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: 5th December 2024 **Time: 10:30-12:30 Hours**

Instructions

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

QUESTION ONE [30 MARKS]

Case Study: Comprehensive Security Assessment for Strathmore University

Strathmore University, a large educational institution with multiple campuses, has requested a comprehensive security assessment of its IT infrastructure. The university is concerned about potential vulnerabilities in its networks, systems, and web applications. Key areas of concern include network security, malware threats, system vulnerabilities, and potential for data breaches.

As a member of the ethical hacking team, you have been tasked with assessing these areas. Your findings and recommendations will help Strathmore University enhance its overall security posture.

a) Explain the concept of ethical hacking and its importance in the context of Strathmore University's security assessment. **(2 Marks)**

b) Describe two key differences between ethical hacking and malicious hacking. Include the objectives and potential consequences of each. (**4 Marks)**

c) Define footprinting and reconnaissance. Explain their significance in the initial phase of ethical hacking. Discuss how these techniques can help identify potential vulnerabilities in Strathmore University's network. **(4 Marks)**

d) Identify two tools you would use for footprinting and reconnaissance. Explain the functionalities of these tools and how they can be used to gather information about Strathmore University's network infrastructure. **(4 Marks)**

e) Explain what network scanning is and describe its potential impact on identifying vulnerabilities in Strathmore University's network. Provide examples of the types of information that can be gathered through network scanning. **(3 Marks)**

f) Outline the methodology you would use to perform a comprehensive network scan of Strathmore University's infrastructure. Include specific tools and techniques you would employ, as well as the steps you would take to ensure minimal disruption to the university's operations. **(4 Marks)**

g) Define enumeration and explain how it differs from network scanning. Discuss the types of information that can be gathered through enumeration. **(2 Marks)**

h) Detail the process you would follow to perform enumeration on Strathmore University's systems. Include the types of information you would attempt to enumerate, the tools you would use, and the potential security implications of the information gathered. **(7 Marks)**

QUESTION TWO [15 MARKS]

a) Strathmore University discovers that some of their systems have been infected with malware, potentially compromising sensitive student and faculty data.
   (i) Describe the process of malware analysis and how it can help identify the extent of a malware infection. **(4 Marks)**
   (ii) Identify and describe two tools that can be used for malware analysis. (**4 Marks**)

b) Describe the process of static malware analysis and how it can help identify the nature and potential impact of malware. **(4 Marks).**

c) Discuss three measures the university can take to enhance the security of its networks. **(3 Marks)**

QUESTION THREE [15 MARKS]

a) Strathmore University uses a variety of operating systems across its infrastructure, including some older versions. They are concerned about system hacking attempts.
   (i) Explain four common techniques used in system hacking. **(4 Marks)**
   (ii) Describe how attackers can exploit these techniques to gain unauthorized access. Provide two specific examples. **(3 Marks)**
   (iii) Discuss three countermeasures that can be implemented to protect against system hacking attempts. **(3 Marks)**

b) Discuss five common vulnerabilities in web applications and their potential impact on the security of Strathmore University's online systems. (**5 Marks**)

QUESTION FOUR [15 MARKS]

Strathmore University uses a centralized authentication system for student and faculty access to various online resources. You have been tasked with assessing the security of this system, focusing on potential vulnerabilities related to session management and sniffing attacks.

a) Explain the importance of secure session management in the context of Strathmore University's centralized authentication system. **(3 Marks)**
b) Describe the methodology you would use to test for session-related vulnerabilities in the university's authentication system. Include the tools and techniques you would use. **(5 Marks)**
c) Discuss two specific types of sniffing attacks that could potentially compromise the university's network security. Explain how you would simulate these attacks during your testing. **(4 Marks)**
d) Recommend three countermeasures to secure the university's authentication system and network against session hijacking and sniffing attacks. **(3 Marks)**

QUESTION FIVE [15 MARKS]

Strathmore University is implementing a new risk management strategy for its IT infrastructure. As an ethical hacking expert, you have been asked to contribute to this process by conducting a vulnerability analysis of the university's systems.

a) Explain the concept of vulnerability analysis and discuss why it is a crucial component of an effective risk management strategy. **(2 Marks)**
b) Describe two different approaches to vulnerability analysis. Provide examples to illustrate how each approach can be applied in the context of Strathmore University's IT infrastructure. **(4 Marks**)
c) Recommend a framework or methodology that Strathmore University could adopt for ongoing vulnerability management. Explain your choice. **(3 Marks)**
d) After completing the vulnerability analysis, describe how you would document your findings and communicate them to Strathmore University's IT management team. Include the key components of a comprehensive vulnerability analysis report and discuss how you would present your recommendations to ensure they are understood and actionable. **(6 Marks)**