Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 4102: ETHICAL HACKING II

DATE: 2nd August 2023 Time: 2 Hours

Instructions

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

QUESTION ONE [30 MARKS]

a) (i) Explain briefly why social engineering is a significant threat in cybersecurity. (3 Marks)
(ii) Outline four common social engineering techniques used by attackers. (4 Marks)

b) Differentiate between:
   (i) Network Scanning and Port Scanning (4 Marks)
   (ii) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. (4 Marks)

c) Discuss three scanning techniques used in port scanning and their purposes. (6 Marks)

d) What are some common threats associated with web servers and mobile platforms? (5 Marks)

e) Describe two common DoS attack techniques. (4 Marks)

QUESTION TWO [20 MARKS]

a) Explain the concept of session hijacking and discuss two techniques used to carry out session hijacking attacks. (8 Marks)

b) Describe the SQL injection vulnerability and its potential impact on a web application. (4 Marks)

c) Discuss the steps involved in conducting a successful SQL injection attack. (8 Marks)

QUESTION THREE [20 MARKS]

a) Explain the common vulnerabilities in web servers and their potential impact on system security. (6 Marks)

b) Discuss the security risks associated with hacking wireless networks and countermeasures to enhance their security. (8 Marks)

c) Explain the vulnerabilities in Microsoft operating systems and the potential risks they pose. (6 Marks)

QUESTION FOUR [20 MARKS]

a) Explain the concept of hacking mobile platforms and discuss two common attack vectors used in mobile platform exploitation. (8 Marks)

b) Discuss the vulnerabilities in Linux operating systems and their potential impact on system security. (6 Marks)

c) Describe the process of cracking Wired Equivalent Privacy (WEP) in wireless networks and its weaknesses. (6 Marks)

QUESTION FIVE [20 MARKS]

a) Explain the process of stealing passwords from HTTPS sessions using a Man-in-the-Middle (MitM) attack. (8 Marks)

b) Discuss the potential consequences of exploiting internet users and their vulnerabilities. (4 Marks)

c) Explain the countermeasures that can be implemented to mitigate the risks associated with stealing passwords through a Man-in-the-Middle attack. (8 Marks)