BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – M.Sc.(ANCS)-2021/M.Sc.(ANCS)-2022/M.Sc.(ANCS)-2023
Course Name – Vulnerability Analysis and Penetration Testing
Course Code - MNCS302
(Semester III)

Full Marks : 60 **Time : 2:30 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 15=15

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

(i) Recognize the primary purpose of a firewall in network security.

a) Data encryption b) Prevent unauthorized access
c) Enhance network performance d) Develop software applications

(ii) Define the "black box" penetration testing approach.

a) Testing with no prior knowledge b) Testing with full system information
c) Testing with a red team d) Testing without external consultants

(iii) Identify the enumeration technique that focuses on querying Domain Name System (DNS) servers to gather information about hosts on a network.

a) Banner grabbing b) DNS enumeration
c) SNMP enumeration d) LDAP enumeration

(iv) Identify the methods and tools used in "DoS/DDoS attacks" and their potential consequences.

a) To gain unauthorized access to a system b) To encrypt network traffic
c) To overwhelm a system or network to make it unavailable d) To create a secure communication channel

(v) Define the role of "honeypots" in cybersecurity and their benefits.

a) To capture network packets b) To block all network traffic
c) To act as decoy systems to attract and study attackers d) To launch DDoS attacks

(vi) Which of the following would you determine as a well-known tool used for carrying out vulnerability scanning comprehensively?

a) Wireshark b) Nessus
c) Nmap d) Metasploit

(vii) Determine which of the following can replicate itself.

a) Spyware b) Trojan
c) Virus d) Worm

(viii) Determine what does the term "footprinting" refer to?

a) Injecting malicious code into a database

b) Encrypting SQL queries

c) Collecting information about a target system

d) Hiding data within images

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

a) msfvenom

b) Metasploit

c) Burp Suite

d) Nmap

(x) Define the key component of the reconnaissance phase.

a) Covering Tracks

b) Information Gathering

c) Privilege Escalation

d) Exploitation

(xi) Select a session ID.

a) A unique identifier for a user's session

b) A user's password

c) A user's email address

d) A database record

(xii) Select the most accurate definition of Cross-Site Request Forgery (CSRF).

a) An attack where malicious scripts are injected into web pages

b) An attack where a user is tricked into submitting a malicious request to a site they are authenticated to

c) An attack where an attacker exploits vulnerabilities in file uploads

d) An attack that targets the server's ability to process URLs

(xiii) Apply the correct measure to mitigate HTTP Host Header attacks in a web application.

a) Allow multiple values for the Host header to handle a variety of domains

b) Perform strict validation on the Host header value to match expected domain names

c) Use wildcard DNS entries to resolve any incoming Host headers

d) Implement cookie-based session management for all users

(xiv) Classify the usage of UNION SQL injection in database exploitation.

a) It is used to execute operating system commands

b) It is used to combine the results of two or more SELECT queries into a single result set

c) It is used to exploit file upload vulnerabilities

d) It allows attackers to dump user credentials

(xv) Select the primary reason for using SQLMap in automated SQL injection testing.

a) It automatically scans web servers for XSS vulnerabilities

b) It simplifies the process of detecting and exploiting SQL injection flaws

c) It assists in manipulating server-side templates

d) It analyzes HTTP headers for missing security flags

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe the purpose of network scanning and enumeration in cybersecurity. (3)
3. Explain Types of scans: NULL, FIN, and Xmas scans, and their open port identification. (3)
4. How can hackers perform Directory Traversal Attacks? (3)
5. What is the purpose of the following commands: msf> show exploits and msf> show payloads? (3)
6. Analyze input validation. (3)

OR

Analyze the process of error-based SQL injection and its implications for database security. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. What is privilege escalation, and why is it a critical step in the hacking process? (5)

8. Compare and contrast the functionalities of amass and subfinder for subdomain enumeration. (5)

9. Analyze the TCP SYN scanning technique. (5)

10. Discuss how HTTP response splitting can be exploited to perform XSS attacks. (5)

11. Evaluate the implications of Remote File Inclusion (RFI) vulnerabilities on a web application's security posture. (5)

12. Analyze the impact of web cache poisoning attacks on web applications. (5)

OR

Analyze the exploitation process of Local File Inclusion (LFI) vulnerabilities. (5)

****