Lab 2: Packet Analysis II

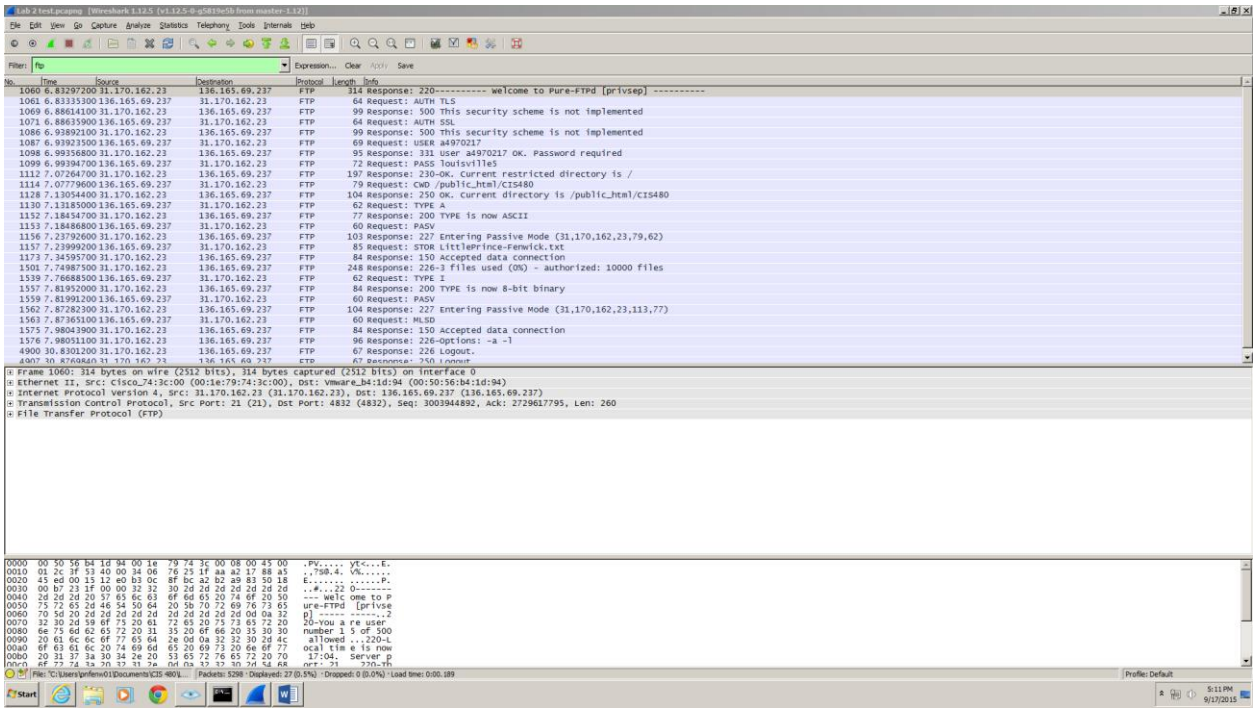
- This is an individual assignment, and is worth 10 points.
- You need to provide your answers using the accompanying submission file. Change the file name following the naming convention suggested below.
- Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Lab 1_ImG.docx). If you do not follow the convention, I will deduct 0.5.
- Do not copy any of the sample screenshots provided as illustrations.

1. Figuring out IP addresses

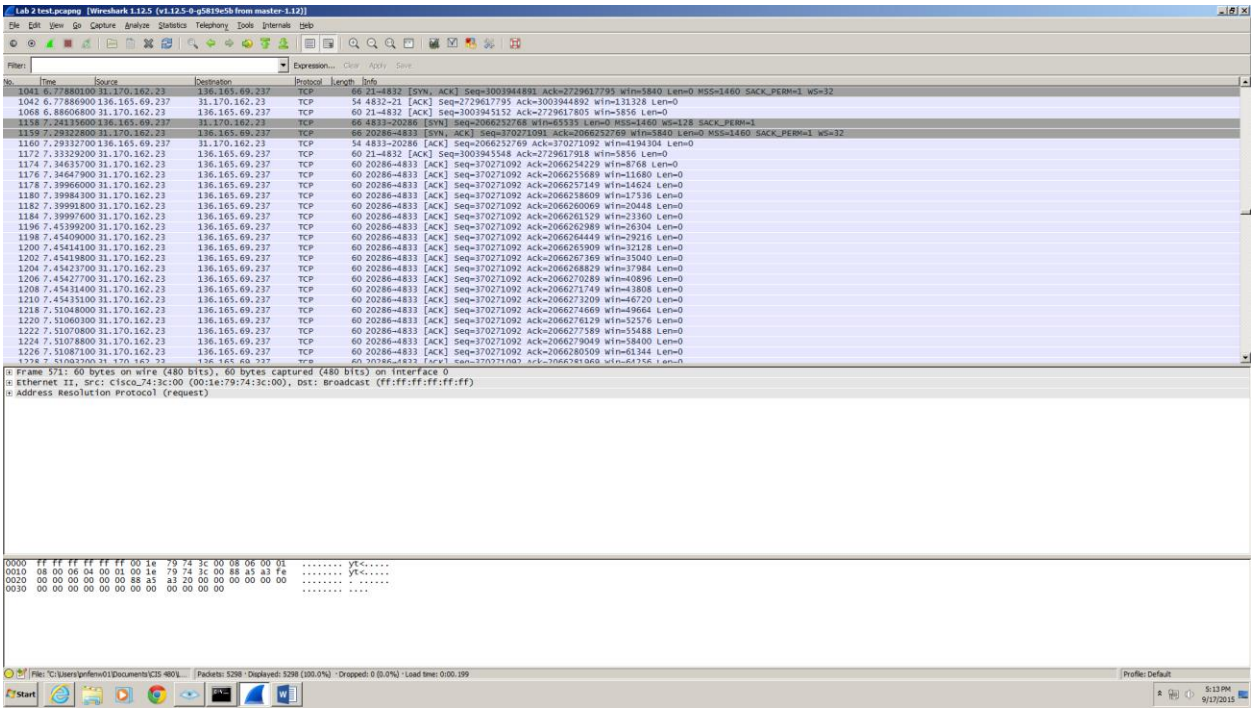
- Task
  a. Report the IP address of your host (use ipconfig /all). 192.168.43.1
  b. Report the IP address of your Kali (use ifconfig /all). 192.168.18.128

2. Analyzing FTP Signatures

- Task
  c. Identify the three TCP packets used for the initial 3-way handshaking. Take a screenshot for it.

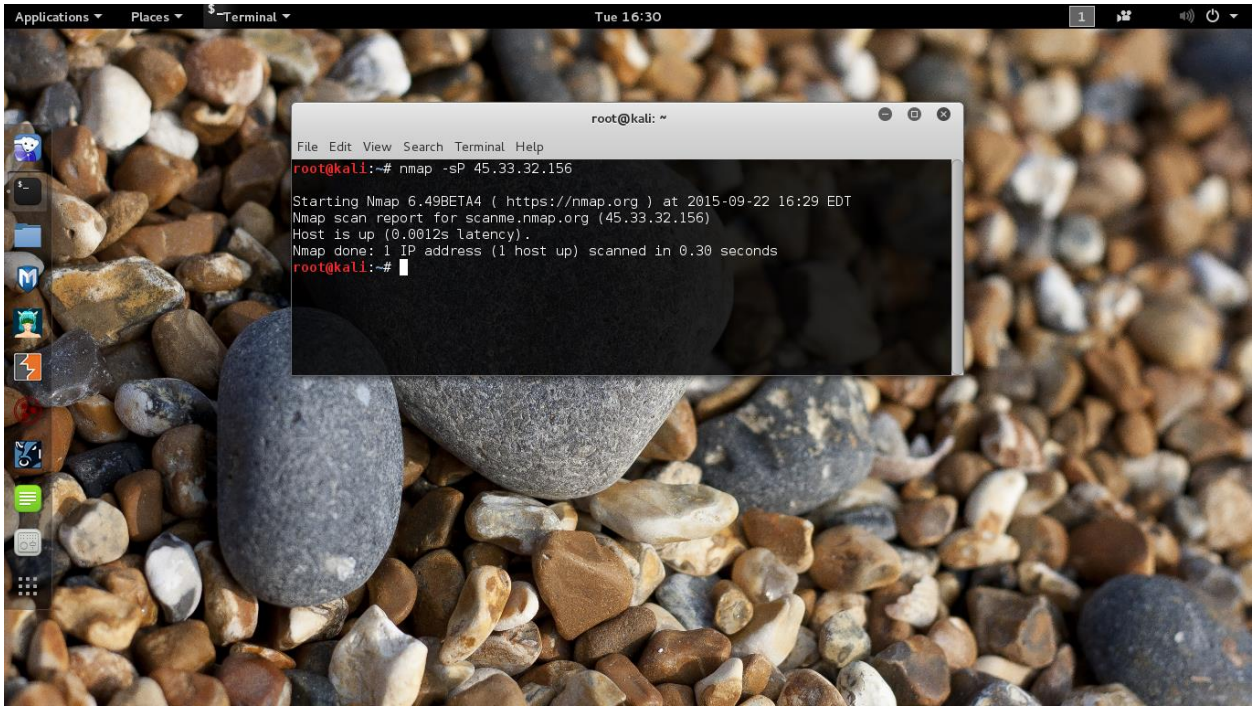


  d. Identify the FTP packets that show Username and Password in plaintext. Take a screenshot for it.



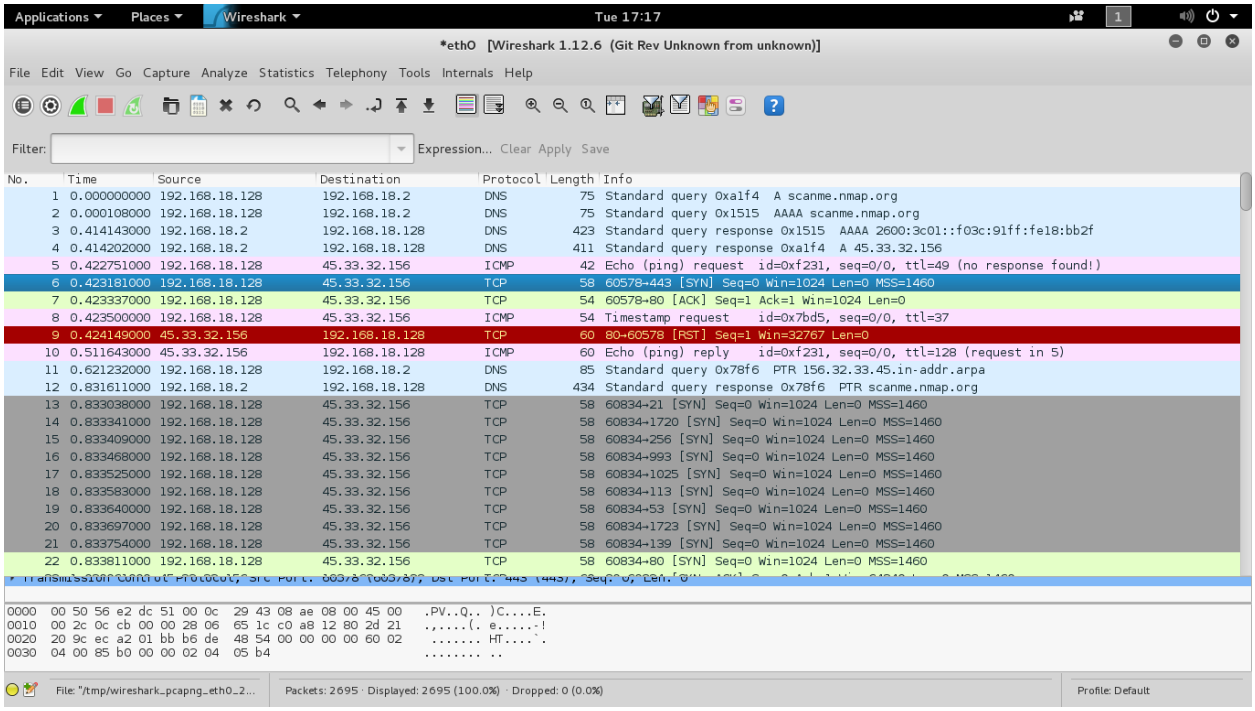
3. Ping Sweeping

- Task
  - Report your result in a screenshot like below.



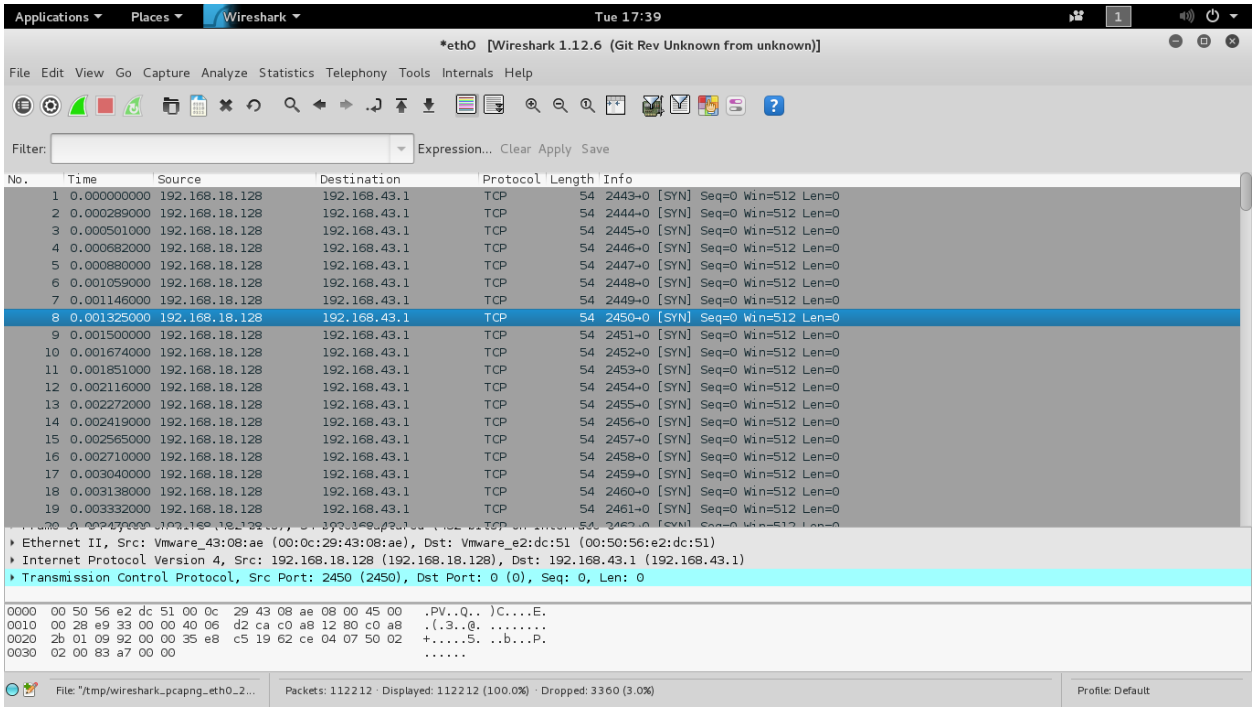
4. Port Scanning

- Task
  - Answer the following questions. Provide a screenshot for each question to support your answer.
    a. What TCP packet (e.g., SYN, SYN/ACK, ACK, etc.) was sent from the sender to the receiver at first? SYN
    b. How did the sender recognize that the specific port (e.g., port 80) of the receiver is open? That is, what TCP packet (e.g., SYN, SYN/ACK, ACK, etc.) was sent from the receiver to the sender? RST



5. SYN Flooding Attack

- Task
  - Launch a SYN flooding attack using the IP address of your host as the target and an arbitrary private IP address as the spoofed address.
    a. Report your result in a screenshot like above.



b. What ports did the attacker use for the SYN flooding attack? Give a sample range of ports you observe.

2443-3041