30. a.	Explain in alternative description for the role of shellcode runners in offensive security testing and elaborate on the concept.	12	4	3	5
	(OR)				
b.	Explain in detail, about examining the potential threats and difficulties related to the usage of shellcode runners.	12	4	3	5
31. a.i.	Can you provide an explanation of the primary function and working mechanism of antivirus software?	6	3	4	1
ii.	Explain the significance of keeping antivirus databases up-to-date and the potential outcomes of failing to update the database.	6	3	4	1
	(OR)				
b.i.	Discuss the technique used in a process injection attack with C#.	6	2	4	1
ii.	Explain the technique used in DLL injection attack with C#.	6	3	4	1
32. a.i.	Explain how to find the antivirus signature of a detected file and use it to add the file to a white list?	6	3	5	1
ii.	Explain the distinction between encoders and encrypters when creating malware.	6	3	5	1
	(OR)				
b.i.	Explain the method employed in antivirus evasion using metasploit and its effectiveness in bypassing antivirus detection.	6	4	5	1
ii.	Explain what is living off the land binaries (LOL Bins) are in offensive security testing and give an example of how they can be utilized?	6	4	5	1

* * * * *

Reg. No.														

B.Tech. DEGREE EXAMINATION, JUNE 2023

Sixth Semester

18CSE412J – OFFENSIVE SECURITY

(For the candidates admitted during the academic year 2018-2019 to 2021-2022)

Note:

(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

(ii) **Part - B & Part - C** should be answered in answer booklet.

Time: 3 hours Max. Marks: 100

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

		Marks	BL	CO	PO
1.	What is the Unix built-in command to get the manual pages of a command or utility in Unix? (A) Help (B) –h (C) Man (D) –?	1	1	1	1
2.	What are the commands available to get the location of an installed application in Unix? (A) Whichis and whereis (B) Whereis and which (C) Whichis and whatis (D) Whereis and whatis	1	1	1	1
3.	What is the usage of this command "pwd"? (A) Printing command to print a current working document (B) Print working directory (C) Print working drive (D) Print working disk	1	1	1	1
4.	What are some of the windows-API functions? (A) Create Process, create file, get message (B) Func create process, func create file (C) Routines, system calls, DLLs (D) User32, DLL, MSDRT.DLL, Kernal32.DLL	1	2	1	1
5.	What is the port number of DNS and TELNET? (A) 53 and 23 (B) 53 and 22 (C) 52 and 22 (D) 52 and 23	1	1	2	1
6.	What is the primary use of NMap? (A) Port scanning (B) Website hacking (C) Password cracking (D) Social engineering	1	2	2	5
7.	What is the purpose of HTML smuggling attacks? (A) To bypass network security devices (B) To compressive browsers (C) To perform DDoS attacks (D) To block network traffic	1	2	2	1

8. What is the purpose of UBA macros in offensive security testing? 1 3 2 1
   (A) To create payloads for exploitation
   (B) To perform network reconnaissance
   (C) To brute force passwords
   (D) To automate tasks in Microsoft office applications

9. What technique is utilized to run shell code through dotnet payloads? 1 3 3 5
   (A) VBA shell code runner
   (B) Power shell shellcode runner
   (C) DOTNET-TO-JSCRIPT
   (D) JSCRIPT payload execution

10. Which payload execution technique requires both stages of the payload to be sent in the same request? 1 2 3 1
   (A) Staged payload
   (B) Non-staged payload
   (C) Reverse payload
   (D) Bind payload

11. What is the primary benefit of utilizing power shell for offensive security testing? 1 3 3 1
   (A) Powershell is easy to use and requires no programming skills
   (B) Powershell scripts can be used to execute malicious commands
   (C) Powershell is cross-platform and can be used on windows linux and mac OS
   (D) Powershell is faster than other scripting languages

12. What is the method used to run harmful code in a genuine process? 1 2 3 1
   (A) Process injection
   (B) DLL injection
   (C) Reflective DLL injection
   (D) Classic DLL injection

13. What is the primary purpose of antivirus software? 1 2 4 1
   (A) To prevent all types of cyber attacks
   (B) To detect and remove malware
   (C) To improve the performance of the system
   (D) To encrypt all files on the system

14. What is the name of the process injection attack type that injects code into a remote process among the following options? 1 2 4 1
   (A) Code injection
   (B) Thread injection
   (C) Remote injection
   (D) Process DLL injection

15. Which of the following is an example of a process injection attack? 1 3 4 1
   (A) SQL injection
   (B) Cross-site scripting (XSS)
   (C) Dynamic-link library (DLL) injection
   (D) Man-in the middle (MITM) attack

16. Pick the rationale behind identifying the antivirus signature from a flagged file? 1 3 4 1
   (A) To delete the file
   (B) To white list the file
   (C) To block the file
   (D) To rename the file

17. What role do encoders play in offensive security testing? 1 2 5 1
   (A) To encrypt data
   (B) To compress data
   (C) To encode payloads to avoid detection by antivirus software
   (D) To decode payloads on the target system

18. What objective is pursued through a windows credentials attacks? 1 2 5 1
   (A) To gain access to sensitive information stored on the target system
   (B) To delete files on the target system
   (C) To encrypt data
   (D) To compress data

19. What objective is aimed for an applocker bypass attack? 1 2 5 5
   (A) To bypass antivirus detection
   (B) To execute payloads on the target system
   (C) To gain access to sensitive information stored on the target system
   (D) To bypass applocker policies and run unauthorized programs

20. What role does an encoder serve in the development of malware? 1 3 5 1
   (A) To encrypt the payload
   (B) To obfuscate the code
   (C) To bypass a firewall
   (D) To create a rootkit

PART – B (5 × 4 = 20 Marks) Marks BL CO PO
Answer **ANY FIVE** Questions

21. What are reconnaissance attacks? 4 2 1 1

22. Difference between the red team and the blue team. 4 3 1 5

23. Explain the process of payload creation with metasploit. 4 3 2 5

24. Difference between staged and nonstaged metasploit payload. 4 3 2 5

25. What is process injection in malware analysis? 4 2 3 1

26. What is the difference between process hollowing and process injection? 4 3 4 1

27. Define applocker and technique to bypass it. 4 2 5 5

PART – C (5 × 12 = 60 Marks) Marks BL CO PO
Answer **ALL** Questions

28. a. Explain in detail the types of penetration testing and its testing style. 12 3 1 1

(OR)

   b. Explain in detail for the following 3 1 1
      (i) Windows API 6
      (ii) Services functions and routines in windows operation system 6

29. a. Explain the HTML smuggling attack used by downloaders and how it can be used to bypass security measures, ways to prevent hem. 12 4 2 5

(OR)

   b. Explain the metasploit framework and its role in penetration testing and ethical hacking. 12 4 2 5