F/E/TY

Reg. No:

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

Final Assessment Test – April 2025

Course: BCSE319L - Penetration Testing and Vulnerability Analysis
Slot: F1
Class NBR(s): 1983/1988
Max. Marks: 100
Time: Three Hours

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions
(10 X 10 = 100 Marks)

1. a) List and explain the five stages of Hacking. [5]
   b) Detail the steps involved in Manual Vulnerability Assessment. [5]

2. a) How a DNS query is resolved? Provide an insight on the use of various servers, DNS record types and files that are used for this purpose. [5]

   b) Illustrate how you will perform the following using DNSRECON tool [5]
   - Provide the dnsrecon command that specifically targets SRV record retrieval for the example.com domain.
   - Perform reverse lookup on all IP addresses within the 172.224.80.115/24 network range.
   - Perform DNS enumeration using a target nameserver ns2.bluehost.in.
   - Perform zone transfer on the domain example.com.
   - Brute force subdomains using a wordlist for a domain example.com.

3. Illustrate how a hacker can perform man in the middle attack using ARP spoofing technique. Provide the counter measures for this attack.

4. Detail the use of the following tools for offline password cracking. Support your explanation with commands.
   - John the Ripper
   - Hashcat

5. Elaborate on WPA handshake process and detail how the following tools can be used to crack the Wi-Fi password by capturing the WPA handshake file.
   - Airmon-ng
   - Airodump-ng
   - Aireplay-ng
   - Aircrack-ng

6. a) Provide an insight into the usefulness of Metasploit's inbuilt PostgreSQL database support. Provide atleast five commands. [5]

b) What is a Meterpreter session? Describe with an example on how do you establish a Meterpreter session after exploiting a target system? [5]

7. Explain with sample html code on how a click jacking attack is performed using iframes. List the ways to prevent this attack.

8. A form receives user input in a textbox and supplies the value directly to a SQL query on the server-side script as shown below. (userinput in the SQL query is the value received from the textbox)

```
$sql = "SELECT username, salary FROM employee WHERE username = '". $userinput . "'";
```

a) Elaborate on how a hacker can manually exploit this weakness to get more control over your database. [5]

b) Provide commands and illustrate how a tool like SQLMAP can be used for dumping passwords from the database. [5]

9.a) Analyse the provided C code snippet. Identify the potential vulnerability a malicious actor could exploit and detail the preventative measures necessary to mitigate this risk.

```
#include <stdio.h>
#include <string.h>

void process_input(char *user_input) {
 char local_buffer[8];
 strcpy(local_buffer, user_input);
 printf("Buffer content: %s\n", local_buffer);
}

int main (int argc, char *argv[]) {
 if (argc != 2) {
  printf("Usage: %s <input>\n", argv[0]);
  return 1;
 }
 process_input(argv[1]);
 printf("Program completed successfully.\n");
 return 0;
}
```

OR

9.b) Provide a comparative analysis of the following Wi-Fi security protocols, detailing their respective strengths and weaknesses

- WEP
- WPA
- WPA2

10.a) Illustrate how to perform Web Application enumeration using the following techniques

i. Viewing Response Headers [5]
ii. Inspecting Page Content [5]

OR

10.b) Elaborate on the use of the following tools for performing Web Application vulnerability scanning. Provide the steps and configuration required to perform the scan.

i. Nikto [5]
ii. Nessus [5]

⇔⇔⇔ F/E/TY ⇔⇔⇔