UNIVERSITY EXAMINATIONS

EXAMINATION FOR JANUARY/APRIL 2023/2024 DIPLOMA IN COMPUTER SCIENCE/DIPLOMA IN INFORMATION TECHNOLOGY/DIPLOMAN IN BUSINESS INFORMATION TECHNOLOGY

RES 027 : VULNERABILTY ASSESMENT & PENETRATION TESTING

DATE: APRIL 2024 TIME: 2 HOURS

GENERAL INSTRUCTIONS:

Students are NOT permitted to write on the examination paper during exam time.

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.**

Question 1 (30 Marks) – Compulsory

(a) Explain the difference between the following concepts. Use examples:

i. Threat and Attack [4marks]

ii. Vulnerability Assessment and Penetration testing [4marks]

(b) Write nmap command to perform the following tests:

i. Check open ports on a host [2marks]

ii. Check the operating system the host. [2marks]

iii. Determine if port 80 is open. [2marks]

(c) Discuss three benefits of performing vulnerability assessment on organization ICT infrastructure. [6marks]

(d) Write sample syntax for performing the following: [6marks]

i. Cross-site scripting test on the input field

ii. SQL Injection on login form.

(e) Explain the four ethical expectations of professional pen testers when performing VAPT assignments. [4marks]

Question 2 (15 Marks)E

(a) Explain the function of the following tools and show how they are used in VAPT.

(i) Tracert [4marks]

(ii) Ping [4marks]

(b) Explain the faces of penetration testing process. [7marks]

Question 3 (15 Marks)

(a) State three advantages of wireless network. [3marks]

(b) Explain four common WIFI related vulnerabilities. [8marks]

(c) Explain the use of the following WIFI testing tools: [4marks]

i. Aircrack-ng

ii. Airodump-ng

Question 4(15 Marks)

(a) Write an nmap command for sql injection vulnerability on a website. [6marks]

(b) Explain the concept : system hacking [1marks]

(c) Explain four characteristics of vulnerable passwords [8marks]

Question 5 (15 Marks)

(a) Name 3 password cracking tools. [3marks]

(b) Explain three social engineering techniques for obtaining password. [6marks]

(c) Using diagram, explain the architecture of secure web application model. [6marks]