Information Security (Fall 2023 – BCS – 7B)

Make-up Quiz Dated: 08/12/2023

- By submitting this quiz, you agree to allow me not to award any marks after specifying a reason that is limited to this paper.

Q1. Attempt any one Scenario. [From syllabus covered after Midterm # 2. Wt 3.5]

<u>Scenario # 1:</u> Tech Innovations Ltd., a leading technology company, recently faced a severe cybersecurity breach. The attackers gained unauthorized access to the company's servers, compromising sensitive client data, proprietary software codes, and employee personal information. The aftermath of the breach involved a series of malicious activities, including data manipulation, financial fraud, and attempts to disrupt critical infrastructure.

a) Which PECA Sections are applicable in Scenario # 1? and Why? [1]

b) Write a short note telling Tech Innovations Ltd.'s CEO about different risk assessment methods. [1]

c) As a security expert doing risk assessment, describe the network security portion of the security policy. Hint: Write specific to Assignment # 1. [1.5]

<u>Scenario # 2:</u> Rachel works as a data analyst for a tech company. Her primary responsibility is to analyze and interpret large datasets for the company's research projects. One day, Rachel comes across a dataset that contains information about customer preferences, which could be valuable for her personal side project—a mobile app she's developing in her free time. The dataset is not directly related to her current work projects, and it's unlikely that anyone would notice if she makes a copy for her personal use. Rachel believes that extracting the data could significantly benefit her app's user experience and increase its chances of success.

Evaluate Rachel's behavior from the perspective of the ACM and IEEE codes of conduct. Is her action ethical or not? If so, why? If not, which principles are being violated, and what actions could the organization take?

<u>Relevant Sections [1.5]:</u>

<u>Ethical violations [2.0]:</u>

Q2. Answer any **SIX** short questions. Only the first two lines will be checked [Midterm # 1 and #2 Syllabus. Wt 1.5]

i. Explain the difference in the way a symmetric and asymmetric encryption cipher processes plaintext to create ciphertext.

ii. Explain the vulnerability/risk that a public key certificate addresses.

iii. Write the name of the crypto library you used in your assignment # 1. Why DoS attack against Google Cloud Infrastructure cannot be effective?

iv. Why do we need stream ciphers?

v. How hash function and MAC code are different?

vi. A novice programmer created a SQL INSERT statement by concatenating five fields named: 1, 2, :3, 4, and 5. Write the string that an attacker gives as input to a field resulting in the removal of a record from a specified database table, should this string be passed without checking. Also, name the field. Suppose s/he has full access to both tables.

vii. How does data privacy come under attack in the cloud?

viii. How does hosting your website on public IaaS change security threats as compared to hosting it in your private cloud?

ix. Define two threats (one per line) against an encrypted database.

x. How authentication is different from authorization?

xi. A hacker finds out that a server scans contents for malicious code everyday night at midnight. Can s/he inject (which method) a particular type of payload that remains hidden (type) from the daily scans?

xii. Explain how botnets are deployed and used to launch a large-scale DDoS attack.