**Birla Institute of Technology & Science, Pilani**

**Work Integrated Learning Programmes Division**

**First Semester 2022-2023**

**Comprehensive Examination**

**(EC-3 Regular)**

Course No. : SS ZG681

Course Title : Cyber Security

Nature of Exam : Open Book

Weightage : 50%

No. of Pages = 3

No. of Questions = 9

Duration : 2 Hours

Date of Exam : 27/11/2022 (FN/AN)

Note to Students:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.
4. Rahul and Rohit are physically located in two different places. They need to communicate with each other secretly. So, they decide to encrypt their messages before exchanging. They know that they need a key to perform the encryption process and they also have a way to share the key with each other. Explain the type of encryption that is being considered in this scenario. There are two important requirements of this encryption. Identify and explain these two requirements.

[2 + 2 + 2 = 6]

1. Why is it important to have audit trail? Explain with example(s). List and explain at least two different categories of audit trails. [6]
2. Cybercrime or computer crime can be categorized based on the role that the computer plays in the criminal activity. Identify and explain these categories of cybercrime using examples under each category. Justify why/how your examples are appropriate under the category you choose. [6]
3. You join a company as a network administrator and this is your first week. You try to understand the number of networks and the IP addresses that are assigned to hosts in a local subnet. You approach your colleague to get the details. However, your colleague gives you the subnet mask and says he doesn’t have much information because the previous network administrator left the organization without documenting any details. Assuming that your organization uses Class B network and the subnet marks is 255.255.255.224, identify the number of networks, total number of IP addresses within each network, and the maximum number of IP addresses that can be assigned to hosts in a local subnet. Does it matter as far the number of hosts are concerned if this mask is used with a Class A or C network address? Explain. [5]
4. You are an employee of an organization. You are not an IT professional, but you are familiar with changing trends in the current technology landscape. You are also aware of increasing cybersecurity threats that is inherent in the growing technological landscape. Suppose you receive an email from a finance company stating that your loan payments are in arrears, and that action is required to correct this. However, as far as you know/remember, you have never applied for, or received, a loan from this company! You think that some kind of cyber attack has happened to you. What may have occurred that led to this situation of loan being created? What type of malware, and on which computer systems, might have provided the necessary information to an attacker that enabled them to successfully obtain this loan? What preventive steps you could have taken to avoid this situation. [2 + 2 + 2 = 6]
5. Security design principles are a collection of generally accepted standards of good practice. It is believed that these principles enforce security policies. Every organization is different and how they interpret and adopt the principles depend on specific circumstances. Considering data integrity, there are several models for achieving and maintaining data integrity. Describe the principle of separate of duty and explain how the Clark-Wilson model accomplishes this principle using an example. [1 + 2 + 3 = 6]
6. Lucy encounters Joseph in an online chat room. Joseph is using his real first name, but only his last initial. However, over a series of online conversations between Lucy and Joseph, he does reveal personal details about his life (marital status, children, occupation, region he lives in, and so forth). Lucy, pretending to be working for a financial company, eventually offers Joseph some piece of advice, such as an investment tip, as a trick to get Joseph’s email address from him. Once she gets his email address, an email exchange begins outside of the chat room, wherein Lucy purports to give Joseph her real name, thus encouraging Joseph to do the same.

Of course, the perpetrator’s name is fictitious, such as “Jane.” But Lucy now has Joseph’s real name, city, marital status, occupation, and so on. Lucy has a number of options she can try, but we will choose a simple one. She begins by using the phone book or the Web to get Joseph’s home address and phone number. She can then use this information to get Joseph’s social security number, in a variety of ways. The most straightforward would be to go through Joseph’s trash while he is at work. However, if Joseph works in a large company, Lucy can just call (or enlist someone to call), claiming to be Joseph’s wife or another close relative, wanting to verify personnel data. If Lucy is clever enough, she may come away with Joseph’s social security number. Then it is a trivial matter to get Joseph’s credit report and to get credit cards in his name.

From this scenario, consider the following questions:

1. What kind of theft is happening here? Explain it in detail.
2. What reasonable steps could Joseph have taken to protect himself?
3. What steps should any employer take to prevent being unwittingly complicit in this kind of theft? [2 + 2 + 2 = 6]
4. You are a networking professional in an organization. Your organization uses IPv4 addresses for its network devices. As you know, there are four octets in an IPv4 address and this rule gives a total of over 4.2 billion possible IP addresses. Although this is a big number, you are aware that this is not enough to support all the devices in the world. So, your organization has to use a technique to to extend the reach of the IPv4 address space. Briefly explain this technique. Explain what gateway routers to the outgoing and incoming packets in order to allow the data packets to be routed through the Internet. [1 + 2 = 3]
5. A security breach or attack can happen either from outside or from inside an organization. As a security professional, you know that there is a greater risk and a higher probability of damage happening from within an organization than from outside it. Many employees are not aware of this fact because they usually hear news stories about the security attacks happening from outside the organization. For instance, attacks such as defacing a website or circumventing a firewall to get access to confidential information typically happens from outside the organization. During the course of the semester, we discussed various types of access control mechanisms that work to keep the outsiders outside and restrict insiders’ abilities to a minimum and audit their actions. Considering threats to Access Control, discuss at least two specific attacks commonly carried out in environments today by insiders or outsiders. Discuss the counter measures to each of these attacks. [3 + 3 = 6]

\*\*\*\*\*\*\*\*\*\*