BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Sc.(ANCS)-Hons-2023
Course Name – Vulnerability Analysis and Penetration Testing
Course Code - BNC37108 (T)
(Semester III)

Full Marks : 40 **Time : 2:0 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 10=10

1. *Choose the correct alternative from the following :*

(i) Which tool is used for building custom payloads for exploitation?

a) msfvenom
b) Metasploit
c) Burp Suite
d) Nmap

(ii) Which phase involves gaining information about the target system, network, and vulnerabilities?

a) Enumeration
b) Gaining Access
c) Scanning
d) Exploitation

(iii) Which type of reconnaissance relies on publicly available knowledge without directly engaging with the target?

a) Active Reconnaissance
b) Passive Reconnaissance
c) Social Engineering
d) Phishing

(iv) Which tool can be used for hiding a secret message within an image?

a) Nmap
b) Steghide
c) Dirbuster
d) Metasploit

(v) Choose a primary purpose of DNS poisoning.

a) To flood the network with fake traffic
b) To steal sensitive information from network traffic
c) To substitute false IP addresses at the DNS level
d) To block access to legitimate websites

(vi) Choose a primary purpose of session hijacking.

a) To encrypt network communication
b) To exploit software vulnerabilities
c) To gain unauthorized access to a web server
d) To impersonate legitimate users

(vii) In SQL injection, what kind of data is injected into the application?

a) JavaScript code
b) XML data
c) SQL queries
d) Image files

(viii) Select a common security measure to protect against credential compromise.

a) Using weak passwords b) Sharing passwords openly
c) Implementing multi-factor authentication d) Storing passwords in plaintext

(ix) What type of cloud security technique involves creating roles for different users?

a) API security b) Access management
c) Encryption d) Network segmentation

(x) Choose a primary defense against SQL injection.

a) Password complexity b) Data encryption
c) Input validation d) User authentication

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Expain the phases that a penetration tester will follow during a penetration testing process. (3)
3. Discuss the tools and methods for finding subdomains of a target site. (3)
4. What is SYN flood in DoS attacks? (3)
5. What is XSS and how can it be used against web servers? (3)
6. Explain 'Vulnerability Priority Rating (VPR)' and how it differs from CVSS. (3)

OR

Express the common query types in nslookup and their retrieved information. (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. What is privilege escalation, and why is it a critical step in the hacking process? (5)
8. What is privilege escalation in the context of hacking? (5)
9. Explain the concept of insecure cryptographic vulnerabilities and their impact. (5)

OR

Explain the further classifications of symmetric key cryptography, including its divisions into classical cryptography and modern cryptography. (5)

****