Name: _________________________

Score: ______ / ______

Midterm

username: user
password: <entered by Proctor>

Closed book/notes, no calculator, scratch paper allowed, word processor allowed.

You may upload a word document with the solutions rather than filling out the answer boxes.

You must successfully upload your document before the time is up.

Word processor (e.g., Microsoft Word) allowed for scratch.

Read each question carefully and answer all parts of the question.

Each answer must be explained. A correct answer without explanation on how the conclusion was obtained will receive no credit.

If you do not understand a question or are confused, do the best you can.

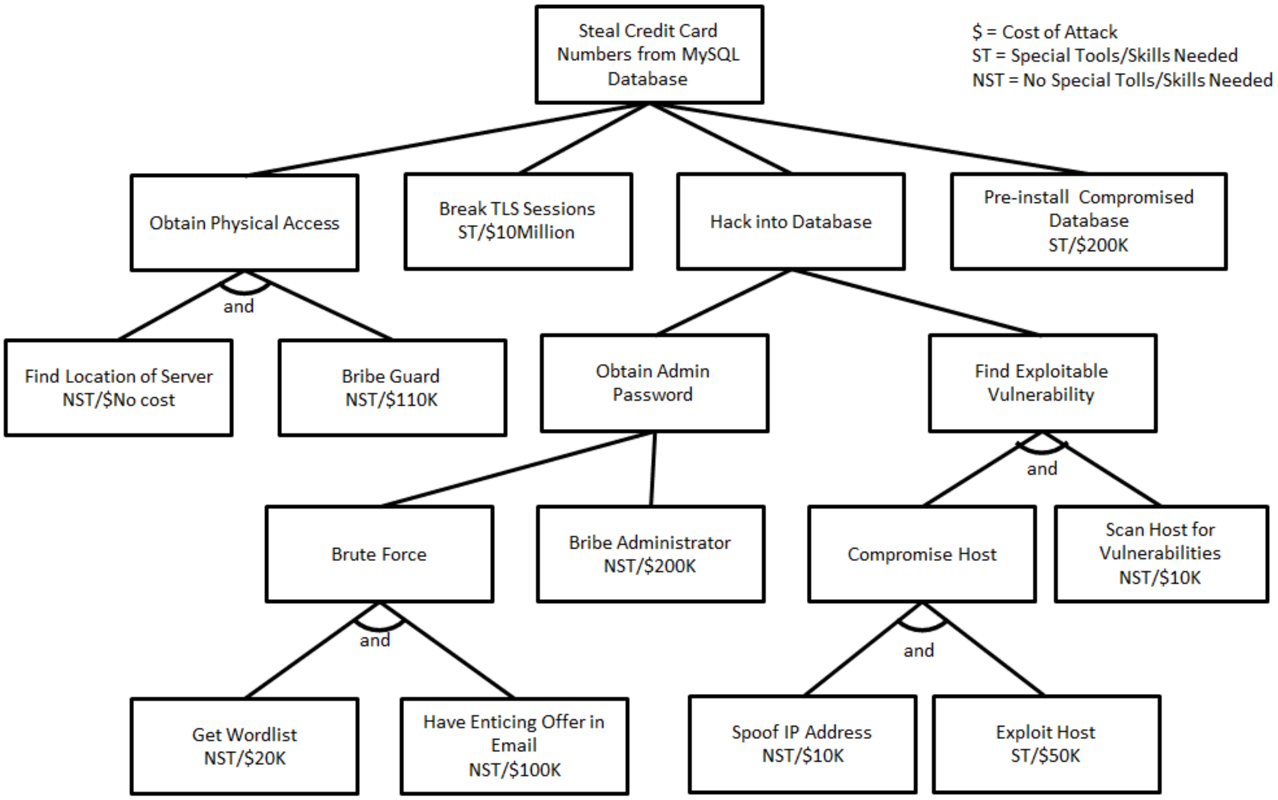
If you have the correct solution and also the incorrect solution in your answer, you will lose points.

Remember that you are being monitored by the proctor.

Part 1

1

1. Attack Trees


Steal Credit Card Numbers from MySQL Database
$ = Cost of Attack
ST = Special Tools/Skills Needed
NST = No Special Tolls/Skills Needed
Obtain Physical Access
Break TLS Sessions ST/$10Million
Hack into Database
Pre-install Compromised Database ST/$200K
and
Find Location of Server NST/$No cost
Bribe Guard NST/$110K
Obtain Admin Password
Find Exploitable Vulnerability
and
Brute Force
Bribe Administrator NST/$200K
Compromise Host
Scan Host for Vulnerabilities NST/$10K
and
and
Get Wordlist NST/$20K
Have Enticing Offer in Email NST/$100K
Spoof IP Address NST/$10K
Exploit Host ST/$50K

The above image shows an attack tree.

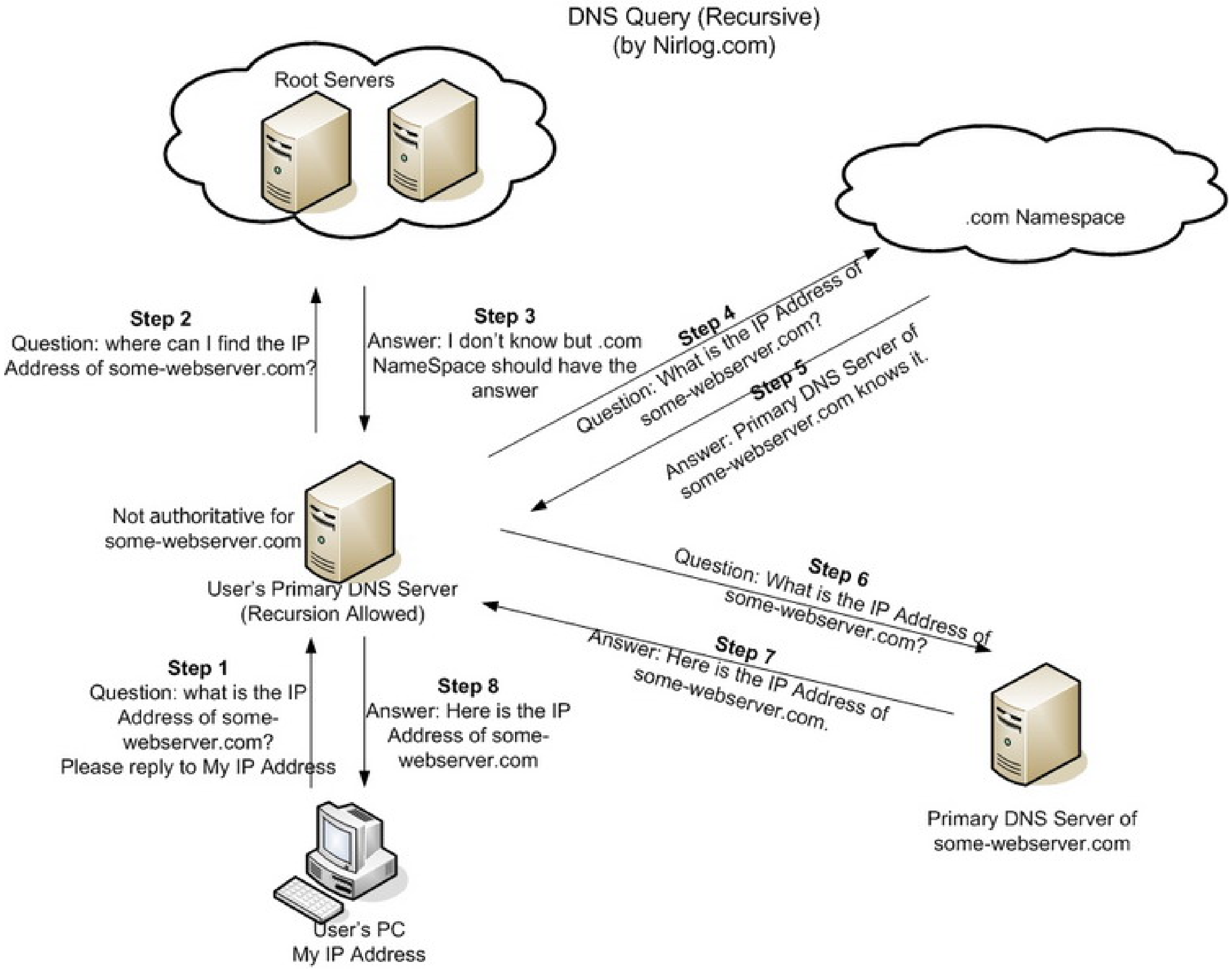
1a. [3 pts] What's the cheapest attack (name and amount) that requires no special tools or skills?

1b. [3 pts] What's the cheapest and most expensive methods (name and amount) to Hack into Database?

1c. [4 pts] Suppose "Find Location of Server" now requires $50k rather than "no cost." Does this change any of the other two answers? If so, how.

2

2. **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

The above image shows a diagram of the recursive DNS process.

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

2a. [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.

2b. [6 pts] What are three issues that the attacker needs to overcome in order to successfully poison the DNS cache?

2c. [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.

3

3. **Exploits**: In the nmap scan option called FTP bounce scan:

3a. [4 pts] What vulnerability in FTP is being used by nmap for port scanning?

3b. [6 pts] Explain how this feature works and describe the possible outcomes.

4

4. **Covert Channels**: Suppose two hosts are communicating to each other using only pings. They have a covert channel set up by piggybacking on the ping echo requests and replies between the two hosts. There is no other communications between the two hosts.

4a. [6 pts] Describe three ways that a covert channel can be established using only fields in the ping header.

4b. [4 pts] Describe two ways that this can be detected and stopped.

5

5. Perform RSA key generation with p=5 and q=11. Note: you must show work for any modular mathematics.

5a. [2 pts] Compute n and φ

5b. [2 pts] Choose the smallest possible public (encryption) exponent e

5c. [3 pts] Choose a private (decryption) exponent d

5d. [2 pts] Encrypt the plaintext message m=25 with the public key

5e. [3 pts] Decrypt your solution in part d to obtain the original message m=25

5f: [2 pts] What mathematical property provides the security of RSA encryption?

6

6. Perform Diffie-Hellman shared key generation with g=6, n=17, Alice selects a=5 as her secret, Bob selects b=11 as his secret. Note: you must show work for any modular mathematics.

6a. [3 pts] calculate Alice's public key A

6b. [2 pts] calculate Bob's public key B

6c. [4 pts] calculate the shared key K

6d. [3 pts] In the Diffie-Hellman exchange, what values can Trudy see, and what values she cannot?

7

7. Block Cipher Mode of Operations: Suppose you have an encryption function as follows, with block size of five bits:

$$\textit{Encryption: } c(m) = m \oplus 11000$$

$$\textit{Decryption: } m(c) = c \oplus 11000$$

For example, for plaintext message *m*=10101, the ciphertext *c* would be 01101.

7a. [3 pts] Does the IV in Cipher Block Chaining (CBC) need to be kept a secret? Explain why or why not.

7b. [3 pts] Decrypt Ciphertext 000110001100011 without using any mode

7c. [6 pts] Decrypt Ciphertext 000110001100011 using CBC and IV=10110

8

8. Scapy: Explain what the following scapy command do:
8a. [4 pts] send(IP(dst="10.10.111.1",ttl=10)/ICMP())
8b. [4 pts] sr(IP(dst="10.10.111.0/24")/TCP(dport=(80,81)))

See attached file below for a reference on scapy.

Attachments
scapy.pdf

9

9. Miscellaneous
9a. [4 pts] What is Split DNS and what attack is and what it's intended to mitigate?
9b. [4 pts] Describe the main reason that an attacker might want install a Reverse WWW Shell onto a target's computer.
9c. [4 pts] Using the standard Vigenere (Poly-alphabetic Encryption) table, decrypt the message LLMN using the key CDB. Show work or explain.

10

If you wish, you may upload your answers in a document and upload that rather than typing out your answers in the boxes provided.

> I will grade the contents of the file and ignore any other text you put in the submission boxes;
> If you submit more than one file or exam, I will only look at the final submission;
> It is your responsibility to ensure that the file has been correctly uploaded. Note that the exam will auto submit after three hours. The onus is on you to ensure that this is done correctly and on-time. No submission from outside the exam site will be accepted.

Click "Browse" to locate your file and then click "Upload" to upload your file.

File: □ Browse: Upload: