Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES (SCES)

CNS

END OF SEMESTER EXAMINATION

CNS 2103 INTRODUCTION TO CYBER SECURITY

DATE: 25th July 2022 Time: 2 Hours

Instructions

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

Question 1 (20 Marks)

a) Clearly explain the following concepts: **(5 Marks)**
   i) Spoofing
   ii) Client-Server interaction
   iii) Data leakage
   iv) Shadow IT
   v) DDOS

b) What is the role of a security information and event management system (SIEM)? **(2 Marks)**

c) Cyber security rests on the pillars of **Confidentiality**, **Integrity**, and **Availability**. Explain each of these pillars, giving examples of a possible attack and possible remediation. **(9 Marks)**

d) Write sample high-level code to explain how a Computer Worm works. **(2 Marks)**

e) Compare Reactive and Proactive cyber security safeguards. **(2 Marks)**

Question 2 (20 Marks)

a) Discuss how an Advanced Persistent Threat is carried out. **(10 Marks)**

b) One approach to reducing cyber security risk involves security compliance. How can the following five requirements in a compliance program reduce the security risk of an APT? **Email filtering, employee awareness, enterprise scanning, pc security and URL filtering**. **(10 Marks)**

Question 3 (20 Marks)

a) To prevent cyber-attacks form wreaking havoc on a network, many security teams have turned to a new form of protection known as **security analytics**. What does this involve? **(2 Marks)**

b) Differentiate between pattern matching and profile-based matching as used in security analytics. **(2 Marks)**

c) How do you go about implementing Behavioral profiling in security analytics? **(8 Marks)**

d) The specific description of an attack is known as a signature. Discuss, with examples, any TWO disadvantages of signatures. **(4 Marks)**

e) What is defense-in-depth? Briefly explain the defense-in-depth model acronym AAA. **(4 Marks)**

Question 4 (20 Marks)

a) Discuss, with examples, **reflection** and **amplification** as fundamental concepts of DDOS. **(6 Marks)**

b) What measures can be taken to reduce the risk of distributed denial of service attacks? **(2 Marks)**

c) Compare and Contrast between **Discretionary Access Control (DAC)** and **Mandatory Access Control (MAC)**. **(4 Marks)**

d) A common security mechanism, known as a **firewall**, sits between clients and servers. Discuss the role and operation of a network firewall. **(4 Marks)**

e) Write a firewall rule to prevent outbound web surfing. **(4 Marks)**

Question 5 (20 Marks)

a) The so-called TCP/IP handshake provides the base communication on which most network security methods operate. Explain the three-way handshake, indicating the different flags. **(6 Marks)**

b) A strategy often used by firewall administrators involves something called default block. What does this involve? What is the benefit? **(3 Marks)**

c) A popular security technique involves using a software tool called a scanner that attempts to connect with target systems or networks across a TCP/IP connection to see what it can find. In which 3 areas can the security team position the scanner? **(3 Marks)**

d) Compare the following different types of scans: **half-scan, full-scan, deep scan**. **(6 Marks)**

e) How is a firewall different from an IDS? **(2 Marks)**