BOWEN UNIVERSITY, IWO

COLLEGE OF COMPUTING AND COMMUNICATION STUDY

COURSE CODE: CYB 403 (3units) SESSION: FIRST SEMESTER 2023/2024

COURSE TITLE: SYSTEMS VULNERABILITY ASSESSMENT AND TESTING

INSTRUCTION: Answer any Four (4) Questions DURATION: 3 Hours

QUESTION ONE

(a) What are the objectives of penetration testing? (1mark)
(b) What are the differences between a Pen Tester and a Hacker? (2marks)
(c) Briefly explain the three (3) widely accepted types of penetration testing, highlight three (3) advantages and disadvantages of each (7marks)
(d) With the help of a compact tree diagram, explain the six criteria and corresponding metrics for defining penetration tests. (10marks)

QUESTION TWO

(a) Briefly explain the three (3) main steps for conducting a penetration test (6marks)
(b) With examples, explain these two methods of reconnaissance (4marks)
(i) active reconnaissance (ii) passive reconnaissance
(c) Briefly discuss the four (4) phases of penetration testing (4marks)
(d) Illustrate and explain the set of activities involves in assessing network vulnerabilities (6marks)

QUESTION THREE

(a) What is the relationship between vulnerabilities, threats, and risks in terms of computer security? Give three (3) examples of each (5marks)
(b) Explain Five (5) reasons why is vulnerability testing is important? (5marks)
(c) Explain succinctly five (5) main vulnerabilities affecting applications and IT systems (5marks)
(d) Differentiate between a host vulnerability assessment and network vulnerability assessment, highlighting their strengths and limitations (5marks)

QUESTION FOUR

(a) With examples, describe the following vulnerability testing methods (8marks)
(i.) Active Testing (iii.) Network Testing
(ii.) Passive Testing (iv.) Distributed Testing
(b) Describe any two (2) techniques used in vulnerability assessment (2marks)
(c) Briefly explain the following information gathering techniques (10marks)
(i.) Foot printing (iii.) Social Engineering (v.) Dumpster Diving
(ii.) Network Scanning (iv.) War Dialing

QUESTION FIVE

(a) (i) Explain the term "password cracking" (2mark)

(ii) How are Hashing and secret salts used in managing a password file? What is their purpose? (5marks)

(b) Briefly explain the following types of password breaking (4marks)

(i.) Dictionary attack (ii.) Brute force attack

(c) Briefly explain three (3) traditional password cracking methods that you know (3marks)

(d) Briefly explain three (3) countermeasures for password cracking (6marks)

(i.) During the password design stage (ii.) After the generation of the passwords

QUESTION SIX

(a) Define the following terms: (10 marks)

(i.) Fuzz testing (iii.) Patch management (v.) attack Surface analysis

(ii.) Fingerprinting (iv.) Security Auditing

(b) Explain the functions of the following penetration testing tools, Give an example of each (7marks)

(i.) Service and Network Mapping Tools

(ii.) Scanning and Vulnerability Assessment Tools

(iii.) Exploitation Tools

(c) Briefly explain these Three (3) different approaches to vulnerability testing: (3marks)

(i.) administrative (ii.) outsider (iii.) hybrid