CS 3710 Introduction to Cybersecurity
Term: Spring 2022

Lab Exercise 3 – Sniffing

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

Name: hz9xs

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.

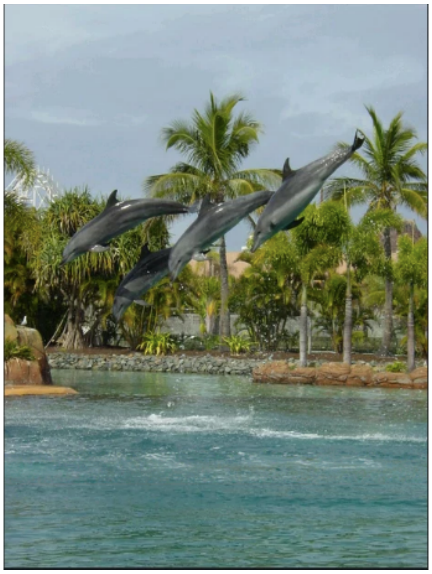
Question #1: What is the username and password of the Telnet user? (.5 point)
Username: fake
Password: user

Question #2: What is the operating system and version of the server that the user logged into? (.5 point)
Operating system: OpenBSD
Version of the server: 2.6-beta

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



Question #5: What is the date and time that the image was downloaded? (.5 point)
Nov 19, 2004 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)
Username: 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

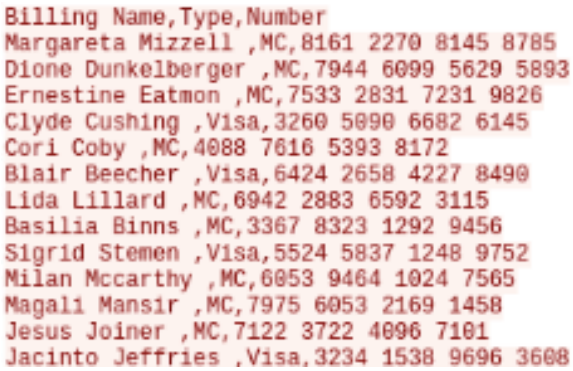
Question #9: What is the content of the file downloaded? (.5 point)
test file for download

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 successful? (.5 point)
Username: golightly
Password: letmein

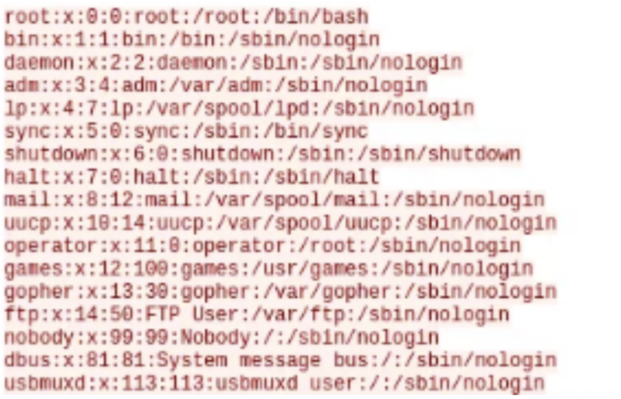
Question #11: What are the names of the 2 files that were downloaded while logged in as this new user? (.5 point)
CC_data.csv
passwd

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)
data in CC_data.csv:



```
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
```

Data in passwd:



```
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
```

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

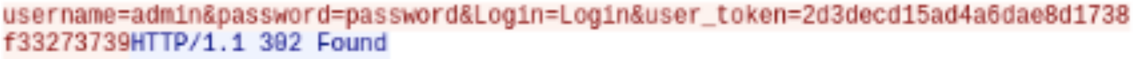
Now let's take a look at some real-time packet capturing. Make sure that you are running Wireshark as **root.**

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)
http.request.method==POST

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



```
username=admin&password=password&Login=Login&user_token=2d3decd15ad4a6dae8d1738
f33273739HTTP/1.1 302 Found
```

Username: admin
Password: password

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/

Modified by Angela Orebaugh, Ph.D, CISSP, University of Virginia