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:22nd 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 ONE [30 MARKS]**

## Case Study: Comprehensive Penetration Testing for XYZ Corporation

**Background:** XYZ Corporation, a mid-sized company specializing in e-commerce and online services, has requested a comprehensive penetration test to evaluate the security posture of its network infrastructure and applications. The company is concerned about potential vulnerabilities that could be exploited by attackers. The key areas of concern include social engineering, port scanning, denial-of-service (DoS) attacks, session hijacking, SQL injection, web server vulnerabilities, and wireless network security.
As a member of the penetration testing team, you have been tasked with assessing these areas. Your findings and recommendations will help XYZ Corporation strengthen its security defenses.

a) Explain the importance of incorporating social engineering testing into a comprehensive penetration test for XYZ Corporation. (**2 Marks**)

b) Describe two specific social engineering techniques you would use to test XYZ Corporation's employee susceptibility to social engineering attacks. Include the objectives and expected outcomes of each technique. (**4 Marks**)

c) Define port scanning and explain its significance in the reconnaissance phase of penetration testing. Discuss how port scanning can help identify potential entry points for attackers. (**4 Marks**)

d) Identify two port scanning tools you would use for this engagement. Explain the functionalities of these tools, including how they can be used to detect open ports and services on XYZ Corporation's network. (**4 Marks**)

e) Explain what a Denial-of-Service (DoS) attack is and describe its potential impact on XYZ Corporation's operations. Provide examples of how a DoS attack can disrupt business continuity. (**3 Marks**)

f) Outline the methodology you would use to identify potential DoS vulnerabilities in XYZ Corporation's network. Include specific tools and techniques you would employ, as well as the steps you would take to simulate and assess the impact of a DoS attack. (**4 Marks**)

g) Define session hijacking and explain the mechanisms through which it can be exploited by attackers to gain unauthorized access to user sessions. (**2 Marks**)

h) Detail the process you would follow to test for session hijacking vulnerabilities in XYZ Corporation's web applications. Include the types of attacks you would simulate, the tools you would use, and the measures you would take to prevent detection. (**7 Marks**)

**QUESTION TWO [15 MARKS]**

a) An e-commerce company discovers that some of their customers' passwords were intercepted through a man-in-the-middle (MITM) attack while accessing their accounts over HTTPS.
   (i) Describe the process of a man-in-the-middle attack and how it can compromise HTTPS sessions. (**4 Marks**)
   (ii) Identify and describe two tools that can be used to perform MITM attacks. (**4 Marks**)

b) A corporation issues mobile devices to employees for work purposes. Recently, several devices were compromised, leading to data breaches and leaks of sensitive information.
   (i) Explain the main attack vectors used in hacking mobile platforms. (**4 Marks**)
   (ii) Discuss three measures the corporation can take to enhance the security of its mobile devices. (**3 Marks**)

**QUESTION THREE [15 MARKS]**

a) A company using Windows XP and Windows 7 machines as part of their infrastructure discovered that several machines were compromised through known vulnerabilities in these operating systems.

   (i) Explain the four typical vulnerabilities found in older Microsoft operating systems like Windows XP and Windows 7. (**4 Marks**)

   (ii) Describe how attackers can exploit these vulnerabilities to gain unauthorized access. Provide two specific examples. (**3 Marks**)

   (iii) Discuss three countermeasures that can be implemented to protect against these vulnerabilities. (**3 Marks**)

b) Discuss five vulnerabilities in Linux operating systems and their potential impact on system security. (**5 Marks**)

**QUESTION FOUR [15 MARKS]**

Ribatech corporation uses wireless networks extensively in their offices and hosts critical applications and services on web servers. You have been tasked with performing a penetration test to identify vulnerabilities in both the wireless networks and web servers, and provide recommendations for securing them.

a) Explain the importance of securing both wireless networks and web servers in an organization like Ribatech. (**3 Marks**)

b) Describe the methodology you would use to conduct a penetration test on Ribatech 's wireless networks and web servers. Include the tools and techniques you would use. (**5 Marks**)

c) Discuss two specific types of attacks on wireless networks and web servers. Explain how you would simulate these attacks during your testing. (**4 Marks**)

d) Recommend three countermeasures to secure both wireless networks and web servers that XYZ Corporation should consider implementing. (**3 Marks**)

**QUESTION FIVE [15 MARKS]**

ABC Corporation has a cloud platform that is suspected to have SQL injection vulnerabilities. As a penetration tester, you are required to evaluate the platform for such vulnerabilities and report your findings.

a) Explain the concept of SQL injection and discuss why it is considered a critical security issue in web applications. (**2 Marks**)
b) Describe two different types of SQL injection attacks. Provide examples to illustrate how each type can be exploited by an attacker. (**4 Marks**)
c) Recommend countermeasures that ABC Corporation should implement to mitigate SQL injection vulnerabilities. (**3 Marks**)
d) After completing the penetration test, describe how you would document your findings and communicate them to ABC Corporation’s management. Include the key components of a comprehensive penetration testing report, and discuss how you would present your recommendations to ensure they are understood and actionable. (**6 Marks**)