Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

MASTER OF INFORMATION SYSTEMS SECURITY

Final Examination

MST 8103: Introduction to Information Security

DATE: 17th December 2024 **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 **[20 marks]**

i. Tailgating
ii. Rootkit
iii. Smishing
iv. Malvertising
v. Deepfake
vi. Whaling
vii. Advanced Persistent Threat(APT)
viii. Sinkhole
ix. Information Stealer
x. Supply chain attack

b) 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 20 and has one vulnerability, which has a likelihood of 0.5 with no current controls. Your assumptions and data are 75% accurate **[4 marks]**
ii. Asset B has a value of 50 and has two vulnerabilities **[6 marks]**
   - Vulnerability #2 has a likelihood of 0.3 with a current control that addresses 50% of its risk
   - Vulnerability # 3 has a likelihood of 0.6 with no current controls.
   - Your assumptions and data are 97% accurate for Asset B

You are expected to compute the risk factor for every vulnerability and rank the above vulnerabilities. You are required to show how you arrive to your final answer

c) Briefly describe 5 motives that drive intruders to breach security of information systems. Illustrate your answer with examples **[10 marks]**

Question 2 [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) Briefly describe 5 factors that influence success of an intrusion. Illustrate your answer with examples **[5 marks]**

Question 3 [15 marks]

a) 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* **[7 marks]**

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

b) Briefly describe 4 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 **[8 marks]**

Question 4 [15 marks]

a) 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]**

b) 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]**

c) Using appropriate examples, describe 3 major reasons why cloud services might become unavailable **[3 marks]**