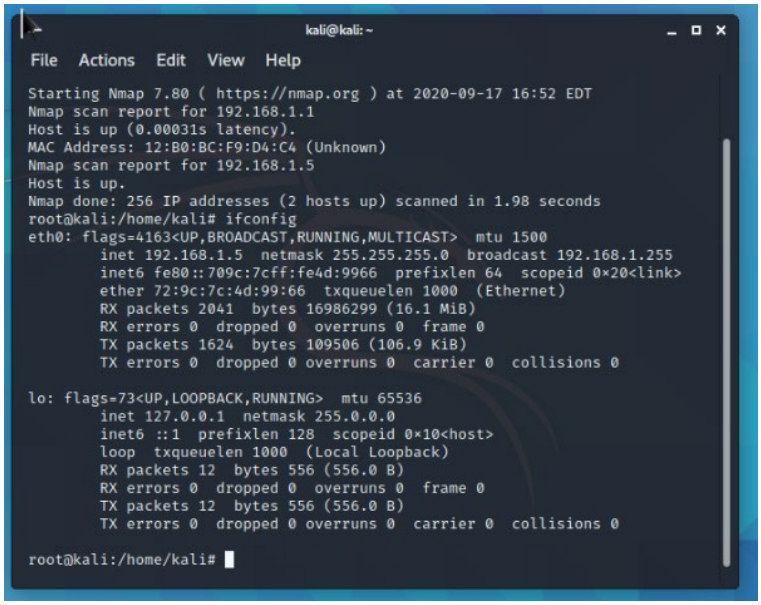
Lab 3: Packet Analysis (Part 2)

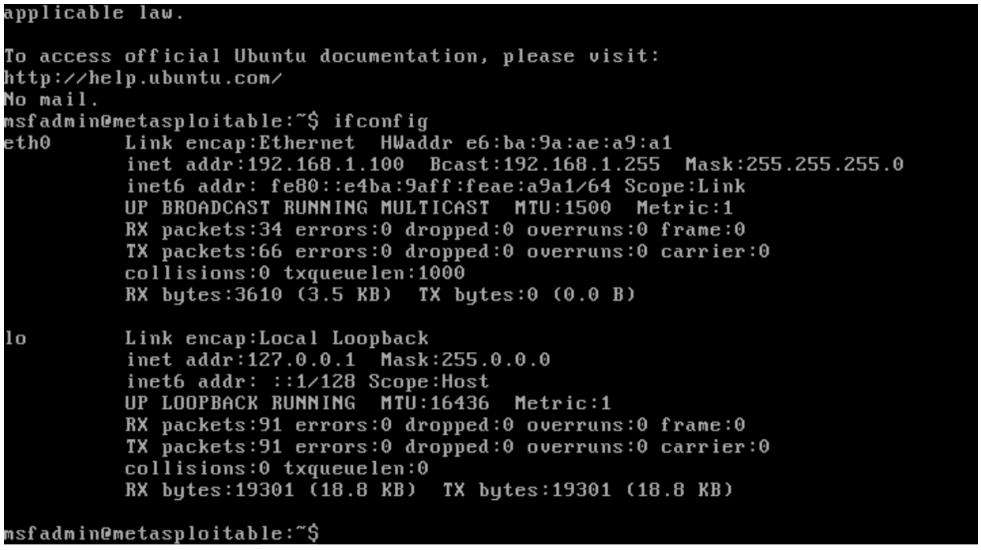
- This is an individual assignment, and worth 20 points.
- The due date is 2:30 (Sec 01) / 5:30 (Sec 76) on Friday, September 18.
- Follow the naming convention.
- You should not scan any live servers using Nmap or send malicious packets using hping3. If caught, you may be expelled from school (not a joke!).

Task 1. Identifying the IP addresses

- Find the IP address and subnet mask of **Kali** (use ifconfig). Report the result with a screenshot.

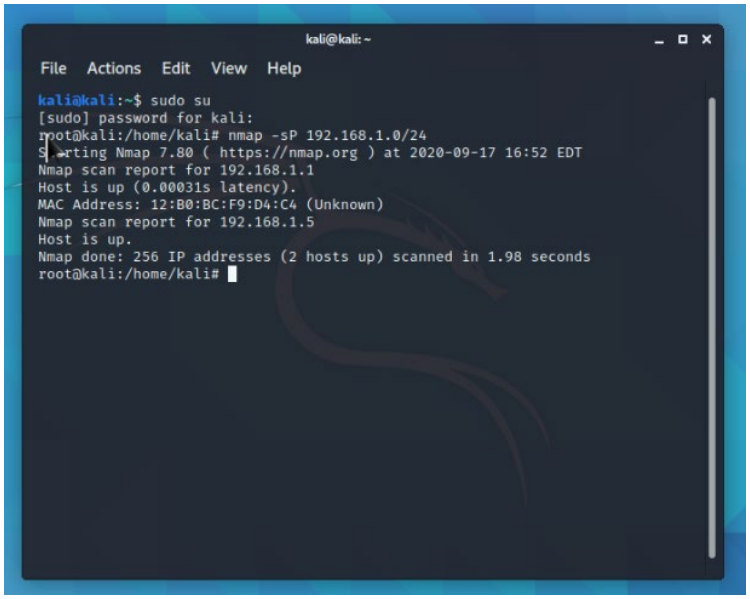


- Find the IP address and subnet mask of **Metasploitable**. Report the result with a screenshot.



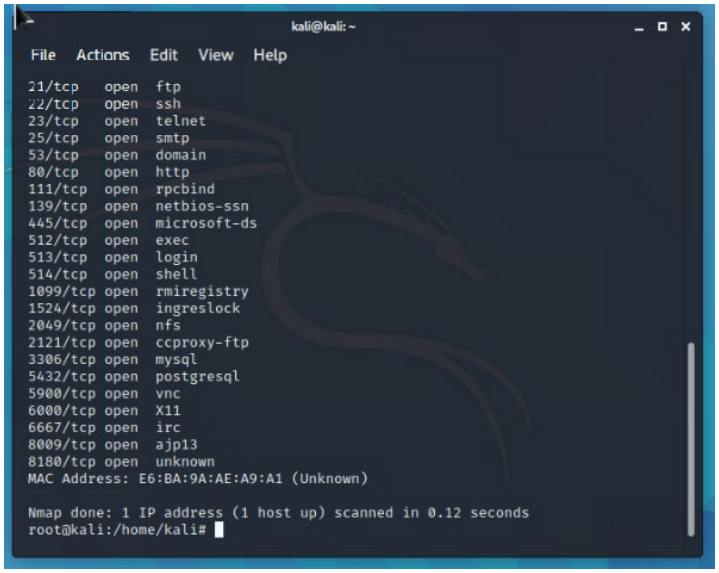
Task 2. Performing a Ping Sweeping

- Report the result with a screenshot.



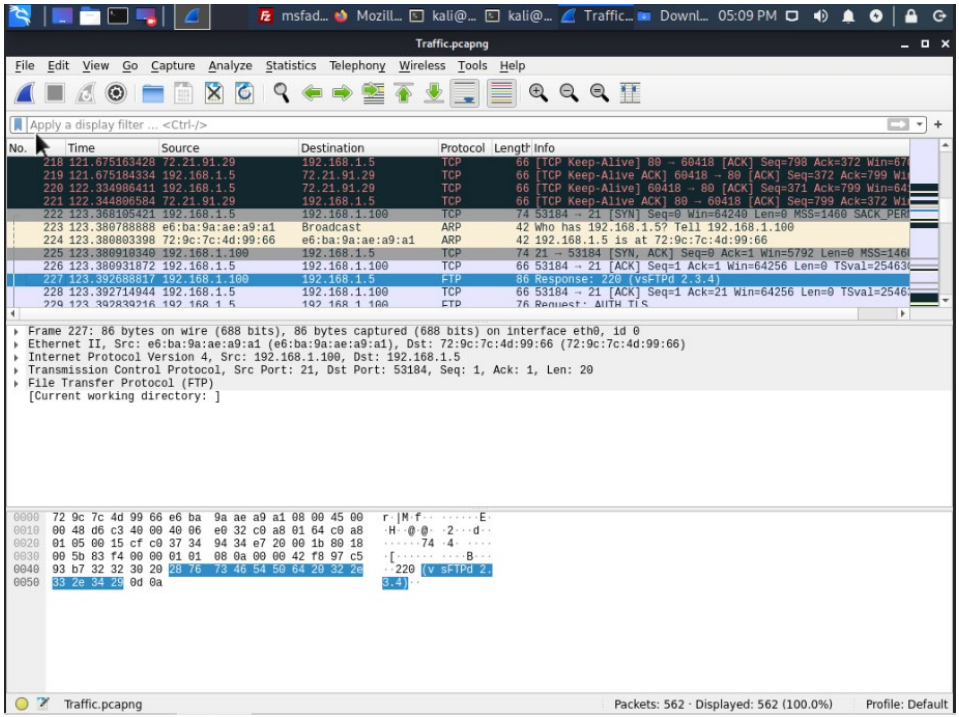
Task 3. Performing a Port Scanning

- Report the result with a screenshot.

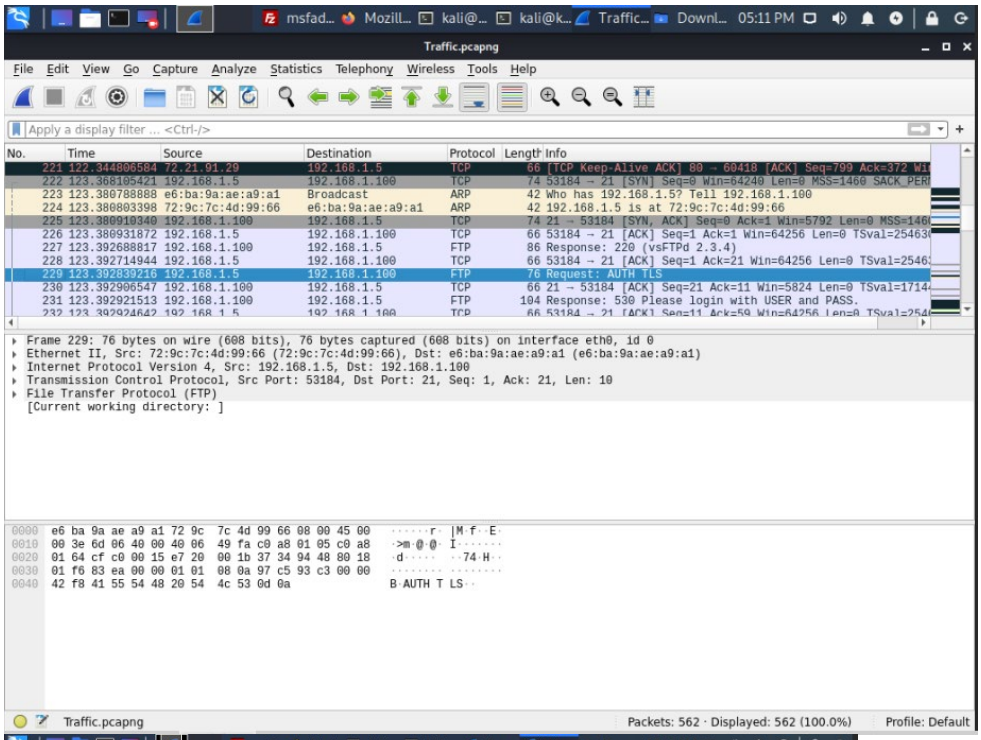


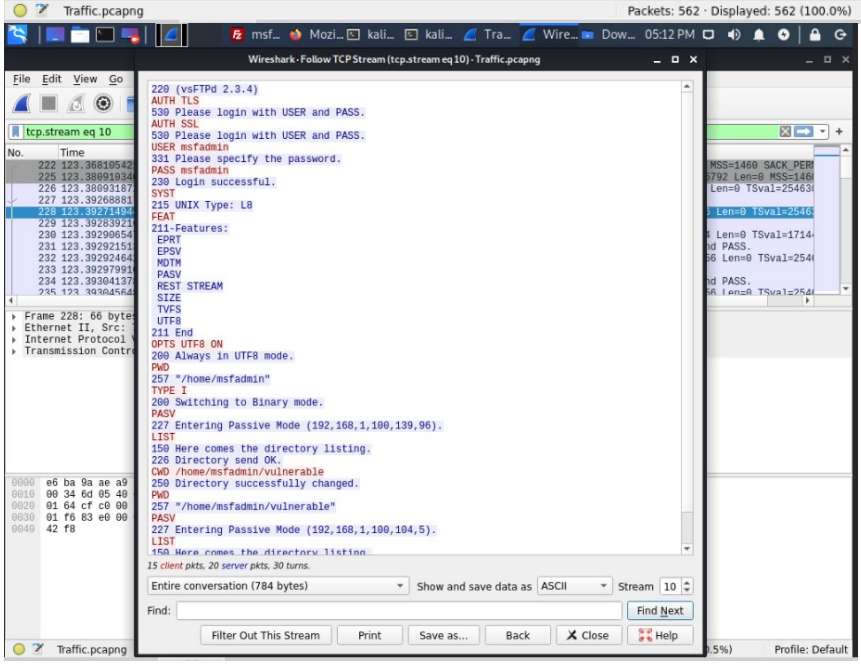
Task 4. Analyzing FTP Signatures

1) Identify the TCP packets used for the initial three-way handshake for the connection to the ftp server. Take a screenshot of those TCP packets. Those packets are placed right before the first ftp packet.

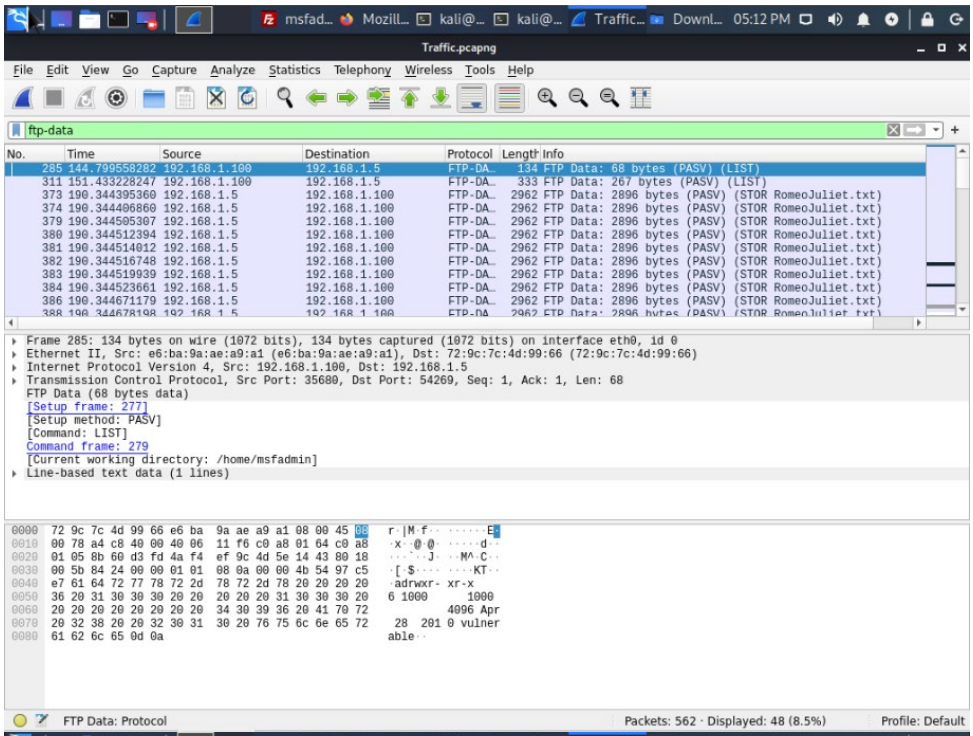


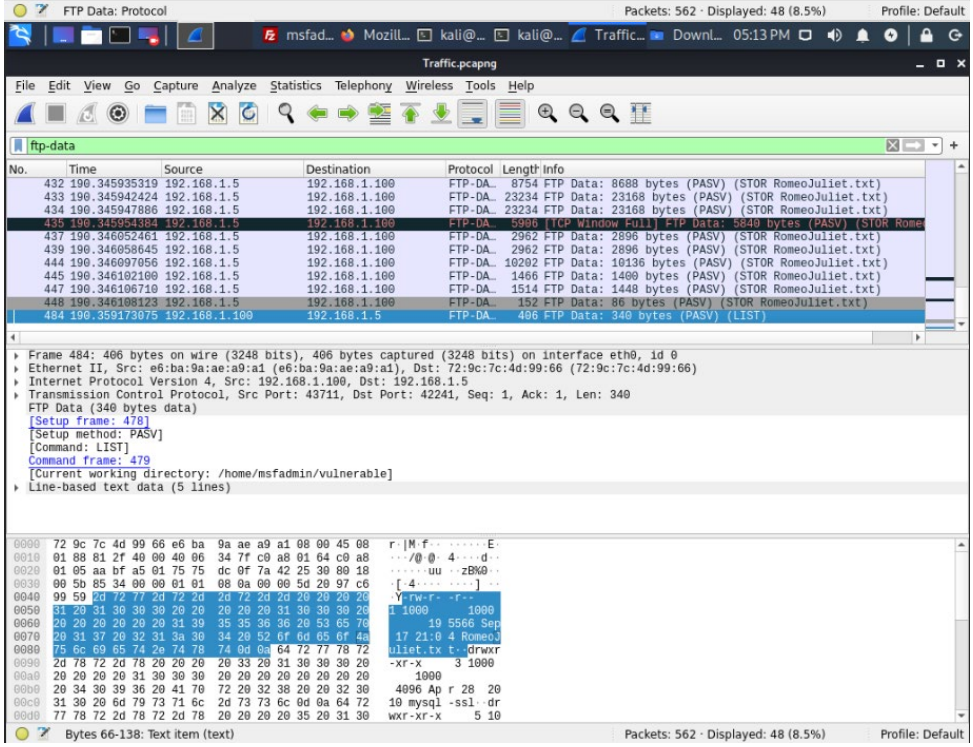
2) Identify the TCP stream used for the authentication of the client to the FTP server. Take a screenshot of the TCP stream.





3) Identify the first and last FTP-DATA packets used for the uploading of the text file. Take a screenshot for each (two required).





4) Discuss security implications of this transfer.

It's unsecure, we were able to connect to the Metaspolitable desktop with their credentials and IP address. As such we had read/write privileges which is extremely dangerous.

Task 5. SYN Flooding Attack

1) Report your Wireshark capture in a screenshot. Show only SYN packets.