CS479 – QUIZ

Date:

(30 pts.)
Name Surname:

Student ID:

1) (10 pts)

   State and explain the basic security concepts.

   a) C

   b) I

   c) A

2) (10 pts)
   Give an example of two factor authentication.

3) (10 pts)
   ..... is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site.

   a) Explain the difference between this attack and pharming?

4) (10 pts)
What does DoS and DDoS stand for?

a) State the security concept these attacks are targeting?

5) (5 pts)
..... is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). This attack must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. This attack is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

6) (5 pts)
In computing, a ..... is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. This system typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

7) (15 pts)
You obtained a network packet dump file namely “net1.pcap” and you will analyze it with tcpdump.

a) Write down the tcpdump filter for listing entries including IP address 192.168.10.10

b) Write down the tcpdump filter for listing entries including IP address 192.168.10.10 and protocol ICMP

c) Write down the tcpdump filter for listing entries including IP address 192.168.10.10 and protocol ICMP and writing the output to a new pcap file namely “net1_filtered.pcap”

8) (15 pts)
Answer the questions below for the network 192.168.10.0/24

a) What is the first usable address in this network?

b) What is the last usable address in this network?

c) What is the broadcast address?

9) (10 pts)
State the commonly used port numbers for the following protocols.

a) HTTP

b) HTTPS

c) DNS

d) SSH

10) (15 pts)
State and describe an attack targeting the DHCP server.

11) (10 pts)
In asymmetric encryption you have a pair of keys.
a) State the names of these keys.

b) Describe the communication methodology using these keys i.e. which is used to encrypt, which to decrypt, which one you will announce.

12) (5 pts)
State the name of an hash algorithm.