Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BACHELOR OF COMPUTER NETWORKING AND SECURITY

CNS 2103: INTRODUCTION TO CYBER SECURITY

END OF SEMESTER EXAM

Date: 31st July 2024 **Time:** 15:30-17:30 Hours

Instructions:

1. This Examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question 1 (20 Marks)

a) Cyber security rests on Confidentiality, Integrity, and Availability of resources. Discuss each of these pillars, giving a possible breach and a corresponding possible mitigation. **(6 Marks)**

b) The rules for enforcing an organization's desired security policy are encoded into the firewall by local administrators. Design firewall rules to prevent outward web surfing. **(4 Marks)**

c) Differentiate between reactive and proactive safeguard strategies. **(4 Marks)**

d) Extensive defence in depth models exist to help cyber security professionals protect their businesses and organizations. One popular model is AAA. Discuss this model. **(6 Marks)**

Question 2 (20 Marks)

a) To help prevent cyber-attacks from wreaking havoc on a network, many security teams have turned to a new form of protection known as security analytics. Explain this method of protection. How is SIEM relevant in this? Discuss the TWO main methods of security analytics. **(10 Marks)**

b) Explain the principle of **Default Block** as used in firewall design. How would argue for it? **(4 Marks)**

c) An important discipline in cyber security involves the threat information sharing between entities. Discuss the requirements for high quality threat feeds. **(6 Marks)**

Question 3 (20 Marks)

a) One approach to reducing cyber security risk involves security compliance. Explain security compliance. How can security compliance be used to reduce the risk of APTs? Briefly explain NIST's Framework for Improving Critical Infrastructure

cybersecurity. Most experts point out problems with compliance tasks. Explain any TWO such problems. **(10 Marks)**

b) Discuss how Public Key Cryptography may be used to achieve both confidentiality and authentication. **(4 Marks)**

c) PKC has had a profound global societal influence by enabling the secure sale of goods on the Internet. Discuss the role of Certificate Authorities (CA) in this process. **(6 Marks)**

Question 4 (20 Marks)

a) An IDS monitors computing activity to detect evidence of cyber-attacks. Discuss any **TWO** disadvantages of signature-based detection as used in Intrusion detection. Give relevant examples. **(4 Marks)**

b) Explain any FOUR ways an intruder might determine your password. **(8 Marks)**

c) How might Two-Factor Authentication (2FA) be implemented? **(4 Marks)**

d) How does 2FA mitigate against spoofing attack? **(4 Marks)**

Question 5 (20 Marks)

a) Explain TCP/IP three-way handshake protocol. **(6 Marks)**

b) There are various types of scans. Compare the half-scan, full-scan and deep-scan.

c) Provide a clear explanation for Advanced Persistent Attacks. How is it implemented? Weave in the following concepts in your explanation: enterprise perimeter, infiltration, lateral traversal, exfiltration, phishing, spear phishing, remote access tool (RAT), Active Directory. What are the goals of an APT? What does Persistent in the acronym signify? **(10 Marks)**

d) TCPdump is a powerful utility with many options. How can you start tcpdump for greater verbosity and to show HEX and ASCII information about the packet. **(1 Mark)**