Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 3202: ETHICAL HACKING I

DATE: 4th December 2023 Time: 13:00-15:00 Hours

Instructions

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

QUESTION ONE [30 MARKS]

a) Differentiate between viruses, worms, and Trojans, providing examples for each type of malware. (5 Marks)

b) Describe the key phases involved in conducting effective malware analysis. (5 Marks)

c) Discuss the role of foot printing and reconnaissance in ethical hacking and the tools commonly used for this purpose. (5 Marks)

d) Explain various network scanning techniques employed by ethical hackers and their importance. (5 Marks)

e) Define system enumeration and enumerate its different techniques in ethical hacking. (5 Marks)

f) Discuss the methodologies and tools used in system hacking during ethical penetration testing. (5 Marks)

QUESTION TWO [20 MARKS]

a) Analyze the characteristics of advanced malware threats such as Advanced Persistent Threats (APTs) and fileless malware. Explain the countermeasures used to mitigate these threats. (10 Marks)

b) Discuss the relevance of Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits in the enumeration phase of ethical hacking. Provide real-world examples of these exploits. (10 Marks)

QUESTION THREE [20 MARKS]

a) Discuss modern techniques and tools for conducting foot printing and reconnaissance in ethical hacking. Provide real-world examples of their application. (10 Marks)

b) Discuss the use of steganography and steganalysis attacks in system hacking. Provide practical examples of how these techniques can be used in ethical hacking. (10 Marks)

QUESTION FOUR [20 MARKS]

a) Describe packet-sniffing techniques used in ethical hacking and their implications for network security. (10 Marks)

b) Explain the importance of information security controls, relevant laws, and standard procedures in the ethical hacking process. (10 Marks)

QUESTION FIVE [20 MARKS]

XYZ Corporation is a medium-sized organization that has recently experienced a data breach, leading to the exposure of sensitive customer data. As an ethical hacker, you have been called in to assess the security posture of XYZ Corporation's network and systems. Based on the case study, answer the following questions:

a) Briefly describe the steps you would take to conduct an initial assessment of XYZ Corporation's security vulnerabilities. (6 Marks)

b) Provide a detailed list of potential security vulnerabilities or weaknesses that may have contributed to the recent data breach. (8 Marks)

c) Suggest specific security measures and best practices that XYZ Corporation can implement to prevent similar incidents in the future. (6 Marks)