Name: _________________________

Score: ______ / ______

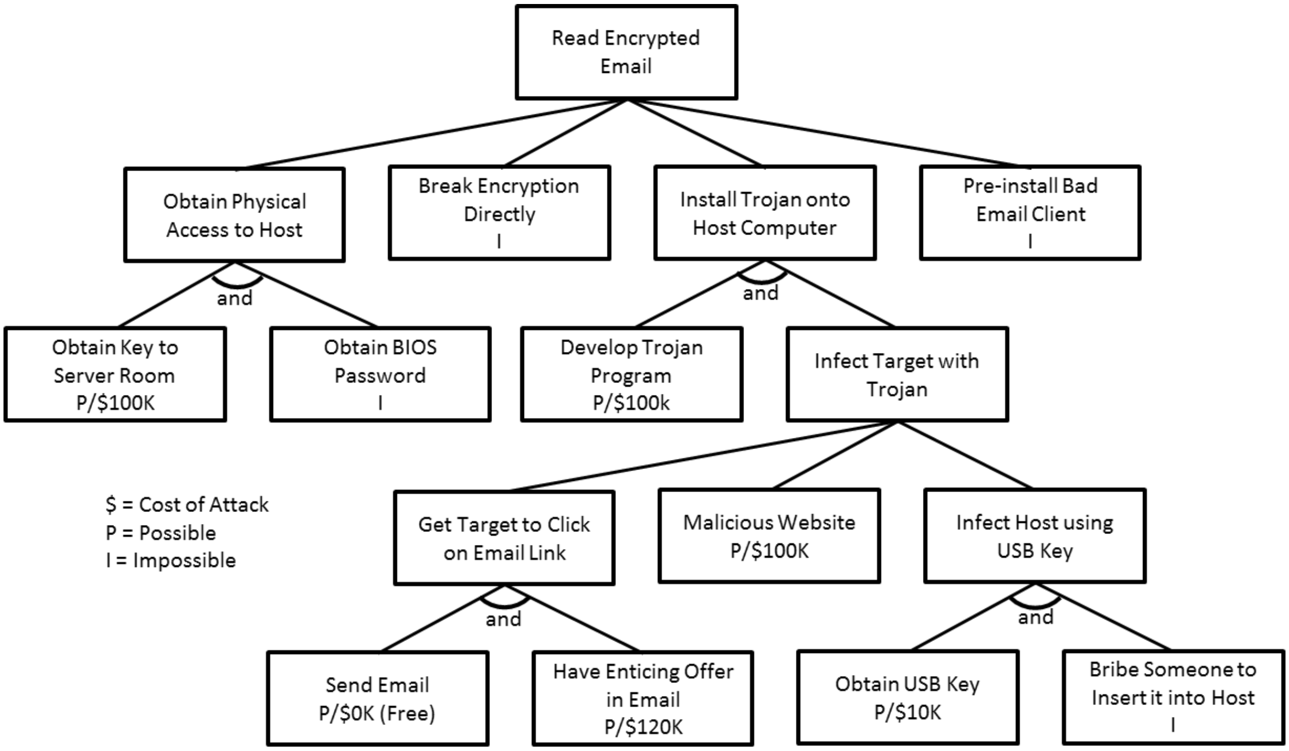
# Midterm

## username: user
## password:

Closed book/notes, no calculator, scratch paper allowed.
Read each question carefully and answer all parts of the question.
If you do not understand a question or are confused, do the best you can.
If you have the correct solution and also the incorrect solution in your answer, you will lose points.
Remember that you are being monitored by the proctor.

## 1

1. Attack Trees



Read Encrypted Email
Obtain Physical Access to Host
Break Encryption Directly I
Install Trojan onto Host Computer
Pre-install Bad Email Client I
and
and
Obtain Key to Server Room P/$100K
Obtain BIOS Password I
Develop Trojan Program P/$100k
Infect Target with Trojan
$ = Cost of Attack
P = Possible
I = Impossible
Get Target to Click on Email Link
Malicious Website P/$100K
Infect Host using USB Key
and
and
Send Email P/$0K (Free)
Have Enticing Offer in Email P/$120K
Obtain USB Key P/$10K
Bribe Someone to Insert it into Host I

1a. [3 pts] What's the cheapest attack (name and amount) that's Possible?

1b. [4 pts] What's the cheapest and most expensive methods (name and amount) that's Possible to **Infect Target with Trojan**?

1c. [3 pts] Suppose it's Possible to "Obtain BIOS Password", and the Cost of Attack for it is $50K.

Now, what is the cheapest attack (name and amount) that's Possible now?

2

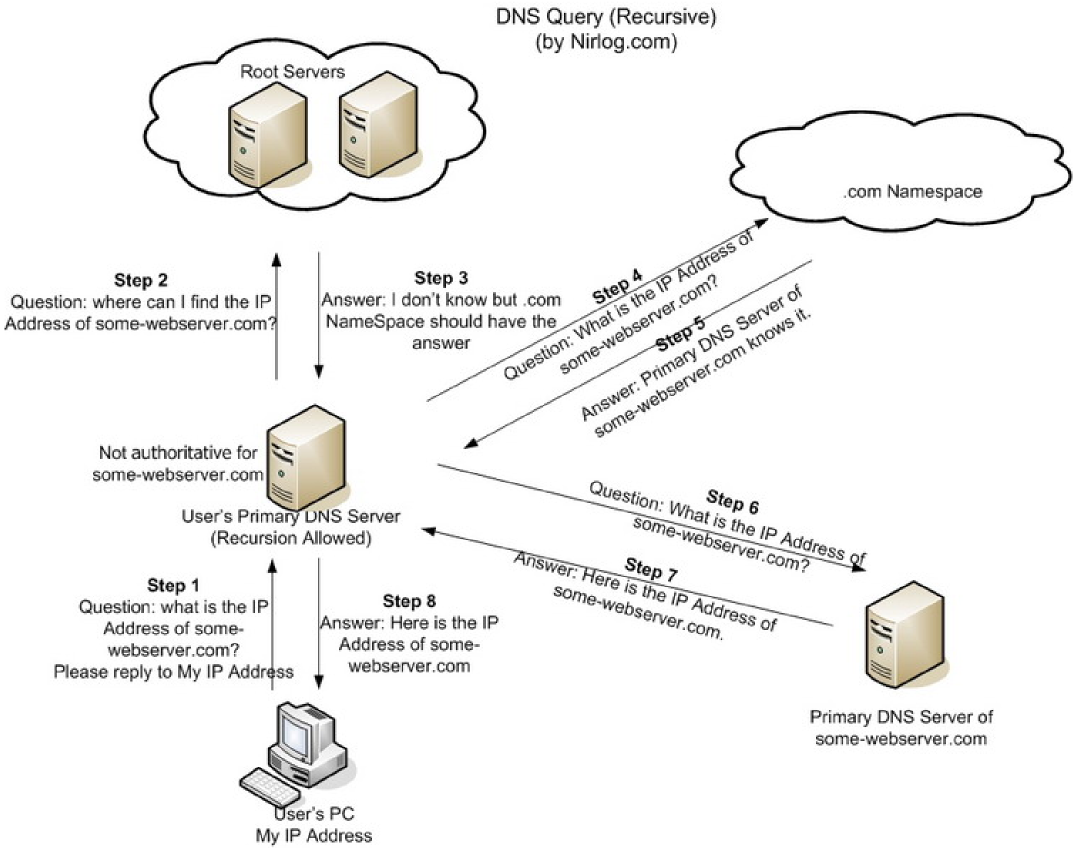
2. **DNS Reconnaissance:** Suppose an attacker is performing reconnaissance on ACME Corporation using only the DNS protocol.

2a. [6pts] What are three methods using only the DNS protocol that an attacker can use to perform reconnaissance on ACME Corporation? Identify what type of information can be obtained.

2b. [4pts] What are two mitigation strategies to minimize what an attacker can obtain from using DNS?

3

3. **DNS Exploits:** Remember that DNS queries are usually recursive, as shown in this diagram:


DNS Query (Recursive)
(by Nirlog.com)
Root Servers
.com Namespace
Step 2
Question: where can I find the IP Address of some-webserver.com?
Step 3
Answer: I don't know but .com NameSpace should have the answer
Step 4
Question: What is the IP Address of some-webserver.com?
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.
Not authoritative for some-webserver.com
User's Primary DNS Server
(Recursion Allowed)
Step 6
Question: What is the IP Address of some-webserver.com?
Step 7
Answer: Here is the IP Address of some-webserver.com.
Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address
Step 8
Answer: Here is the IP Address of some-webserver.com
Primary DNS Server of some-webserver.com
User's PC
My IP Address

Suppose an attacker wants to perform DNS cache poisoning so the domain name acmecorporation.com is diverted it to a malicious website.

3a. [3 pts] Identify the step number(s) in the diagram in which the attacker can insert traffic to poison the DNS cache. Explain your answer.

3b. [6 pts] What are three issues that the attacker needs to overcome in order to successfully poison the DNS cache?

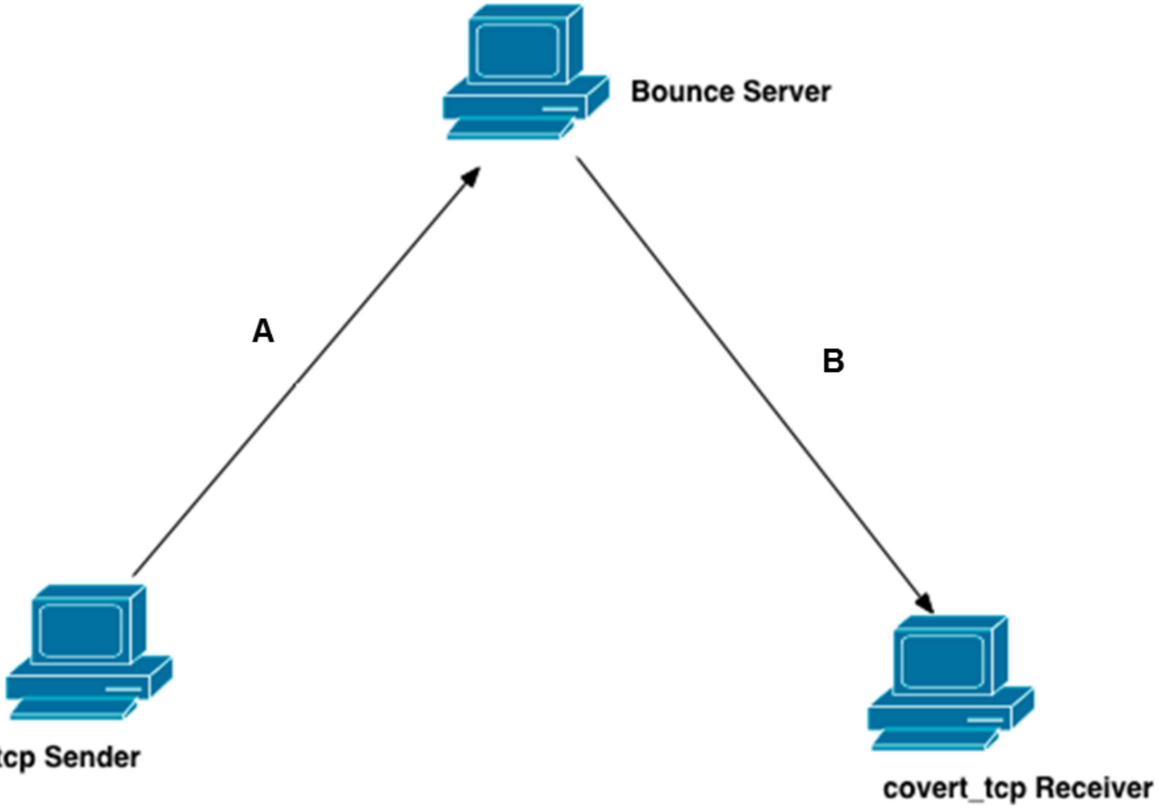
3c. [3 pts] Explain the main difficulty with using ingress filtering to prevent IP spoofing. Ingress filtering is only allowing subnets at the router that are supposed to be connected to the router.

4

4. [6 pts] Using the standard nmap TCP SYN scan, how does nmap decide if a port is open, closed, or filtered?

5

5. [10 pts] This diagram represents the covert_tcp (TCP ACK Method) of transferring data from one host to another.



Describe the method by which the “covert_tcp Sender” can send a message to “covert_tcp Receiver” using the Bounce Server. Include necessary details on the IP or TCP headers in order to explain your answer.

5a. [4 pts] Details of communications for label A.

5b. [6pts] Details of communications for label B.

6

6. Suppose an attacker has installed HackerDefender on a target machine and has hidden itself and netcat on the host. Netcat on the host is configured to listen on port 1234 and upon an incoming connection will send the file password.txt, and then exit.

6a. [4 pts] Write the netcat command for the attacker to run in order to retrieve the file and save the file to the current directory.

6b. [4 pts] With the netcat process and port hidden on the target machine, can the port that netcat is using be found using a network scanning tool (such as nmap) from another host on the network? Explain.

7

7. Vignere

7a. [4] Using the standard Vignere (Vigenere) (Poly-alphabetic Encryption) table, decrypt the message HEFF using the key CAB.

7b. [2] Does the table in Vignere need to be kept secret for this cryptographic scheme to work?

8

8. Perform RSA key generation with *p=3* and *q=11*. Note: you must show work for any modular mathematics.

8a. [2 pts] Compute *n* and *φ*

8b. [2 pts] Choose the **smallest possible** public (encryption) exponent *e*

8c. [4 pts] Choose a private (decryption) exponent *d*

8d. [4 pts] Encrypt the plaintext message *m=6* with the public key

8e: [2 pts] Is RSA the preferred or non-preferred choice for encrypting large messages?  Explain why.

9

9. Perform Diffie-Hellman shared key generation with *g=2*, *n=11*, Alice selects *a=9* as her secret, Bob selects *b=4* as his secret. Note: you must show work for any modular mathematics.

9a. [3 pts] Calculate Alice's public key *A*

9b. [2 pts] Calculate Bob's public key *B*

9c. [4 pts] Calculate the shared key *K*

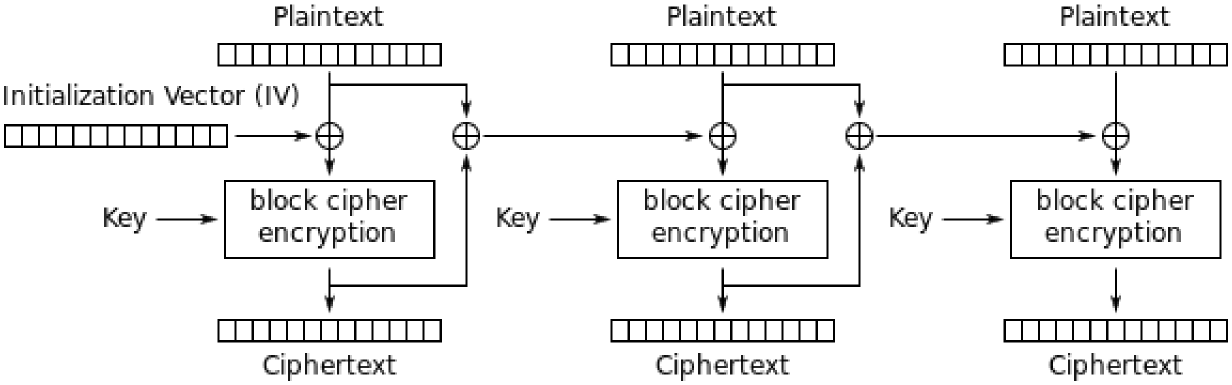
9d. [3 pts] What values are publically shared between Alice and Bob?

10

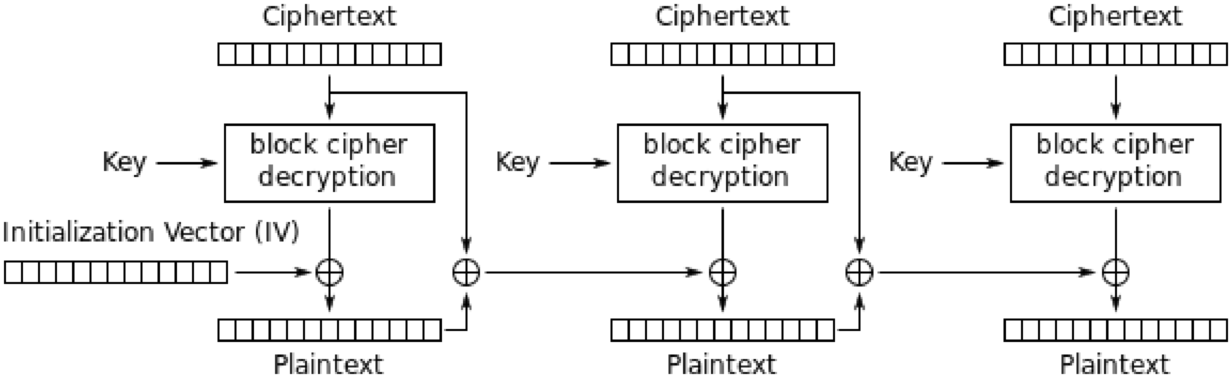
10. Block Cipher Mode of Operations

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

The following diagram shows Propagating cipher-block chaining (PCBC), a similar mode of operation to CBC.



Propagating Cipher Block Chaining (PCBC) mode encryption



Propagating Cipher Block Chaining (PCBC) mode decryption

10a. [3 pts] If Trudy intercepted Ciphertext 001110110011 from Alice to Bob and knows that CBC is used, can she easily figure out that blocks are repeating?

10b. [3 pts] Decrypt Ciphertext 001110110011 without using any mode

10c. [6 pts] Decrypt Ciphertext 001110110011 using PCBC and IV=1010