Strathmore UNIVERSITY

# SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

## MASTER OF INFORMATION SYSTEMS SECURITY

**Final Examination**

**MST 8103: Introduction to Information Security**

**DATE**: 11th January 2023 **TIME:** 2.5 Hours

**Instructions: Answer Question 1 (Compulsory) and any other two Questions**

**Question 1 [40 marks]**

**a)** Briefly define the following terminologies as used in the field of cyber security **[12 marks]**

i. Tailgating
ii. Rootkit
iii. Smishing
iv. Malvertising
v. Deepfake
vi. Whaling

**b)** Using appropriate diagrams, differentiate between Direct Distributed Denial of Service (DDoS) attack and Reflector Distributed Denial of Service (DDoS) attack **[6 marks]**

**c)** If you were to start a job as an IT Risk Officer at a blue-chip company due to the previous guy being fired for incompetence. You are presented with the following information:

i. Asset A has a value of X and has one vulnerability, which has a likelihood of 0.5 with no current controls. Your assumptions and data are 85% accurate **[2 marks]**

ii. Asset B has a value of Y and has two vulnerabilities **[6 marks]**

- Vulnerability #2 has a likelihood of 0.3 with a current control that addresses 60% of its risk
- Vulnerability # 3 has a likelihood of 0.6 with no current controls.
- Your assumptions and data are 95% accurate for Asset B

You are expected to compute the risk factor for every vulnerability and rank the above vulnerabilities. You are required to define your own values of X and Y. Show how you arrive to your final answer

**d)** Briefly explain 4 control strategies you would take to address any type of risk you face in your company. Use examples to illustrate your answer **[8 marks]**

**e)** You are engaged in a penetration-test where you are attempting to gain access to a protected location. You are presented with this login screen. Using relevant examples and illustrations, demostrate 3 ways how you would break into the system **[6 marks]**


**Question 2 [15 marks]**

**a)** Differentiate the following terminologies as applied in information security discipline. Illustrate with diagrams where possible **[10 marks]**

i. Plain text and ciphertext
ii. Cipher and key
iii. Cryptanalysis and cryptology
iv. Cryptography and Steganography
v. Virus and Worm

**b)** Briefly describe 5 reasons why a security analyst should avoid being overconfident after implementing or improving information security management in an organisation? Illustrate your answer with suitable examples **[5 marks]**

**Question 3 [15 marks]**

**a)** Imagine yourself as a security analyst in an organization whose server has been successfully attacked by a ransomware. You have just discovered the break-in, and the attacker seems to be "occupying" the system.

i. How would you expect to become aware of the successful break-in? That is, what "observable phenomena" would lead you to the conclusion that a computer system had been compromised by a ransomware? State 4 symptoms**[4 marks]**
ii. Provide 2 vectors for ransomware **[2 marks]**
iii. What, in general terms, would normally be your first 4 actions on discovering the break-in of ransomware? Explain briefly why you would take these actions **[4 marks]**

**b)** Using appropriate examples, describe 5 major reasons why cloud services might become unavailable **[5 marks]**

**Question 4 [15 marks]**

**a)** Suppose a web service provider implements a CAPTCHA as a security feature. The CAPTCHA has four images and require users to identify the one that shows a 'dog'. Discuss 3 ways how such a security feature can be compromised by intruders. Illustrate your answer with appropriate examples. *Assumptions may be provided in the answer* **[6 marks]**

**b)** Below is a table showing different types of attacks against elements of security. Indicate clearly by ticking (√) which attack corresponds to a given security aspect. *Hint: 1 attack may affect more than one security aspect and wrong answer attracts a penalty* **[5 marks]**

| | Release of message contents | Masquerade | Replay | Modification of messages | Denial of service |
|---|---|---|---|---|---|
| **Authentication** | | | | | |
| **Access control** | | | | | |
| **Confidentiality** | | | | | |
| **Data integrity** | | | | | |
| **Non-repudiation** | | | | | |
| **Availability** | | | | | |

**c)** Below is a security feature commonly used to offer security services to web based applications. Briefly describe the security importance of this feature **[4 marks]**