Tufts University
Department of Computer Science
COMP 116: Introduction to Computer Security
Spring 2020
Practice Quiz 1. Closed Book.

Quiz 1 will cover the following topics:

- Networking
- Packet analysis
- Network scanning
- Network sniffing
- Distributed Denial of Service (DDoS) attacks
- Encoding

Types of questions on the quiz will include drawing, multiple choice, fill-in-the-blank, true or false, really short answer. No essays.

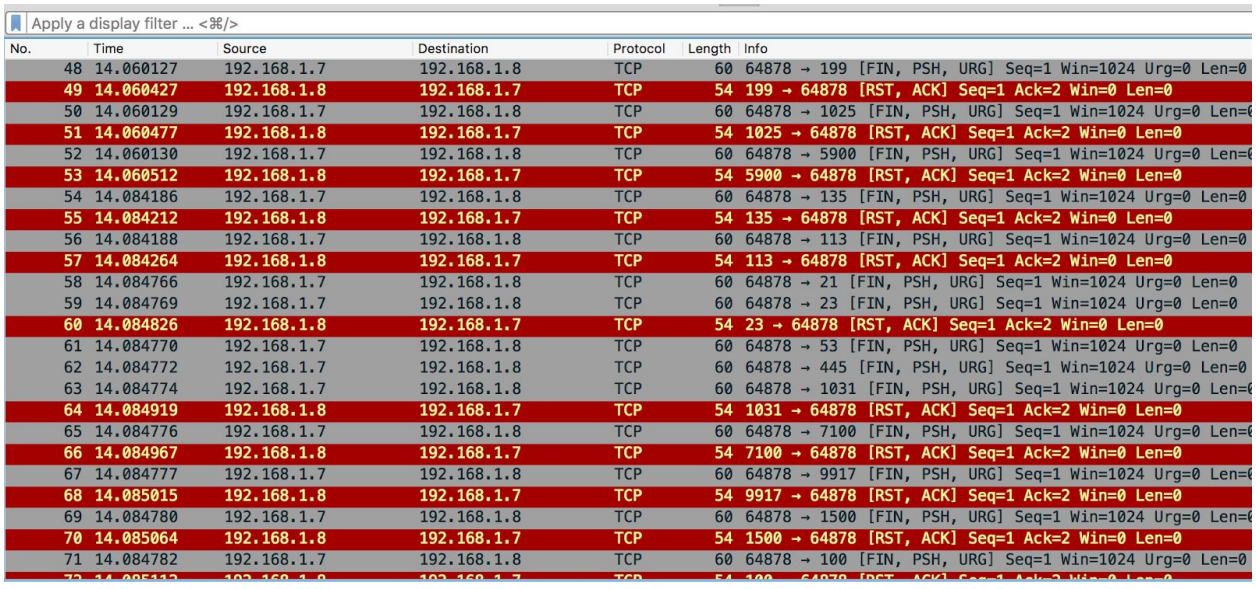
Sample Questions:

1 (5 points). We discussed various methods of scanning a network. Detail at least three port scanning techniques

2 (3 points). In order to sniff a network, the user needs to be _____.

3 (2 points). How can you defend your system against scanners?

4 (3 points). Consider the following snapshot of the packets from Wireshark. Identify the incident.


Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
48	14.060127	192.168.1.7	192.168.1.8	TCP	60	64878 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
49	14.060427	192.168.1.8	192.168.1.7	TCP	54	199 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
50	14.060129	192.168.1.7	192.168.1.8	TCP	60	64878 → 1025 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
51	14.060477	192.168.1.8	192.168.1.7	TCP	54	1025 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
52	14.060130	192.168.1.7	192.168.1.8	TCP	60	64878 → 5900 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
53	14.060512	192.168.1.8	192.168.1.7	TCP	54	5900 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
54	14.084186	192.168.1.7	192.168.1.8	TCP	60	64878 → 135 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
55	14.084212	192.168.1.8	192.168.1.7	TCP	54	135 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
56	14.084188	192.168.1.7	192.168.1.8	TCP	60	64878 → 113 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
57	14.084264	192.168.1.8	192.168.1.7	TCP	54	113 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
58	14.084766	192.168.1.7	192.168.1.8	TCP	60	64878 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
59	14.084769	192.168.1.7	192.168.1.8	TCP	60	64878 → 23 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
60	14.084826	192.168.1.8	192.168.1.7	TCP	54	23 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
61	14.084770	192.168.1.7	192.168.1.8	TCP	60	64878 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
62	14.084772	192.168.1.7	192.168.1.8	TCP	60	64878 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
63	14.084774	192.168.1.7	192.168.1.8	TCP	60	64878 → 1031 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
64	14.084919	192.168.1.8	192.168.1.7	TCP	54	1031 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
65	14.084776	192.168.1.7	192.168.1.8	TCP	60	64878 → 7100 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
66	14.084967	192.168.1.8	192.168.1.7	TCP	54	7100 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
67	14.084777	192.168.1.7	192.168.1.8	TCP	60	64878 → 9917 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
68	14.085015	192.168.1.8	192.168.1.7	TCP	54	9917 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
69	14.084780	192.168.1.7	192.168.1.8	TCP	60	64878 → 1500 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
70	14.085064	192.168.1.8	192.168.1.7	TCP	54	1500 → 64878 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
71	14.084782	192.168.1.7	192.168.1.8	TCP	60	64878 → 100 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

5 (3 points) Using pictures and few words, *illustrate* a DDoS attack. Do not write sentences or paragraphs.

6 (3 points) Using pictures and few words, *illustrate* how the OSI model works. Do not write sentences or paragraphs.

Selected Answers to Sample Questions:

1. TCP SYN, XMAS, NULL, FIN, vanilla (using Netcat, attempt to connect to all 65,536 ports one at a time)

2. root / superuser / administrator

3. Close unnecessary services

4. XMAS scan