Reg. No.															

B.Tech. DEGREE EXAMINATION, MAY 2024
Fifth & 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

	Question	Marks	BL	CO	PO
1.	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) User 32, DLL, MSVRT.DLL, kernel 32.DLL	1	1	1	1
2.	There long beeps during the power on self test indicate ______. (A) Mouse error (B) Program error (C) RAM module error (D) Keyboard error	1	1	1	1
3.	What port numbers do SMTP and POP3 use _______. (A) 25 and 110 (B) 110 and 25 (C) 111 and 25 (D) 110 and 26	1	1	1	1
4.	______ protocol allows devices to be managed and monitored remotely. (A) NetBIOS enumeration (B) SNMP enumeration (C) LDAP enumeration (D) NTP enumeration	1	1	1	1
5.	______ identifying the users on the target system. (A) Vulnerability scanning (B) Port scanning (C) User enumeration (D) Service enumeration	1	1	2	1
6.	_______ is used for web application security testing. (A) Burp suite (B) Scout suite (C) Suite (D) Testing tool	1	1	2	1
7.	_______ is the command line utility for transferring data from or to a server using the supported protocols. (A) WGET (B) NIKTO (C) CURL (D) GET	1	1	2	1
8.	______ are useful when there is limited space to work with or when speed is critical. (A) Staged payload (B) Customized payload (C) Restricted payload (D) Non staged payload	1	1	2	1

9. Portable executable injection and loading does not require the ______ to be stored on disk. 1 1 3 1

(A) SQL (B) DDL
(C) DSL (D) HTML

10. ______ isolate and analyze suspicious files, URLs, or email attachments to detect and prevent HTML smuggling attacks. 1 1 3 1

(A) Sand boxing (B) White boxing
(C) Black boxing (D) Grey boxing

11. ______ identify weakness in a systems security by simulating real world attacks. 1 1 3 1

(A) VBA macros (B) CURL
(C) Shellcode runners (D) WGET

12. ______ is used to inject malicious code into running processes. 1 1 3 1

(A) SQL injection (B) Server injection
(C) DLL injection (D) Process injection

13. _____ is the first virus. 1 1 4 1

(A) Creeper (B) Code red
(C) Root kit (D) Stux net

14. Regular database updates help antivirus software maintain ________. 1 1 4 1

(A) Reduce false positives and reduce detection rate (B) Reduced false positive and high detection rate
(C) High false positives and high detection rate (D) High false positives and reduced detection rate

15. ______ in which the attackers send deceptive emails, messages or website that trick users into revealing their login credentials 1 1 4 1

(A) Brute force attacks (B) Keyloggers
(C) Credential dumping (D) Phishing attacks

16. ______ is the first phase of ethical hacking. 1 1 4 1

(A) ARP poisoning (B) Enumeration
(C) Foot printing (D) DNS poisoning

17. ______ is designed to prevent unauthorized software. 1 1 5 1

(A) App locker (B) Mobil locker
(C) LOL bins (D) Software locker

18. DNS translates a domain name to ________. 1 1 5 1

(A) Hex (B) Binary
(C) IP (D) URL

19. ______ protects data from modification by unknown users. 1 1 5 1

(A) Confidentiality (B) Integrity
(C) Authentication (D) Non repudiation

		Marks	BL	CO	PO
20.	______ is not the strongest security protocol. (A) HTTPS (B) SSL (C) SFTP (D) SMTP	1	1	5	1

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

		Marks	BL	CO	PO
21.	A company shares all the information with its testers. What type of penetration testing does the tester use to find the vulnerability? Write a short note on the type of penetration testing that the tester opted for.	4	2	1	1
22.	Compare active and passive reconnaissance. Give examples.	4	4	1	1
23.	Brief about persistence techniques.	4	1	2	1
24.	Write the steps of how autoruns are used to remove malware.	4	2	2	1
25.	Illustrate how the HTML smuggling works. Give examples.	4	2	3	1
26.	Write short notes on the basic function of the antivirus engine.	4	1	4	1
27.	What are living off the land binaries (LOL bins) in offensive security testing and given an example of how they can be utilized.	4	1	5	1

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

		Marks	BL	CO	PO
28. a.	Explain with examples the following Linux commands (i) ls command (ii) rm command (iii) echo command (iv) df command (v) chmod command (vi) apt-get command	12	3	1	5
	(OR)				
b.i.	How does the windows registry work and when to use the windows registry?	6	2	1	1
ii.	Discuss the services, functions and routines in windows operating system.	6	2	1	1
29. a.i.	What is the Metasploit frame work?	4	1	2	1
ii.	Write the syntax of each step involved in creating and executing payloads in Metasploit.	8	3	2	5
	(OR)				
b.	Explain in detail about persistence techniques with example commands.	12	3	2	1
30. a.i.	Write the VBA Macros code to open a program.	6	3	3	5

	ii.	Write the VBA Macros code for workbook_open_close.	6	3	3	5
		(OR)				
	b.	What is social engineering? Discuss in detail the steps used by SET to clone to site in Kali Linux.	12	2	3	5
31.	a.	Discuss in detail the techniques used in DLL injection attacks.	12	2	4	1
		(OR)				
	b.	How is open source intelligence used? Find the difference between passive versus active OSINT.	12	2	4	1
32.	a.	Describe the process of finding the antivirus signature from the detected file.	12	2	5	1
		(OR)				
	b.	Discuss in detail the following with examples		2	5	1
		(i) encoders	6			
		(ii) encrypters	6			

* * * * *