JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR DIPLOMA IN CYBER SECURITY

2nd Year 1st SEMESTER 2024/2025 ACADEMIC YEAR

MAIN REGULAR

COURSE CODE: ISD 1205

COURSE TITLE: CYBER SECURITY ASSESMENT AND TESTING

EXAM VENUE: **STREAM: (DIP. CYBER SECURITY)**

DATE: **EXAM SESSION: SEPT – DEC 2024**

TIME: 2.00 HOURS

Instructions:

This paper consists of two sections A and B

i. Attempt **ALL** questions in section A and any **THREE** in section B
ii. Candidates are advised not to write on the question paper.
iii. Candidates must hand in their answer booklets to the invigilator while in the examination room.

SECTION A

(Answer All questions in this section)

1. Define passive reconnaissance and provide one example of a tool used for it. (4 Marks)
2. List and explain the TWO main types of reconnaissance. (3 Marks)
3. Explain the role of social engineering in reconnaissance. (3 Marks)
4. Discuss the difference between WHOIS and NSLookup in information gathering. (3 Marks)
5. What is the importance of mapping an organization's internal structure in reconnaissance? (3 Marks)
6. Explain the purpose of network scanning and give one tool used in this process. (4 Marks)
7. Describe the difference between a **ping sweep** and a **port scan**. (3 Marks)
8. What is the importance of creating a network topology map? (4 Marks)
9. Define **service enumeration** and explain why it is important in network mapping. (3 Marks)
10. How can vulnerability assessment tools like **Nessus** and **OpenVAS** assist in network security? (3 Marks)
11. Describe how an **Nmap** TCP SYN scan works and its benefits. (3 Marks)
12. What is **Wireshark** used for in network mapping, and what kind of information can it provide? (2 Marks)
13. Describe how search engines can be used for reconnaissance and provide an example of a search query. (2 Marks)

SECTION B

(Answer ANY THREE questions from this section)

14. (a) Define network resource enumeration and explain its importance in cybersecurity assessments. (10 Marks)

    (b) Enumerate the common tools used for network resource enumeration and explain their functions. (10 Marks)
15. (a) Explain what a vulnerability is, and identify the different types of vulnerabilities in cybersecurity. (10 Marks)

    (b) Describe the process of exploiting a known vulnerability, including the steps involved from research to post-exploitation. (10 Marks)
16. (a) Discuss the key components that should be included in a security assessment report. (10 Marks)

    (b) Explain the role of proof of concept in a security assessment report and its importance in documenting vulnerabilities. (10 Marks)

17. (a) Describe the process of network scanning and mapping in a cybersecurity assessment. How do tools like Nmap assist in discovering vulnerabilities? (12 Marks)

(b) Given the importance of informed consent in social engineering simulations, describe how you would ethically design and conduct a phishing simulation to assess employees' vulnerability to such attacks. (8 Marks)