UNIVERSITY EXAMINATIONS
EXAMINATION FOR JANUARY/APRIL 2023/2024 FOR DIPLOMA IN CYBER SECURITY/DIPLOMA IN ETHICAL HACKING

RES 028: PROTECTION FROM CYBER ATTACKS

DATE: 12TH APRIL, 2024 **TIME: 2 HOURS**

GENERAL INSTRUCTIONS:
Students are NOT permitted to write on the examination paper during examination period.
This is a closed book examination. Text book/Reference books/notes are not permitted.

SPECIAL INSTRUCTIONS:
This examination paper consists Questions in Section A followed by section B.
Answer **Question 1 and any Other Two** questions.
QUESTIONS in ALL Sections should be answered in answer booklet(s).

1. **PLEASE start the answer to EACH question on a NEW PAGE.**
2. **Keep your phone(s) switched off at the front of the examination room.**
3. **Keep ALL bags and caps at the front of the examination room and DO NOT refer to ANY unauthorized material before or during the course of the examination.**
4. **ALWAYS show your working.**
5. **Marks indicated in parenthesis i.e. ( ) will be awarded for clear and logical answers.**
6. **Write your REGISTRATION No. clearly on the answer booklet(s).**
7. **For the Questions, write the number of the question on the answer booklet(s) in the order you answered them.**
8. **DO NOT use your PHONE as a CALCULATOR.**
9. **YOU are ONLY ALLOWED to leave the exam room 30minutes to the end of the Exam.**
10. **DO NOT write on the QUESTION PAPER. Use the back of your BOOKLET for any calculations or rough work.**

SECTION A (COMPULSORY)

QUESTION ONE (30 Marks)

a) Differentiate between a threat and an attack in the context of cybersecurity, highlighting the key distinctions and explaining how they relate to the overall risk landscape **(4 marks)**

b) Your organization's network experiences a sudden slowdown in performance, and suspicious files are found on several computers. How would you investigate the possibility of a malware infection, and what actions would you take to contain and remove the malware? **(6 marks)**

c) Explain the workings of a Denial of Service (DoS) attack, including its underlying principles and techniques used to disrupt or disable a targeted system's availability **(4 marks)**

d) Describe the concept and mechanism of a buffer overflow attack, outlining how it occurs and the potential consequences it poses to the security of a targeted system **(4 marks)**

e) Identify and explain the primary objective of a rootkit and discuss its implications for the security of a compromised system. **(4 marks)**

f) A particular database threat utilizes a SQL injection technique to penetrate a target system. How would an attacker use this technique to compromise a database **(3 marks)**

g) Provide an explanation of a phishing attack, using a specific example to illustrate its methodology and the potential risks it poses to individuals or organizations and how the risk can be mitigated. **(5 marks)**

SECTION B: (ANSWER ANY TWO QUESTIONS)

QUESTION TWO (20 Marks)

a) David was peacefully browsing and had opened several tabs to access different websites, one of the tabs opened was directed to an attackers website. Based on the scenario described, identify the type of attack that occurred when David unknowingly accessed an attacker's website and how the attack can be prevented **(4 marks)**

b) Using a diagram, illustrate and describe the mechanism and impact of a DDoS attack, highlighting the key components, stages, and the overall flow of the attack and recommend ways though which the attack can be mitigated. **(4 marks)**

c) Define malware and provide a comprehensive explanation, including relevant examples, to illustrate its nature and potential impact on computer systems. Additionally, outline and describe various countermeasures and best practices that individuals or organizations can employ to protect against malware threats. **(8 marks)**

d) Explain the concept of cross-site scripting (XSS) and its potential implications for web application security. Furthermore, outline effective preventive measures and best practices that can be implemented to mitigate the risk of XSS attacks **(4 marks)**

QUESTION THREE (20 Marks)

a) A colleague receives a suspicious phone call from someone claiming to be from the IT department, asking for their login credentials to "fix a problem with their account." Provide guidance on how to handle this situation and avoid falling victim to a social engineering attack **(4 marks)**

b) Provide a detailed explanation of DDoS attacks, including their characteristics, objectives, and the techniques used to execute them. Additionally, outline effective strategies and countermeasures that organizations can employ to mitigate and counteract DDoS attacks **(10 marks)**

c) Using a diagram, illustrate and describe the process of the three-way handshake in TCP/IP communication. Explain the purpose and sequence of each step involved in establishing a connection between a client and a server **(6 marks)**

QUESTION FOUR (20 Marks)

a) Outline and categorize various types of threats and attacks commonly encountered in the realm of cybersecurity. Provide brief explanations and examples for each type, highlighting their potential impact and associated risks **(8 marks)**

b) Using a diagram, illustrate and explain the workings of a Smurf attack, highlighting the key steps and components involved. Describe the purpose, impact, and countermeasures that can be employed to mitigate the effects of such an attack **(8 marks)**

c) Differentiate between DNS poisoning and ARP poisoning, explaining their distinct mechanisms, objectives, and potential impacts on network security **(4 marks)**

QUESTION FIVE (20 Marks)

a) Describe common types of social engineering attacks, providing examples and explanations for each type. Discuss the techniques employed in these attacks and the potential consequences they pose to individuals and organizations **(8 marks)**

b) Your organization's website is defaced by a hacker who exploits a vulnerability in the content management system (CMS). Explain how you would you restore the website to its original state, investigate the source of the breach, and implement measures to secure the CMS and prevent future defacement attacks **(8 marks)**

c) A competitor company claims to have access to your organization's confidential documents and is threatening to release them unless a ransom is paid. Explain how would you investigate the breach, negotiate with the attacker, and prevent similar incidents in the future.

(4 marks)