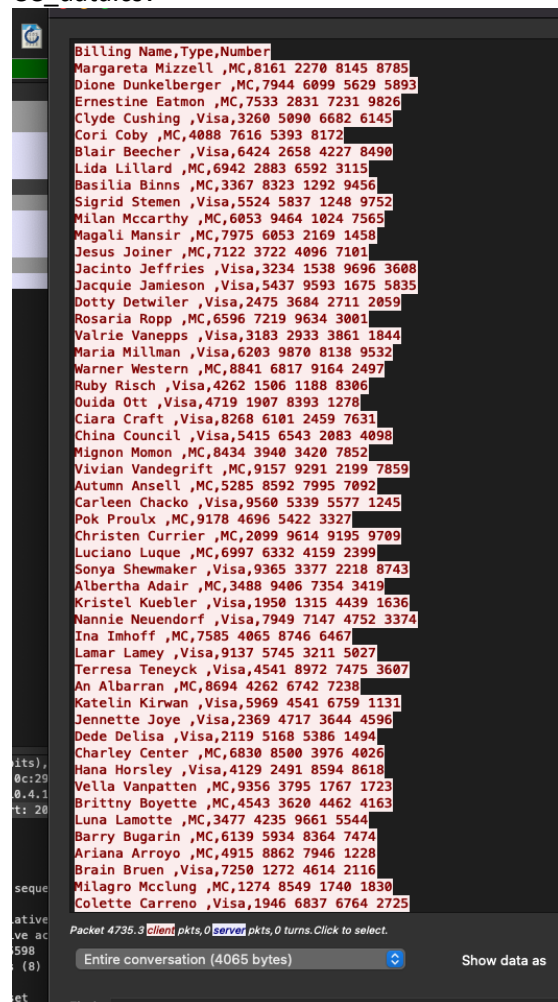
User: golightly  
Password: letmein

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

CC\_data.csv  
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)

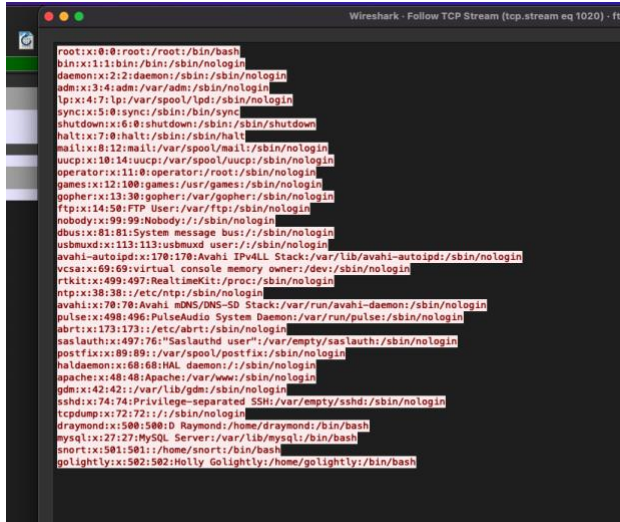
CC\_data.csv



The screenshot shows a network traffic analysis tool displaying a list of billing records. The records are organized into columns: Billing Name, Type, and Number. The list includes names such as Margaret Mizzell, Dione Dunkelberger, Ernestine Eatmon, Clyde Cushing, Cori Coby, Blair Beecher, Lida Lillard, Basilia Binns, Sigrid Stemen, Milan McCarthy, Magali Mansir, Jesus Joiner, Jacinto Jeffries, Jacquie Jamieson, Dotty Detwiler, Rosaria Ropp, Valrie Vanepps, Maria Millman, Warner Western, Ruby Risch, Ouida Ott, Ciara Craft, China Council, Mignon Momon, Vivian Vandegrift, Autumn Ansell, Carleen Chacko, Pok Proulx, Christen Currier, Luciano Luque, Sonya Shewmaker, Albertha Adair, Kristel Kuebler, Nannie Neundorf, Ina Imhoff, Lamar Lamey, Terresa Teneyck, An Albarran, Katelin Kirwan, Jennette Joye, Dede Delisa, Charley Center, Hana Horsley, Vella Vanpatten, Brittny Boyette, Luna Lamotte, Barry Bugarin, Ariana Arroyo, Brain Bruen, Milagro McClung, and Colette Carreno. The tool also shows packet details at the bottom, including packet 4735.3, client packets, and server packets.

Passwd:





*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. You will need to research how to extract them.*

## Task 2: Capturing traffic real-time using Wireshark

**\*\*NOTE – Task 2 must be completed in the Cyber Range.**

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](http://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.

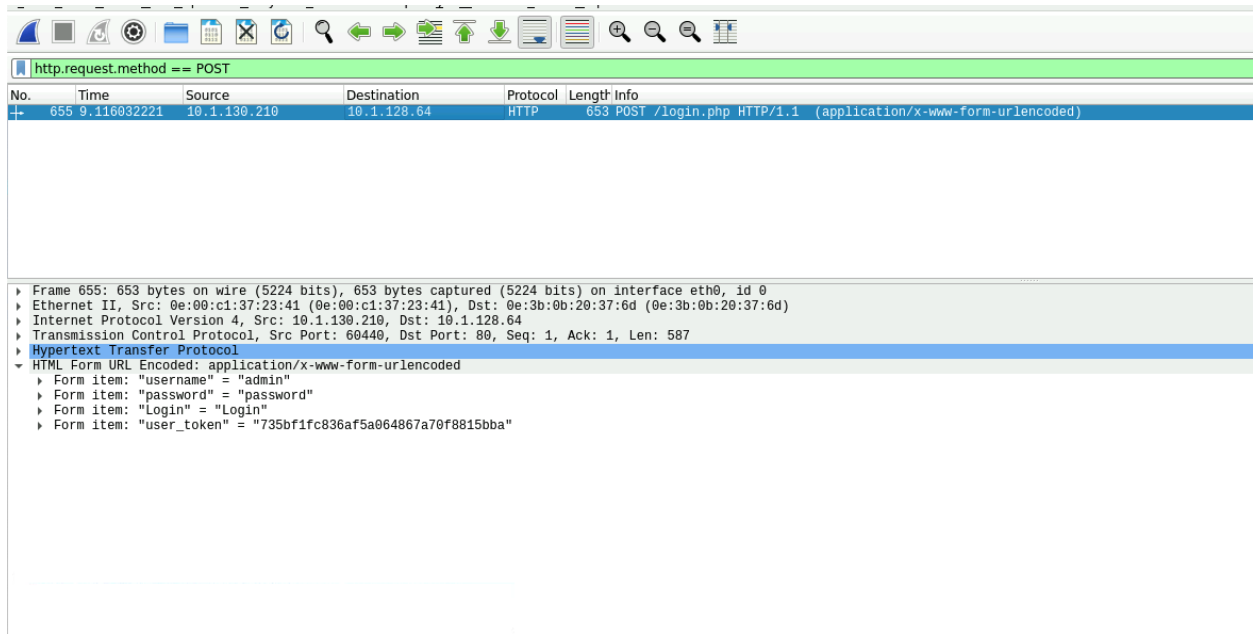
Filter your packet capture to show the HTTP POST where you entered your username and password.

**Question #13:** What filter did you use? (.5 point)

`http.request.method == POST`

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





**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/>