COMSATS University Islamabad (CUI)

Department of Computer Science

Midterm Examination Spring - 2023
BS (SE)– VIII SEMESTER
BS (CYS/ DS)– II-III-IV-V SEMESTER

Course: CSC432-Information Security
Maximum Marks: 25
Dated: 4 -5-2023
Allowed: 90 Minutes

- *All questions are self-explanatory and require no further explanations during exam time.*
- *Make sure that you have signed the attendance sheet before leaving the examination room.*
- *Return the question paper along with the answer sheet.*
- *Attempt all questions.*

CLO-1 **Question 1. Short Question Answers [1.5*6=9 Marks]**

a) Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your e-mail client, Web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system.

b) Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book". Should you be suspicious that a game wants these types of permissions? Discuss threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? Show what types of malware might it be?

c) Assume that you are a major public figure and that a foreign intelligence agency wants your phone. However, they won't have custody of you, i.e., they won't grab the phone while you were trying to enter their country. Is it safe for you to use biometric unlock? Explain.

d) Apply your knowledge to describe the difference among a "phishing" attack, a "whaling" attack and a "tailgating" attack, particularly in terms of who the target may be?

e) Apply your knowledge to explain different levels in a system that a rootkit may use.

f) Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

a). John peeks at Alice's password when she is logging in.

b). John logs into Alice's account using Alice's password without Alice knowing about it.

c). There is a process running in Alice's machine, which is updating a database from a remote machine. John interrupts the process, results in inconsistent databases.

d). John copies a file from Alice's account and then deletes the file from Alice's directory.

CLO-1 **Question 2. [1+1+1 Marks]**

In November 2018, Marriott International announced that cyber thieves had stolen data on approximately 500 million customers. The breach actually occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018. For some of the victims, only name and contact information were compromised. The attackers were able to take some combination of contact info, passport number, Starwood Preferred Guest numbers, travel information, and other personal information. Marriott believes that credit card numbers and expiration dates of more than 100 million customers were stolen, although the company is uncertain whether the attackers were able to decrypt the credit card numbers. The breach was eventually attributed to a Chinese intelligence group seeking to gather data on US citizens, according to a New York Times article. If true, this would be the largest known breach of personal data conducted by a nation-state."

Read the case-study above, and answer the following:

1. Which security breach (es) has occurred?
2. What could possibly go wrong with this type of security attack(s).
3. What are the appropriate measures that can be taken to reduce the risks of such attacks?

CLO – 2 **Question 3. [1+1+1+1 Marks]**

Recall the concept of authentication and complete the following table:

Authentication method	Example	Application area (where it is used)	Advantage	Disadvantage	Vulnerable to which attack
Something you know					
Something you have					
Authentication by Location					
Biometric Authentication					

CLO – 2 **Question 4. [1+1+1 Marks]**

(a) Assume that the user's password is not stored on the client machine, and the client's key KC is computed from the user's password by a known function. Why is Kerberos more convenient, for the human user, than a system in which the TGS is eliminated, and the client makes a Kerberos-style request to the KDC for each server connection?

(b) In Kerberos v4, it is possible for an attacker to request a ticket for C, or simply overhear a request and response for C. Explain how this allows an attacker to do an offline dictionary attack.

(c) Explain the difference between Kerberos and LDAP

CLO – 2 **Question 5. [1 Marks]**