SECURITY ENGINEERING

Final Exam (May 29th 2017) NIA:

Surname: Name:

FREE RESPONSE QUESTION I

(3.5pt) The University Clinic Rober Interstellar has hired you as a Security Engineer and, among your first tasks, is to design the mechanisms that will regulate the access controls of the different subjects who work in the clinic to the different objects with which they deal. Currently, the clinic has a role-based system (RBAC) with discretionary access control (DAC), where the components each role can access are determined as follows

Role = {Component1, component2 … componentN}

The roles currently defined in the clinic are:

Assistant = {A1, A2} Resident= {R1, R2} Nurses = {F1, F2}

Administration and Services Staff = {PA1, PA2}

And the objects with which they work:

Clinical Histories (CH), Treatment Sheets (TS), Laboratory Tests, Economic Data

The access matrix representing the permitted operations is as follows:

	CH	TS	LT	ED
Assistants	rw	rw	r	r
Residents	r	r	r	r
Nurses	-	r	-	r
Admin. & Servic.	-	-	-	rw

In view of this scenario, answer in a reasoned way and exclusively in the space destined to it, the following questions.

1. What is the difference between habilitation and ACL? Put an example by filling out the following tables

Habilitation				

ACL				

2. Could someone from the administration and services staff read a medical history in some way?

3. What model would avoid the problem described in the previous section? Set up a labeling model which guarantees the confidentiality of the medical records and avoids this problem.

4. What model would you implant if you wanted to ensure the integrity of the Treatment Sheets? State its two main properties.

SECURITY ENGINEERING

Final Exam (May 29th 2017) NIA:

Surname: Name:

FREE RESPONSE QUESTION II

(3.5 pt) We have recently witnessed a massive global attack that has affected more than 100 countries. According to the report published by the CCN-CERT, the infection procedure was as follows:

a. The infection in the computer is produced by another infected machine using the exploit which takes advantage of the bug solved with the bulletin MS17-010 (Note: It is suspected that the first infection could have be caused by an email attachment).

Once the malicious code (MC) is executed, the following actions are performed on the victim's computer:

b. The MC checks the existence of a certain domain on the Internet. If the domain exists and can be accessed using HTTP, the MC execution ends.
c. The MC creates system services.
d. The MC creates copies in certain folders.
e. The MC creates an entry in the Windows registry to ensure its persistence.
f. The MC extracts from an embedded resource a series of files that will be used in the subsequent encryption process.
g. The MC creates numerous threads for different tasks.
h. It also creates a mutex with a specific name. In case this mutex already exists in the system, the harmful encryption code ends its execution.
i. It encrypts all found files that meet an extension pattern on all drives found on the compromised system.
j. Deletes system shadow-copies.
k. The MC proceeds to infect new machines in local network and internet through several ports (137,138, 129 and 445) through the exploit that takes advantage of SMB failure CVE-2017-0145 solved with the bulletin MS17-010 and that have not been patched.
l. The MC stops certain database program processes in order to encrypt their related files
m. Finally, it proceeds to raise a window asking for the payment of a ransom in exchange for the decryption of the data.

In view of this scenario, answer in a reasoned way and exclusively in the space destined to it, the following questions.

1. Could you break down and describe what types of attacks or malicious programs can be identified in the described process?

2. Could you define the characteristics of at least two of the types of the malicious programs that you have identified in question 1?

3. Could you identify what phases can be distinguished in the process described and group steps a. to k. into to these phases?

4. Why do you think that common corporate malware detection tools have had troubles detecting the malware and therefore, general alarm was not raised until the first rescue request screen was displayed to a user?

5. In your opinion, which is the profile the attackers meet? What mitigation measures and types would you recommend to a company that has not yet been infected?