Tufts University
Department of Computer Science
COMP 116: Introduction to Computer Security
Fall 2016
Practice Quiz 1. Closed Book.

Quiz 1 will cover the following topics:

- Basic “thinking like an attacker” / social engineering
- Networking
- Packet analysis
- Network scanning
- Network sniffing

Types of questions on the quiz will include:

- Multiple choice
- Fill-in-the-blank
- True or false
- Really short answer

Sample Questions:

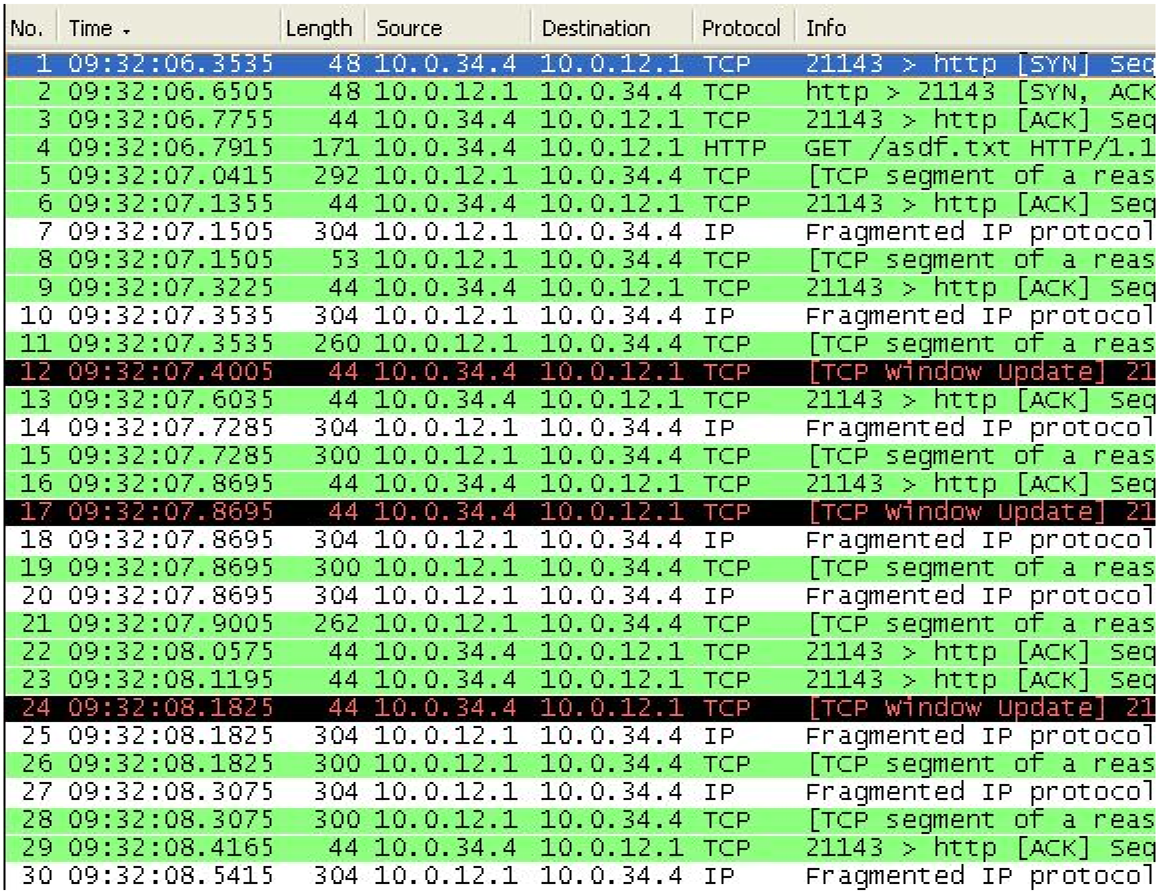
1 (2 points). __________ relies on IP but does not guarantee delivery or use handshaking.

2 (5 points). We discussed various methods of scanning a network. Detail three ways to scan a network for open ports.

3 (3 points). In order to sniff a network, the user need to be __________.

4 (2 points). How can you defend your system against scanners?

5 (5 points). Consider the following illustration. Identify what is happening and how can you conduct the similar activity.



No.	Time	Length	Source	Destination	Protocol	Info
1	09:32:06.3535	48	10.0.34.4	10.0.12.1	TCP	21143 > http [SYN] Seq
2	09:32:06.6505	48	10.0.12.1	10.0.34.4	TCP	http > 21143 [SYN, ACK
3	09:32:06.7755	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
4	09:32:06.7915	171	10.0.34.4	10.0.12.1	HTTP	GET /asdf.txt HTTP/1.1
5	09:32:07.0415	292	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
6	09:32:07.1355	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
7	09:32:07.1505	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
8	09:32:07.1505	53	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
9	09:32:07.3225	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
10	09:32:07.3535	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
11	09:32:07.3535	260	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
12	09:32:07.4005	44	10.0.34.4	10.0.12.1	TCP	[TCP Window Update] 21
13	09:32:07.6035	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
14	09:32:07.7285	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
15	09:32:07.7285	300	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
16	09:32:07.8695	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
17	09:32:07.8695	44	10.0.34.4	10.0.12.1	TCP	[TCP Window Update] 21
18	09:32:07.8695	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
19	09:32:07.8695	300	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
20	09:32:07.8695	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
21	09:32:07.9005	262	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
22	09:32:08.0575	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
23	09:32:08.1195	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
24	09:32:08.1825	44	10.0.34.4	10.0.12.1	TCP	[TCP Window Update] 21
25	09:32:08.1825	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
26	09:32:08.1825	300	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
27	09:32:08.3075	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol
28	09:32:08.3075	300	10.0.12.1	10.0.34.4	TCP	[TCP segment of a reas
29	09:32:08.4165	44	10.0.34.4	10.0.12.1	TCP	21143 > http [ACK] Seq
30	09:32:08.5415	304	10.0.12.1	10.0.34.4	IP	Fragmented IP protocol

Answers to Sample Questions:

1. UDP

2. Ping sweep, Nmap SYN scan, Nmap Xmas scan

3. root / superuser

4. Close unnecessary services

5. Packet fragmentation. You can use nmap, fragroute, or hping to perform this.