

Hand in a stapled, printed copy with your answers.

**Homework: /SI110/Cyber Operations/Cyber Attack-Reconnaissance**

1. What are the *three phases* of a cyber attack?

2. Recall our definition of a cyber attack as an action that violates one of the five *pillars of Information Assurance*.

Scenario 1: An employee at Company X is looking at shared documents on the company's fileserver and notices some discrepancies that indicate that one of the executives is embezzling money. He uses this information to blackmail the executive.

Scenario 2: An employee at Company X breaks into an executive's computer account and finds a file there which indicates that the executive is embezzling money. He uses this information to blackmail the executive.

Why is Scenario 2 a *cyber attack*, but Scenario 1 is not?

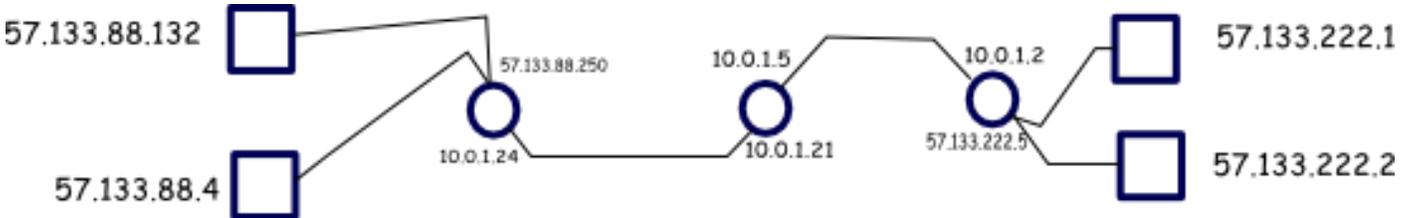
3. Label each of the following activities as either **Active Recon** or **Passive Recon**.

a. Pulling up your target's website and checking out a few links.

b. Trying to make a TCP connection to the host that runs your target's webserver at each of the 500 most commonly used ports to see what other services the host is running.

c. Doing web searches on employees of the company your targeting to find out personal information about them in blogs, social media sites, news stories, etc.

4. We've been acting as if routers have one IP address but, by definition, a router has more than one IP address: one for each of its ports. So, we have pictures that look like this:



Traceroute shows you incoming IP address for each router on the path. So if 57.133.88.132 gives the command **traceroute 57.133.222.2**, the path shown is: 57.133.88.250 -> 10.0.1.21 -> 10.0.1.2 -> 57.133.222.2.

What path would be shown if host 57.133.222.2 gave the command: **traceroute 57.133.88.132**?

Hand in a stapled, printed copy with your answers.

5. Suppose my IP Address is 57.133.88.132, and as part of my cyber recon I give three trace route (*tracert* on Windows, *traceroute* on UNIX) commands shown below:

```
tracert 57.133.88.4      tracert 57.133.222.1      tracert 57.133.222.2
1 57.133.88.4           1 57.133.88.250          1 57.133.88.250
                        2 10.0.1.21              2 10.0.1.21
                        3 10.0.1.2              3 10.0.1.2
                        4 57.133.222.1          4 57.133.222.2
```

a. What's my gateway router?

b. Which of the following diagrams shows the correct *network topology* (i.e. how the hosts are connected)? Note in these diagrams routers are depicted as circles, regular hosts as squares.

Diagram 1:

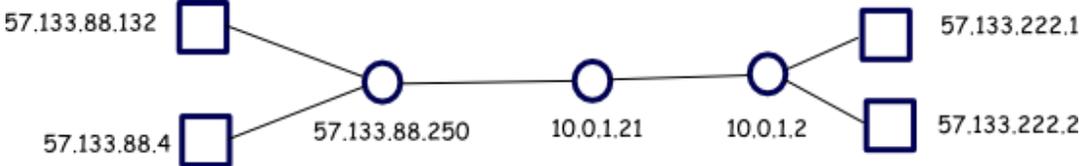


Diagram 2:

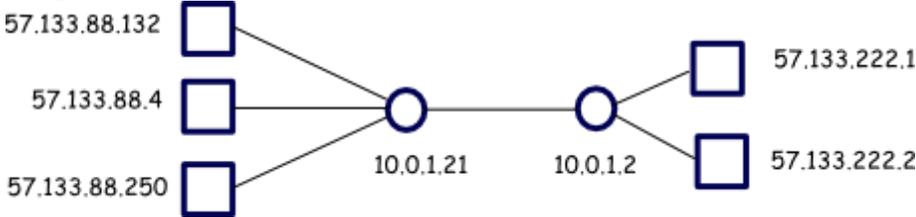


Diagram 3:



Diagram 4:

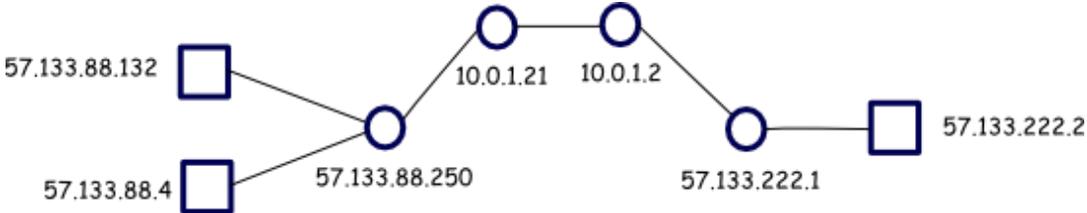


Diagram:

c. Explain your answer to 4.b.: