17500

LIBRARY
Brainware University
Barasat, Kolkata -700125

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(ANCS)-Hons-2024
Course Name – Vulnerability Analysis and Penetration Testing
Course Code - BNC37104 (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) Predict the first phase in the penetration testing process, involving gathering information about the target system or network.

a) Reconnaissance b) Reporting
c) Privilege Escalation d) Gaining Access

(ii) Predict the name of the database to find Proof of Concepts (PoCs) that demonstrate the exploitation of vulnerabilities.

a) NVD (National Vulnerability Database) b) Vulnerability Research Framework (VRF)
c) Vulnerability Scoring System d) Exploit-DB

(iii) Match with the port that a WHOIS server listens on.

a) 43 b) 53
c) 443 d) 80

(iv) Recall the Linux tool used to extensively enumerate SMB shares and user information.

a) nmap b) smbclient
c) enum4linux d) dig

(v) Identify the Nmap timing template representing the most aggressive scan speed.

a) -T0 b) -T2
c) -T4 d) -T5

(vi) Identify the phase focused on erasing evidence to avoid detection.

a) Covering Tracks b) Reconnaissance
c) Enumeration/Scanning d) Gaining Access

(vii) Match the protocol type vulnerable to sniffing when unencrypted.

a) HTTPS b) SMTP
c) FTP d) SSH

(viii) Predict the encryption algorithm that employs a 128-bit block size and supports 256-bit keys.

a) DES
b) 3DES
c) AES
d) RC4

(ix) Predict the TLS version now considered insecure and recommended for disabling.

a) TLS 1.3
b) TLS 1.2
c) TLS 1.1
d) TLS 1.0

(x) Recall the sequence that comments out the remainder of a MySQL query during SQL injection.

a) --
b) /* */
c) #!
d) ;#

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Classify the phases followed by penetration testers during a typical assessment. (3)
3. Illustrate the process of DNS Zone Transfer and its purpose in enumeration. (3)
4. Infer the consequences of a DNS Amplification Attack on web servers. (3)
5. Demonstrate the steps involved in a Time-based Blind SQL Injection attack. (3)
6. Classify the enumeration techniques that attackers use to identify system vulnerabilities. (3)

OR

Analyze how SNMP assists in enumeration and describe the role of SNMP traps. (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. Discuss enumeration techniques using protocols such as LDAP, SNMP, NetBIOS, SMB, and NTP. (5)
8. Discuss the phases of a web server attack methodology. (5)
9. Evaluate different privilege escalation techniques. (5)

OR

Compare and contrast the CVSS and VPR frameworks for vulnerability scoring in terms of methodology, applicability, and real-world effectiveness. (5)

****

LIBRARY
Brainware University
Barasat, Kolkata -700125