Number:		Name:	

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC, MEIC

1st Test Recovery, January 27th, 2020

- The duration of the test is of 1:00 hours.
- **Identify all sheets.**
- Read all paragraphs of each question before you answer the first one.
- Be objective and concise in your answers. Use only the space given for each question.
- The exam can be answered in Portuguese or in English.
- Wrong answers in multiple choice questions with N options, count -1/(N-1) of the value.
- **Justify all answers.**

1. A **ransomware** attack encrypts all data files in each computer in a network with a key generated by the attacker. In exchange for the key, that may allow for the recovery of the files, the attacker requests a ransom, for example, a Bitcoin payment.

   a. Which of the CIA properties are affected by the described ransomware attack?

   b. *"For a well-managed infrastructure, ransomware is a low probability but high impact attack"*. Do you agree? Prescribe a risk mitigation strategy.

Yes / No

2. Consider an **Ethernet local area network** with three machines: **A**lice, **B**ob and **E**ve. Each machine can connect to the Internet through Rachel, a router connected to an ISP network wide area network. Rachel performs NAT.

   a. What is NAT? Can it be considered a security mechanism?

   b. What is a passive network attack?
   In this scenario, who is in a position to perform such an attack?

3. *"A TCP connection, once established, can no longer be hijacked".*
   Do you agree with the statement? Detail your answer

4. vBulletin is a proprietary Internet forum software package. It is written in PHP and uses a MySQL database server. In the login page of the vBulletin server code, the following is being done:
   ("in_id" and "in_pwd" are user input variables)

```
$conn = getDBConnection();
$sql = "SELECT id, name, nickname, password FROM credential
WHERE id= '$in_id' and password='$in_pwd'";
$result = $conn->query($sql));
```

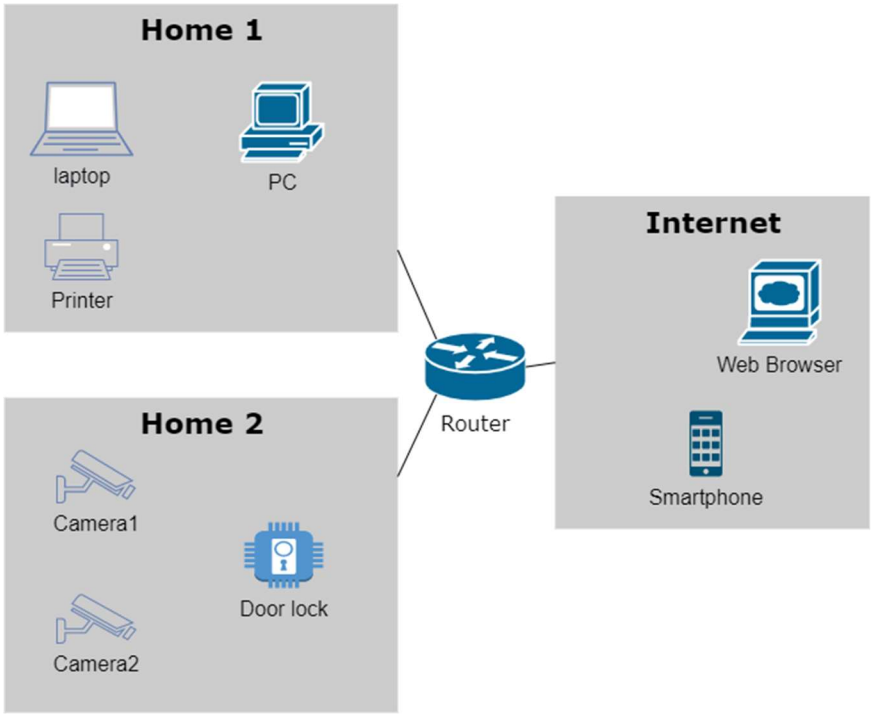
   Is this code susceptible to **SQL injection attacks**?
   In case it is vulnerable: explain how you would perform the attack;
   in case it is not vulnerable: justify why is it secure.

Yes / No

5. Consider a **smart home** with two computers and a printer connected to the Wireless Local Area Network, but also three Internet of Things devices, namely, two security cameras and one smart lock.

   In order to isolate IoT devices, the network administrator decided to create two separate networks, **home1** and **home2**, one for the computers and printer, and the other for the IoT devices.

   There is router device with three network adapters, one connected to the home1 network, another to the home2, and a third one connected to the Internet. This router has a **stateful packet filter**.



a. Please complete the following firewall table with rules that enforce the policy:
   - Allow the PC and laptop to browse the Internet using DNS, HTTP and HTTPS;
   - Allow the PC to control the lock and cameras from the local network using HTTPS;
   - Allow the cameras to stream video to PC using RTP protocol;
   - Allow the Smartphone to control the lock (it has an app to open and close the door) from anywhere on the Internet using HTTPS;
   - Deny everything else.

Interface	Source IP	Source port	Protocol	Destination IP	Destination port.	State	Action
*	*	*	*	*	*	Established	Accept

* is a wildcard; for readability, you can use the machine names instead of IP addresses.
Ports: HTTP – 80 TCP, HTTPS – 443 TCP, SSH – 22 TCP, DNS – 53 both UDP and TCP, RTP (Real-time Transport Protocol) – audio and video streaming – 16500-65000 UDP.

b. Consider the following policy statement:
"The cameras can only stream to the PC <u>after</u> the PC has issued a control command."

Can the firewall enforce this policy?
If yes: explain how; If no: suggest an alternative to enforce this policy statement.

Yes / No

6. Consider a protocol that is focused on providing **confidentiality** in data communication. The following are details of the current implementation.

Send message:
- Compress data with the ZIP algorithm to reduce the data volume;
- A random 128-bit session key is generated;
- The session key is encrypted with the "X" key;
- The message data is encrypted with the session key.

Receive message:
- Key "Y" is used to recover the session key;
- Message is decrypted with key "Z";
- The data is decompressed.

a. What keys are X, Y, and Z ? Propose **concrete cryptographic algorithms** and **key sizes** for implementing the respective operations.

b. What are the main security concerns to have when generating the session key?

c. *"The cipher with the session key should use CBC mode so that …"*
Complete the sentence and motivate the use of CBC.

d. *Extend* the protocol with a way to **authenticate** the **sender**, assure **integrity** and **freshness**.

Draw a diagram with a legend to specify what is sent from sender to receiver in the extended version of the protocol.

.

Grading:

1:	a) 1,0 b) 1,0	T= 2,0
2:	a) 1,5 b) 1,5	T= 3,0
3:	1,5	T= 1,5
4:	2,0	T= 2,0
5:	a) 3,0 b) 1,5	T= 4,5
6:	a) 1,5 b) 1,5 c) 1,5 d) 2,5	T= 7,0
		= 20,0 points