

Lab 2: Packet Analysis II

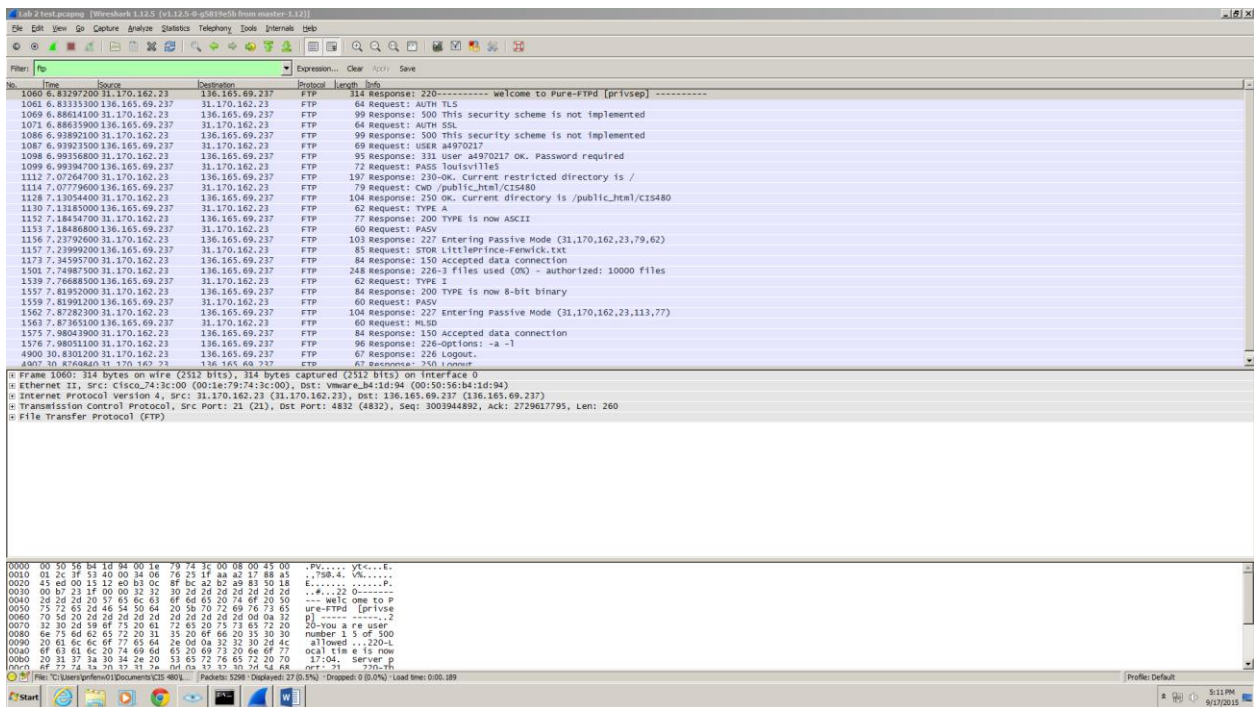
- This is an individual assignment, and is worth 10 points.
- You need to provide your answers using the accompanying submission file. Change the file name following the naming convention suggested below.
- Naming convention is as follows: homework, underscore, last name, first initial, and extension (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

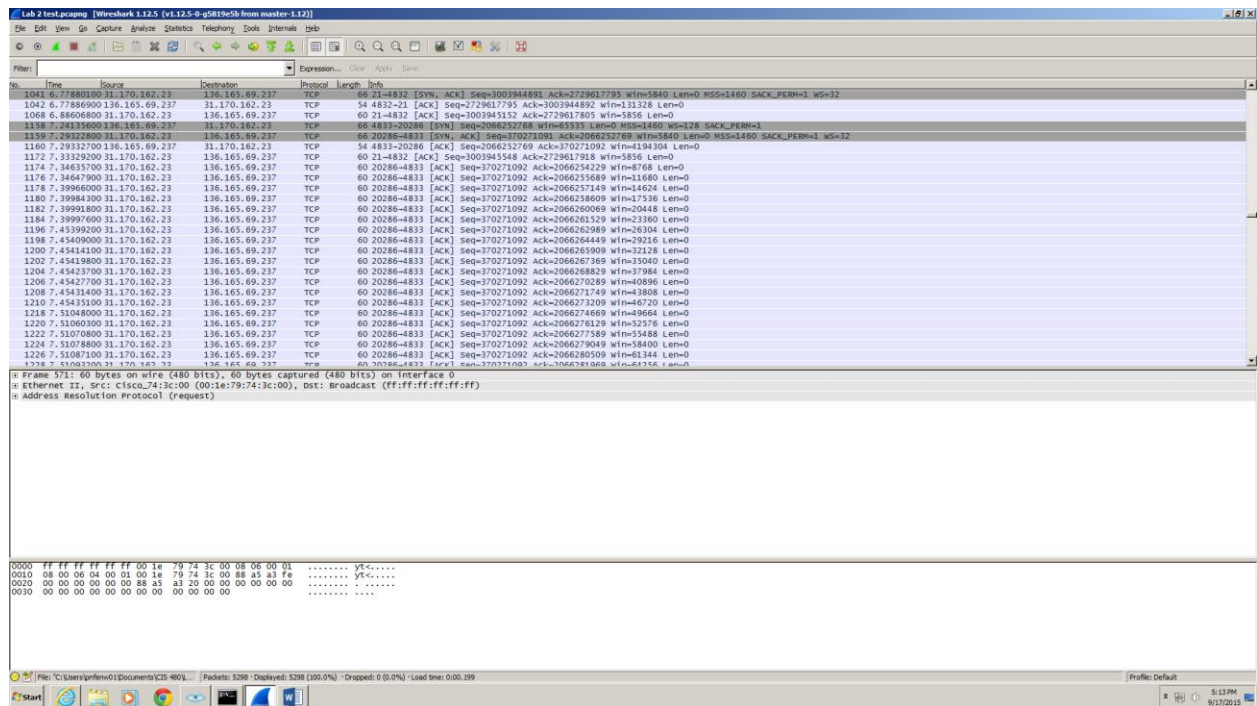
- Task
 - a. Report the IP address of your host (use `ipconfig /all`). 192.168.43.1
 - b. Report the IP address of your Kali (use `ifconfig /all`). 192.168.18.128

2. Analyzing FTP Signatures

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

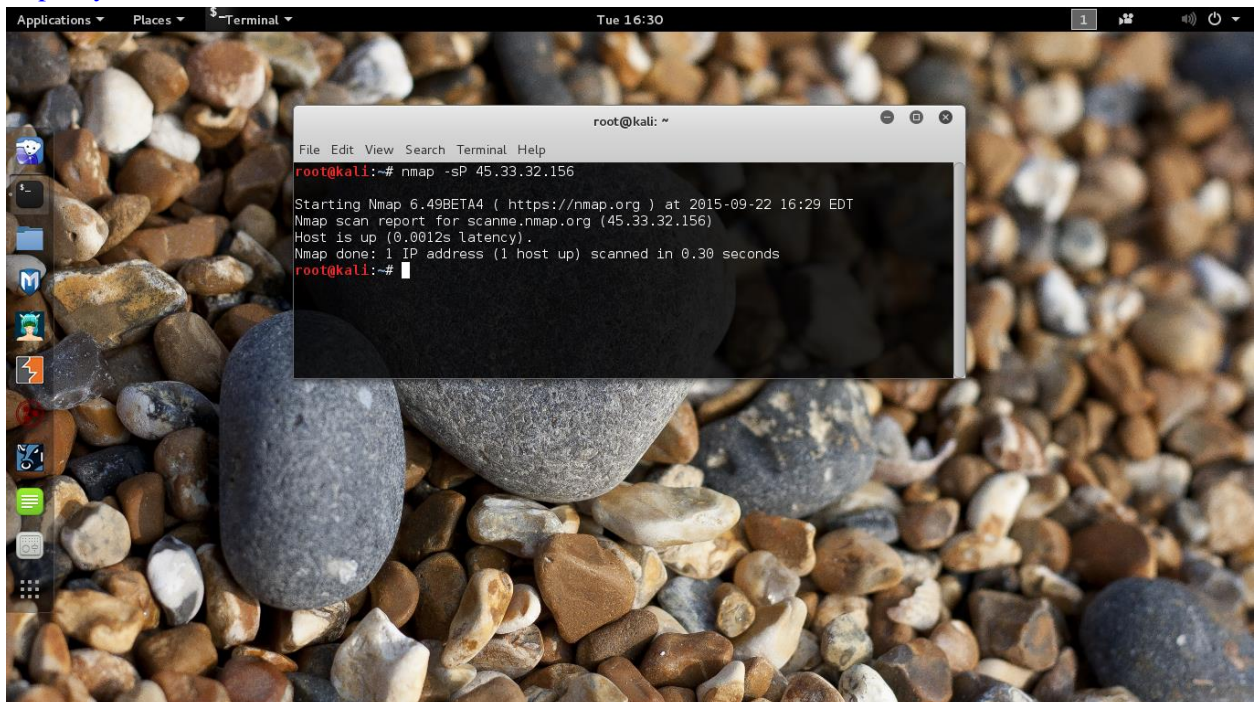


- d. Identify the FTP packets that show Username and Password in plaintext. Take a screenshot for it.



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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.18.128	192.168.18.2	DNS	75	Standard query 0x1f4 A scanme.nmap.org
2	0.000108000	192.168.18.128	192.168.18.2	DNS	75	Standard query 0x1515 AAAA scanme.nmap.org
3	0.414143000	192.168.18.2	192.168.18.128	DNS	423	Standard query response 0x1515 AAAA 2600:3c01:f03c:91ff:fe18:bb2f
4	0.414202000	192.168.18.2	192.168.18.128	DNS	411	Standard query response 0x1f4 A 45.33.32.156
5	0.422751000	192.168.18.128	45.33.32.156	ICMP	42	Echo (ping) request id=0xf231, seq=0/0, ttl=49 (no response found!)
6	0.423181000	192.168.18.128	45.33.32.156	TCP	58	60578→443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.423337000	192.168.18.128	45.33.32.156	TCP	54	60578→80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.423500000	192.168.18.128	45.33.32.156	ICMP	54	Timestamp request id=0x7bd5, seq=0/0, ttl=37
9	0.424149000	45.33.32.156	192.168.18.128	TCP	60	80→60578 [RST] Seq=1 Win=32767 Len=0
10	0.511643000	45.33.32.156	192.168.18.128	ICMP	60	Echo (ping) reply id=0xf231, seq=0/0, ttl=128 (request in 5)
11	0.621232000	192.168.18.128	192.168.18.2	DNS	85	Standard query 0x78f6 PTR 156.33.33.45.in-addr.arpa
12	0.831611000	192.168.18.2	192.168.18.128	DNS	434	Standard query response 0x78f6 PTR scanme.nmap.org
13	0.833038000	192.168.18.128	45.33.32.156	TCP	58	60834→21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.833341000	192.168.18.128	45.33.32.156	TCP	58	60834→1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.833409000	192.168.18.128	45.33.32.156	TCP	58	60834→256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.833468000	192.168.18.128	45.33.32.156	TCP	58	60834→993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.833525000	192.168.18.128	45.33.32.156	TCP	58	60834→1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.833583000	192.168.18.128	45.33.32.156	TCP	58	60834→113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.833640000	192.168.18.128	45.33.32.156	TCP	58	60834→53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.833697000	192.168.18.128	45.33.32.156	TCP	58	60834→1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.833754000	192.168.18.128	45.33.32.156	TCP	58	60834→139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	0.833811000	192.168.18.128	45.33.32.156	TCP	58	60834→80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

File: "/tmp/wireshark-pcapng_eth0-2..." Packets: 2695 · Displayed: 2695 (100.0%) · Dropped: 0 (0.0%) Profile: Default

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.



Page 4 of 4