Do not begin until asked to do so

Name:

Poly ID:

Instructions:

- Be sure to read the questions carefully and answer all parts
- Less verbose answers are better

1. ACME Corporation has a shopping website that makes a profit of $1000 per day. It's vulnerable to a particular DDOS attack that can bring the entire web server down for five days in a single incident. The engineers calculated each DDOS incident will cost the company $200 per day in security consulting fees along with the lost profit. The engineers also calculate that the chance of a DDOS attack is once in two years.

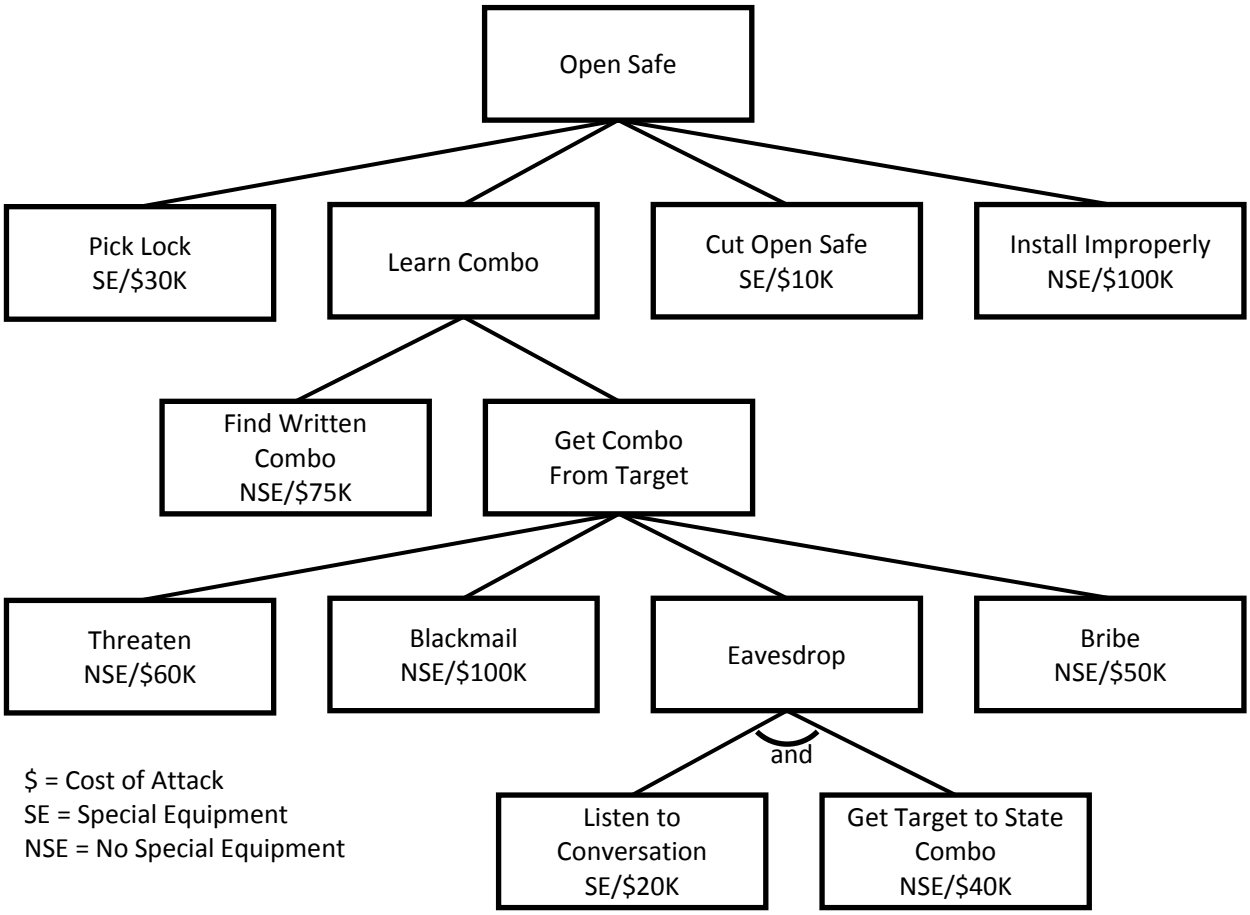
1a. [3pts] What's the Single Loss Expectancy (SLE)?

1b. [2 pts] What's the Annualized Rate of Occurrence (ARO)?

1c. [2 pts] What's the Annualized Loss Expectancy (ALE)?

1d. [3 pts] Would a firewall that can prevent this particular DDOS attack that cost $10k to purchase with an annual licensing cost of $1000 per year be worth it? Explain.

2. Attack Trees



$ = Cost of Attack
SE = Special Equipment
NSE = No Special Equipment

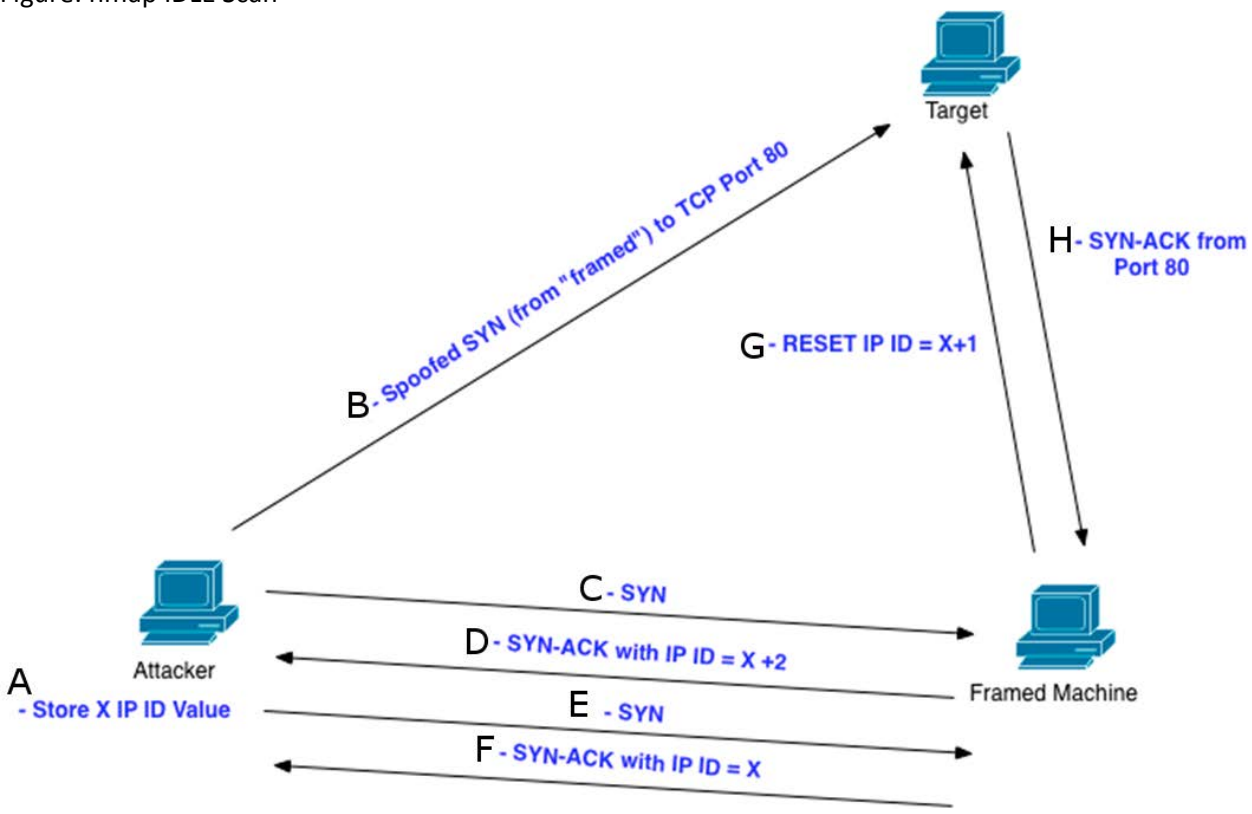
2a. [3pts] What's the cheapest attack (name and amount) that requires no special equipment?

2b. [4pts] What's the cheapest and most expensive methods and amounts to **Get Combo From Target**?

2c. [3pts] What's the most expensive attack (name and amount) that requires special equipment?

3. [10 pts] Suppose Trudy wants to transfer a file from her computer to Bob's computer. Bob's computer is behind a home firewall which only allows outgoing connections to port 80. Trudy's IP is 22.22.22.22 and Bob's IP is 10.0.0.10. What netcat command would you run on Bob and Trudy's machine in order to transfer a file named rootkit.exe from the Trudy to Bob?

Figure: nmap IDLE Scan



4. [8 pts] In the above illustration, place A-H in the correct sequence order.

5. Network Time Protocol (NTP) is a common protocol used to sync the time between client and server. Windows PCs are set by default to sync the clock from a Microsoft NTP server. NTP operates on UDP port 123. In normal usage, a client sends a request (packet size about 48bytes) to an NTP server for the time, and then the client listens for a response from the server. NTP also has a feature called "monlist" in which a client can request (packet size about 48bytes) a list that contains the last 600 hostnames with IP addresses of clients that have connected to that server. The NTP request also contains a 32-bit Reference ID that the server response must contain for the client to accept the response.

5a. [6 pts] Describe in detail three ways an attacker can abuse this protocol. Describe how difficult it would be to perform the attack.

5b. [4 pts] Describe in detail methods to stop an attacker from abusing this protocol.

6. Perform RSA key generation with *p=5* and *q=13*.
6a. [2 pts] Compute *n* and *φ*
6b. [2pts] Choose the **smallest possible** public (encryption) exponent *e*
6c. [4 pts] Choose a private (decryption) exponent *d*
6d. [4 pts] Encrypt the plaintext message *m=5* with the public key
6e: [2 pts] Are the values of the exponent *e* and exponent *d* a good choice? Why or why not?

7. Perform Diffie-Hellman shared key generation with *g=5*, *n=19*, Alice selects *a=5* as her secret, Bob selects *b=6* as his secret.
7a. [3pts] calculate Alice's public key *A*
7b. [2pts] calculate Bob's public key *B*
7c. [4pts] calculate the shared key *K*
7d. [3pts] Based on the size of *a*, *b*, *g*, and *n*, would this key exchange be difficult to break if Trudy intercepted the publically exchanged values? Why or why not?

8. Cipher Block Chaining (CBC)

Input	**Output**	**Input**	**Output**
0000	1111	1000	0111
0001	1110	1001	0110
0010	1101	1010	0101
0011	1100	1011	0100
0100	1011	1100	0011
0101	1010	1101	0010
0110	1001	1110	0001
0111	1000	1111	0000

8a. [3 pts] If Trudy intercepted Ciphertext 001110110011 from Alice to Bob and she knows that Cipher Block Chaining (CBC) is not used, what can she figure out about the message?
8b. [3 pts] Decrypt 001110110011 without CBC
8c. [6 pts] Decrypt 001110110011 using CBC and IV=1010

9. Miscellaneous
9a. [2 pts] Encrypt "HELLO WORLD" with Julius Ceasar's Cipher of key 5 (positive 5).
9b. [4 pts] Define what a chosen-plaintext attacks is.
9c. [4 pts] What attack does SYN Cookies mitigate? How does it do that?
9d. [4 pts] What are four things that need to be configured in HackerDefender for it to be hidden from the user?

This page is blank.