CS 3710 Introduction to Cybersecurity
Term: Fall 2023

Lab Exercise 3 – Sniffing

Due Date: February 17, 2023 11:59pm
Points Possible: 7 points

Name: Sidhardh Burre

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.

```
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on ttyp2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
..........
.--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
.          ..         .cshrc     .login     .mailrc    .profile   .rhosts
$ exit
```

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

If we use rightclick a Telnet package and select "follow > TCP Stream" we can examine the entire transmission. We find that the username is "fake" and the password is "user".

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

The operating system is OpenBSD and the version is 2.6-beta.

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

The user ran the "/sbin/ping www.yahoo.com" command which I believe pings yahoo.com. They also performed two "ls's". The first was an "ls" that returned nothing. But after they added the "-a" flag and re-ran the command they got some results (seen in the sc). The user subsequently exited.

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
Open this file in Wireshark to analyze it.

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)

This was downloaded Nov 19, 2004 at 22:29:25 UTC.

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)

The username is "anonymous" and the password is "h4x0r@evil.com".

4340	87.186188	112.13.12.16	10.10.4.1	TCP	74	52159 → 21 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=87574351 TSecr=0 WS=64
4341	87.186471	10.10.4.1	112.13.12.16	TCP	74	21 → 52159 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=201611 TSec
4342	87.186492	112.13.12.16	10.10.4.1	TCP	66	52159 → 21 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=87574351 TSecr=201611
4343	87.229611	10.10.4.1	112.13.12.16	FTP	86	Response: 220 (vsFTPd 2.2.2)
4344	87.230018	112.13.12.16	10.10.4.1	TCP	66	52159 → 21 [ACK] Seq=1 Ack=21 Win=5888 Len=0 TSval=87574362 TSecr=201654
4346	94.172984	112.13.12.16	10.10.4.1	FTP	82	Request: USER anonymous
4347	94.173614	10.10.4.1	112.13.12.16	TCP	66	21 → 52159 [ACK] Seq=21 Ack=17 Win=14528 Len=0 TSval=208602 TSecr=87576098
4348	94.174145	10.10.4.1	112.13.12.16	FTP	100	Response: 331 Please specify the password.
4349	94.174215	112.13.12.16	10.10.4.1	TCP	66	52159 → 21 [ACK] Seq=17 Ack=55 Win=5888 Len=0 TSval=87576098 TSecr=208603
4351	107.804261	112.13.12.16	10.10.4.1	FTP	87	Request: PASS h4x0r@evil.com
4352	107.845522	10.10.4.1	112.13.12.16	TCP	66	21 → 52159 [ACK] Seq=55 Ack=38 Win=14528 Len=0 TSval=222279 TSecr=87579506
4353	107.851351	10.10.4.1	112.13.12.16	FTP	89	Response: 230 Login successful.
4354	107.851527	112.13.12.16	10.10.4.1	TCP	66	52159 → 21 [ACK] Seq=38 Ack=78 Win=5888 Len=0 TSval=87579517 TSecr=222285
4355	107.851756	112.13.12.16	10.10.4.1	FTP	72	Request: SYST
4356	107.852242	10.10.4.1	112.13.12.16	TCP	66	21 → 52159 [ACK] Seq=78 Ack=44 Win=14528 Len=0 TSval=222286 TSecr=87579518
4357	107.853342	10.10.4.1	112.13.12.16	FTP	85	Response: 215 UNIX Type: L8
4358	107.891689	112.13.12.16	10.10.4.1	TCP	66	52159 → 21 [ACK] Seq=44 Ack=97 Win=5888 Len=0 TSval=87579528 TSecr=222287

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

I believe that it is vsFTPd version 2.2.2. This is detailed two lines above the blue line in the sc above.

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

The name of the downloaded file is "file.txt"

4499	151.923075	112.13.12.16	10.10.4.1	FTP	81	Request: RETR file.txt
4500	151.923973	10.10.4.1	112.13.12.16	TCP	74	20 → 54778 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=266367 TSecr=0 WS=64
4501	151.924008	112.13.12.16	10.10.4.1	TCP	74	54778 → 20 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=87590536 TSec…
4502	151.924474	10.10.4.1	112.13.12.16	TCP	66	20 → 54778 [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=266368 TSecr=87590536
4503	151.924858	10.10.4.1	112.13.12.16	FTP	132	Response: 150 Opening BINARY mode data connection for file.txt (24 bytes).
4504	151.964708	112.13.12.16	10.10.4.1	TCP	66	52159 → 21 [ACK] Seq=359 Ack=1132 Win=5888 Len=0 TSval=87590546 TSecr=266368
4505	152.020070	10.10.4.1	112.13.12.16	FTP-DA…	90	FTP Data: 24 bytes (PORT) (RETR file.txt)
4506	152.020574	10.10.4.1	112.13.12.16	TCP	66	20 → 54778 [FIN, ACK] Seq=25 Ack=1 Win=14656 Len=0 TSval=266464 TSecr=87590536
4507	152.020969	112.13.12.16	10.10.4.1	TCP	66	54778 → 20 [ACK] Seq=1 Ack=25 Win=5824 Len=0 TSval=87590560 TSecr=266463
4508	152.021238	112.13.12.16	10.10.4.1	TCP	66	54778 → 20 [FIN, ACK] Seq=1 Ack=26 Win=5824 Len=0 TSval=87590560 TSecr=266464
4509	152.021688	10.10.4.1	112.13.12.16	TCP	66	20 → 54778 [ACK] Seq=26 Ack=2 Win=14656 Len=0 TSval=266465 TSecr=87590560
4510	152.024555	10.10.4.1	112.13.12.16	FTP	90	Response: 226 Transfer complete.

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

After hitting "follow TCP stream" I came up with:

Wireshark · Follow TCP Stream (tcp.stream eq 1008) · ftp_attack.pcap

```
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)

The new username is "golightly" and the password is "letmein"

4676	274.730814	112.13.12.16	10.10.4.1	TCP	66	52164 → 21 [ACK] Seq=1 Ack=21 Win=5888 Len=0 TSval=87621237 TSecr=389174
4677	279.341692	112.13.12.16	10.10.4.1	FTP	82	Request: USER golightly
4678	279.342384	10.10.4.1	112.13.12.16	TCP	66	21 → 52164 [ACK] Seq=21 Ack=17 Win=14528 Len=0 TSval=393787 TSecr=87622390
4679	279.342906	10.10.4.1	112.13.12.16	FTP	100	Response: 331 Please specify the password.
4680	279.342977	112.13.12.16	10.10.4.1	TCP	66	52164 → 21 [ACK] Seq=17 Ack=55 Win=5888 Len=0 TSval=87622390 TSecr=393787
4681	282.613924	112.13.12.16	10.10.4.1	FTP	80	Request: PASS letmein
4682	282.619807	192.168.5.1	192.168.5.129	ICMP	113	Destination unreachable (Port unreachable)
4683	282.619823	192.168.5.129	192.168.5.1	DNS	85	Standard query 0xc40e PTR 16.12.13.112.in-addr.arpa
4684	282.620318	192.168.5.1	192.168.5.129	ICMP	113	Destination unreachable (Port unreachable)
4685	282.620332	192.168.5.129	192.168.5.1	DNS	85	Standard query 0xc40e PTR 16.12.13.112.in-addr.arpa

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

The first file is "CC_data.csv" and the second file is "passwd".

Wireshark · Follow TCP Stream (tcp.stre

```
220 (vsFTPd 2.2.2)
USER golightly
331 Please specify the password.
PASS letmein
230 Login successful.
SYST
215 UNIX Type: L8
PORT 112,13,12,16,228,108
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
PWD
257 "/home/golightly"
PORT 112,13,12,16,167,225
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 112,13,12,16,163,246
200 PORT command successful. Consider using PASV.
RETR CC_data.csv
150 Opening BINARY mode data connection for CC_data.csv (4065 bytes).
226 Transfer complete.
TYPE A
200 Switching to ASCII mode.
PORT 112,13,12,16,176,160
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD ..
250 Directory successfully changed.
PORT 112,13,12,16,176,93
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD ..
250 Directory successfully changed.
PWD
257 "/"
CWD etc
250 Directory successfully changed.
TYPE I
200 Switching to Binary mode.
PORT 112,13,12,16,186,19
200 PORT command successful. Consider using PASV.
RETR passwd
150 Opening BINARY mode data connection for passwd (1669 bytes).
226 Transfer complete.
```

Packet 4675. 24 client pkt(s), 31 server pkt(s), 48 turn(s). Click to select.

Entire conversation (1404 bytes) Show and save data as ASCII

Find:

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)

For “CC_data.csv”:

Wireshark - Follow TCP Stream (tcp.stream eq 1017) - ftp_attack.pcap

```
Billing Name,Type,Number
Margareta Mizzell ,MC,8161 2270 8145 8785
Dione Dunkelberger ,MC,7944 6099 5629 5893
Ernestine Eatmon ,MC,7533 2831 7231 9826
Clyde Cushing ,Visa,3260 5090 6682 6145
Cori Coby ,MC,4088 7616 5393 8172
Blair Beecher ,Visa,6424 2658 4227 8490
Lida Lillard ,MC,6942 2883 6592 3115
Basilia Binns ,MC,3367 8323 1292 9456
Sigrid Stemen ,Visa,5524 5837 1248 9752
Milan Mccarthy ,MC,6053 9464 1024 7565
Magali Mansir ,MC,7975 6053 2169 1458
Jesus Joiner ,MC,7122 3722 4096 7101
Jacinto Jeffries ,Visa,3234 1538 9696 3608
Jacquie Jamieson ,Visa,5437 9593 1675 5835
Dotty Detwiler ,Visa,2475 3684 2711 2059
Rosaria Ropp ,MC,6596 7219 9634 3001
Valrie Vanepps ,Visa,3183 2933 3861 1844
Maria Millman ,Visa,6203 9870 8138 9532
Warner Western ,MC,8841 6817 9164 2497
Ruby Risch ,Visa,4262 1506 1188 8306
Ouida Ott ,Visa,4719 1907 8393 1278
Ciara Craft ,Visa,8268 6101 2459 7631
China Council ,Visa,5415 6543 2083 4098
Mignon Momon ,MC,8434 3940 3420 7852
Vivian Vandegrift ,MC,9157 9291 2199 7859
Autumn Ansell ,MC,5285 8592 7995 7092
Carleen Chacko ,Visa,9560 5339 5577 1245
Pok Proulx ,MC,9178 4696 5422 3327
Christen Currier ,MC,2099 9614 9195 9709
Luciano Luque ,MC,6997 6332 4159 2399
Sonya Shewmaker ,Visa,9365 3377 2218 8743
Albertha Adair ,MC,3488 9406 7354 3419
Kristel Kuebler ,Visa,1950 1315 4439 1636
Nannie Neuendorf ,Visa,7949 7147 4752 3374
Ina Imhoff ,MC,7585 4065 8746 6467
Lamar Lamey ,Visa,9137 5745 3211 5027
Terresa Teneyck ,Visa,4541 8972 7475 3607
An Albarran ,MC,8694 4262 6742 7238
Katelin Kirwan ,Visa,5969 4541 6759 1131
Jennette Joye ,Visa,2369 4717 3644 4596
Dede Delisa ,Visa,2119 5168 5386 1494
Charley Center ,MC,6830 8500 3976 4026
Hana Horsley ,Visa,4129 2491 8594 8618
Vella Vanpatten ,MC,9356 3795 1767 1723
Brittny Boyette ,MC,4543 3620 4462 4163
Luna Lamotte ,MC,3477 4235 9661 5544
Barry Bugarin ,MC,6139 5934 8364 7474
Ariana Arroyo ,MC,4915 8862 7946 1228
Brain Bruen ,Visa,7250 1272 4614 2116
Milagro Mcclung ,MC,1274 8549 1740 1830
Colette Carreno ,Visa,1946 6837 6764 2725
```

For “passwd”:

Wireshark · Follow TCP Stream (tcp.stream eq 1020) · ftp_attack.pcap

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
saslauth:x:497:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
draymond:x:500:500:D Raymond:/home/draymond:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
snort:x:501:501::/home/snort:/bin/bash
golightly:x:502:502:Holly Golightly:/home/golightly:/bin/bash
```

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. 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.

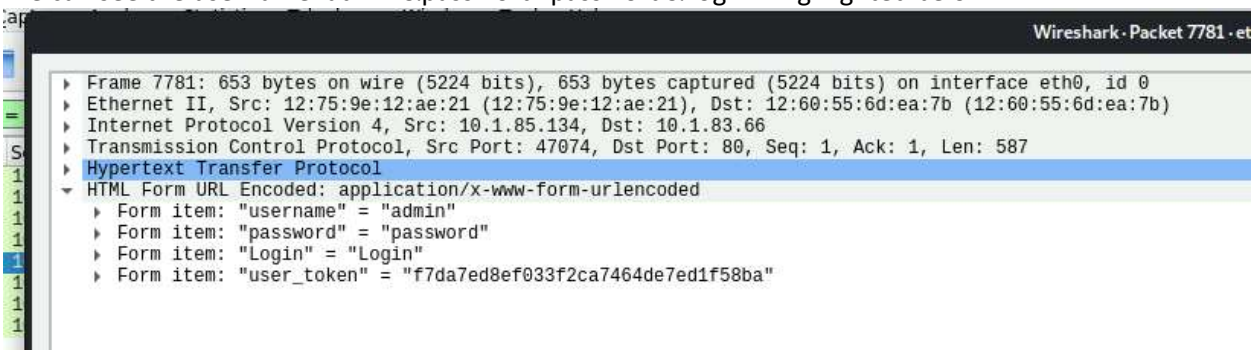
Question #13: What filter did you use? (.5 point)

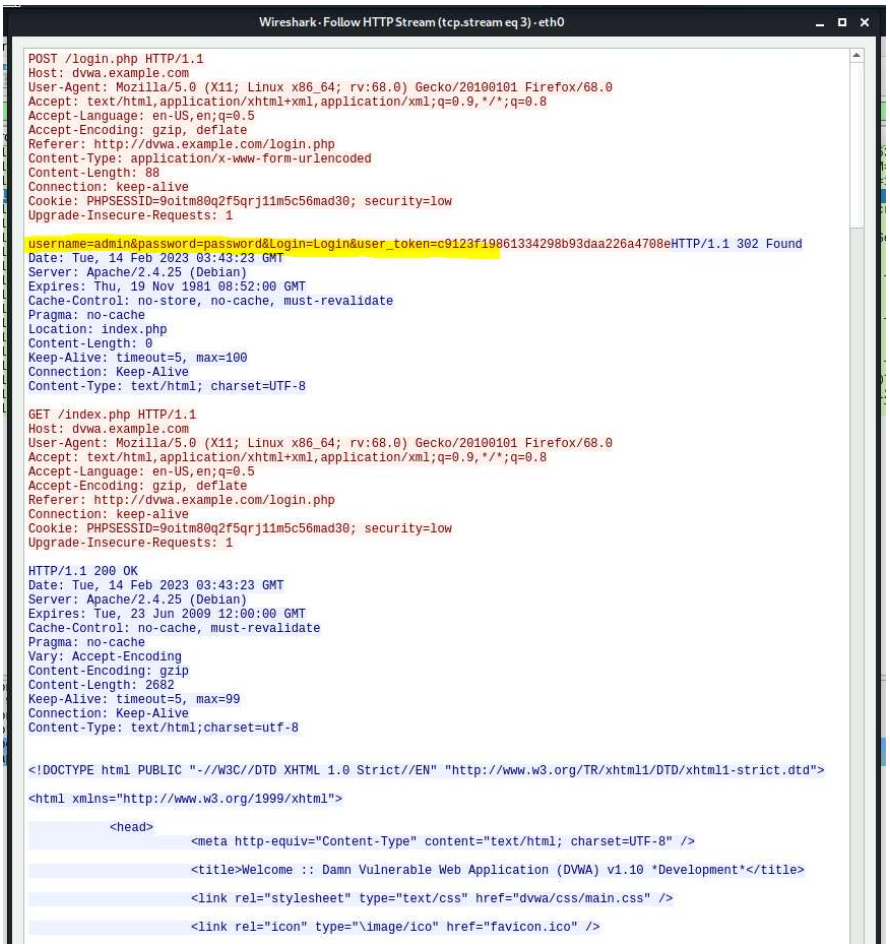
I used the filter: "http.request.method == "POST""

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

The screenshot of the packet capture found by using follow TCP stream:

We can see the username=admin&password=password&Login… highlighted below.





Wireshark · Follow HTTP Stream (tcp.stream eq 3) · eth0

```
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: 88
Connection: keep-alive
Cookie: PHPSESSID=9oitm80q2f5qrj11m5c56mad30; security=low
Upgrade-Insecure-Requests: 1

username=admin&password=password&Login=Login&user_token=c9123f19861334298b93daa226a4708eHTTP/1.1 302 Found
Date: Tue, 14 Feb 2023 03:43:23 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: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

GET /index.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
Connection: keep-alive
Cookie: PHPSESSID=9oitm80q2f5qrj11m5c56mad30; security=low
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Tue, 14 Feb 2023 03:43:23 GMT
Server: Apache/2.4.25 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2682
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

                <title>Welcome :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>

                <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

                <link rel="icon" type="\image/ico" href="favicon.ico" />
```

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/