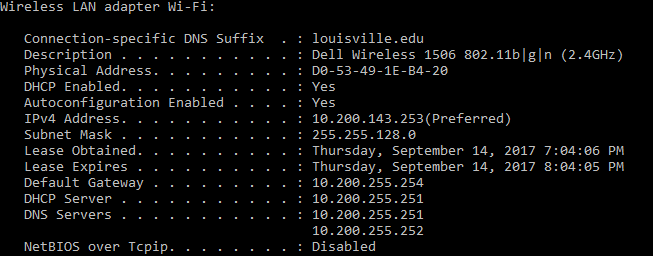
|  |
| --- |
| Lab 3: Packet Analysis II  * The due date and time is 4:00 Thur, September 21 (Sec 01) / 7:00 Thur, September 21 (Sec 76). * This is an individual assignment, and is worth 20 points. * You should provide the answers using the accompanying outcome file. Change the file name following the naming convention suggested below. * The naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Lab 1\_ImG.docx). If you do not follow the convention, I will deduct 1. * Do not copy any of the sample screenshots provided as illustrations. * You should not scan any live servers using Nmap and hping3. For violation, you may be expelled from the school (not a joke!). |

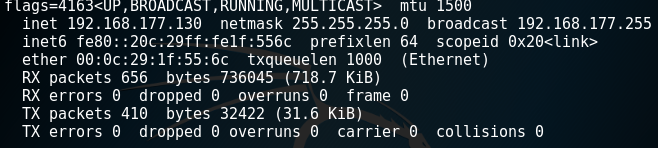
## Task 1. Figuring out the IP addresses

* Task

1. Report the IP address of your host and the subnet mask (use ipconfig /all). If you use wireless, the IP address of “Wireless LAN adapter Wi-Fi” is the active physical interface. Report with a screenshot.



1. Report the IP address of your Kali (use ifconfig). Report with a screenshot.

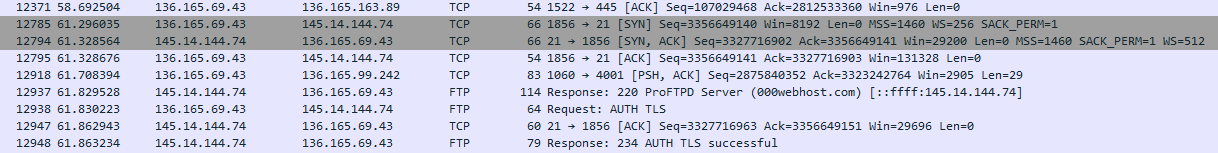


## Task 2. Analyzing FTP Signatures

* Task

1. Identify the three TCP packets used for the initial 3-way handshaking. Take a screenshot of the TCP packets.

* **Hint**: These packets are placed right before ftp packets.



1. Identify the FTP packets that show the Username and the Password. In fact, the Username and the Password are encrypted and we cannot figure it out. However, we can guess which packets have that information. Follow the TCP stream and take a screenshot of the TCP stream.

* **Hint**: Use the display filter “ftp.” And right-click on the packet of your interest and Follow > TCP Stream to understand the data flow. Use the IP address of the ftp server to recognize the relevant TCP stream. Use the display filter “tcp.stream eq xx” (replace xx with the integer) as necessary.



1. Identify the FTP-DATA packets used for the textfile uploading. Follow the TCP stream and take a screenshot of the TCP stream. The textfile is uploaded across many FTP-DATA packets. So, any part of the data is okay.

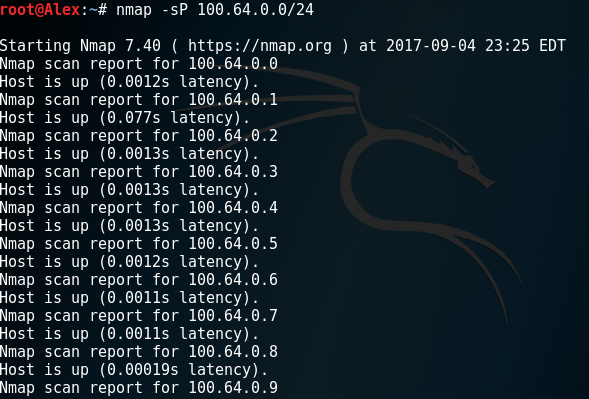
* **Hint**: You need to check out TCP packets after FTP packets.



## Task 3. Ping Sweeping

* Task

1. Report your result in a screenshot like below.



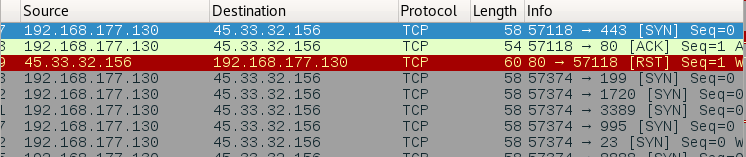
## Task 4. Port Scanning

* Task

Answer the following questions. Provide a screenshot for each question to support your answer. For the answers, use the display filter “tcp.stream eq xx” (replace xx with the integer) as necessary.

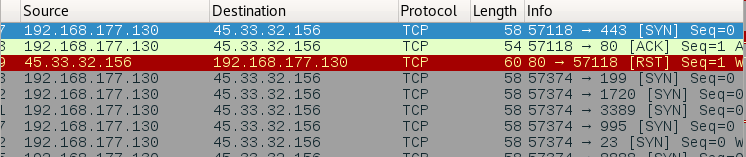
1. Which type of TCP packet (e.g., SYN, SYN/ACK, or ACK) was sent from your Kali to the victim?

SYN packet was sent from Kali to victim.



1. Which type of TCP packet (e.g., SYN, SYN/ACK, or ACK) was received from the victim to the Kali in response?

RST packet was sent from victim to Kali.



## Task 5. SYN Flooding Attack

* Task

1. Launch a SYN flooding attack using the IP address of your host as the victim and a random private IP address as the spoofed address. Report your Wireshark result in a screenshot.

