Reg. No.															

B.Tech. DEGREE EXAMINATION, DECEMBER 2023

Sixth Semester

18CSE412J – OFFENSIVE SECURITY

(For the candidates admitted from the academic year 2020-2021 & 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 command to remove a directory which contains files inside? 1 1 1 1
   (A) Rmdir _rf "directory name" (B) Rmdir _f "directory name"
   (C) Rmk _rf "directory name" (D) Del_f "directory name"

2. How to determine the file type of a file? 1 1 1 1
   (A) "filename" _help (B) File "filename" -help
   (C) File "filename" (D) Man "filename"

3. What are the multiple options available to create a file in Unix? 1 1 1 1
   (A) Vm, echo, touch, nano (B) Vim, touch, nano, echo
   (C) Vim, cat, touch, create, "filename" (D) Mkdir, vm, create, "filename", cat

4. What is PID value in Unix and windows operating? 1 2 1 1
   (A) Program ID (B) Process ID
   (C) Process-list ID (D) Performance ID

5. What is the port number of SSH and FTP? 1 1 2 1
   (A) 21 and 22 (B) 22 and 21
   (C) 23 and 22 (D) 21 and 23

6. Which tool is used for web server vulnerability scanning? 1 2 2 3
   (A) Nmap (B) Metasploit framework
   (C) Nikto (D) Netcat

7. What is the purpose of creating custom malware for phishing attacks? 1 2 2 1
   (A) To steel user credentials (B) To perform network reconnaissance
   (C) To brute force passwords (D) To perform DDoS attacks

8. What is the primary use of power shell in offensive security testing? 1 3 2 1
   (A) To perform web server vulnerability scanning (B) To analyze custom malware for phishing attacks
   (C) To automate tasks on windows systems (D) To analyze network traffic

9. What is the best way to protect against phishing attacks from initial point of contact? 1 3 3 5

(A) User strong and unique password
(B) Install antivirus software on all device
(C) Verity the authenticity of emails and links
(D) Use a VPN to encrypt network traffic

10. What technique is employed to implement shellcode through Jscript? 1 2 3 1

(A) VBA shellcode runner
(B) Powershell shellcode runner
(C) DOTNET-TO-JSCRIPT
(D) JSCRIPT payload execution

11. What is process injection? 1 3 3 1

(A) A technique used to load a DLL into memory without using the standard windows API functions
(B) A technique used to bypass security measures and gain authorized access to a system or network
(C) A technique used to encrypt files on a computer or network
(D) A technique used to block incoming network traffic

12. What does an update to the antivirus database mean? 1 2 3 1

(A) To add new features to the antivirus software
(B) To improve the performance of the antivirus software
(C) To update the list of known malware signatures
(D) To block all incoming network traffic

13. What is the method employed in DLL injection attacks among the following options? 1 2 4 1

(A) Overwriting system files
(B) Loading malicious code into memory
(C) Disabling antivirus software
(D) Code injection

14. What is a preventive measure that can be implemented to thwart process injection attacks among the following options? 1 2 4 1

(A) Implementing firewalls and intrusion detection systems
(B) Using recuse passwords for user accounts
(C) Using code-signing certificates to verify the authenticity of processes
(D) Keeping antivirus software up-to-date

15. What is a typical objective of both process and DLL injection attacks among the following options? 1 3 4 1

(A) Stealing sensitive data from the machine via the target process
(B) Overwriting system files
(C) Disabling antivirus software
(D) Deleting system files

16. What is the main purpose of using encrypters in offensive security testing? 1 3 4 1

(A) To encrypt sensitive data
(B) To decrypt sensitive data
(C) To encrypt payloads to avoid detection by antivirus software
(D) To decrypt payloads on the target system

17. What role do minikatz and memory dumping play in offensive security testing? 1 2 5 1

(A) To bypass antivirus detection
(B) To execute payloads on the target system
(C) To gain access to sensitive information stored in memory and to recover passwords and credentials
(D) To delete files on the target system

18. What are living off the land binaries? 1 2 5 1

(A) Malicious executables that are not detected by antivirus
(B) Legitimate executables used of malicious purpose
(C) A type of encryption algorithm
(D) A type of encoding technique

19. How would you define an antivirus signature? 1 2 5 5

(A) A unique identifier for a virus
(B) A way of authenticating users
(C) A type of encryption algorithm
(D) A tool for bypassing firewalls

20. Can you describe what the VBA shellcode runner is? 1 3 5 1

(A) A tool used to deliver malware via Microsoft office document
(B) A tool used to scan for vulnerabilities in windows systems
(C) A tool used to perform network reconnaissance
(D) A tool used to automate tasks in Microsoft office applications

PART – B (5 × 4 = 20 Marks)

Answer **ANY FIVE** Questions

		Marks	BL	CO	PO
21.	Write an IP grabber script in bash program and explain each step.	4	2	1	1
22.	What is enumeration in hacking?	4	3	1	5
23.	What is Nmap and justify why we need it in our network.	4	3	2	5
24.	Explain HTMl smuggling in detail.	4	3	2	5
25.	What is process hollowing?	4	2	3	1
26.	What is OSINT framework in cyber security?	4	3	4	1
27.	What is living off the land binaries?	4	2	5	5

PART – C (5 × 12 = 60 Marks)

Answer **ALL** Questions

		Marks	BL	CO	PO
28. a.	Explain in detail for the following		3	1	1
	(i) Windows API	6			
	(ii) Windows process, threads, jobs	6			

(OR)

b. Explain in detail the “Cyber kill chain” stages. 12 3 1 1

29. a. Explain the concept of staged and non-staged payloads in offensive security testing. 12 4 2 5

(OR)

b. Explain how VBA macros can be used offensively to deliver malware or steal sensitive information, explain how to detect and prevent them. 12 4 2 5

30. a. Explain the differences and similarities among different types of shellcode runners, such as the VBA shellcode runner, powershell shellcode runner, Jscript payload execution, Dotnet-to-Jscript. 12 4 3 5

(OR)

b. Explain powershell shellcode runner in detail and proposing measures for identifying and mitigating such attacks? 12 4 3 5

31. a.i. Explain the purpose and working of the process injection technique. 6 3 4 1

ii. What is DLL injection, and how can it be used for offensive security testing purpose? 6 3 4 1

(OR)

b.i. How can a process injection attack with C# be detected and mitigates? 6 3 4 1

ii. List some of the prevalent techniques employed by antivirus software for ensuring their databases are current. 6 3 4 1

32. a.i. Explain the differences between encoders and encrypters in offensive security testing and given an example of how both can be implemented. 6 3 5 1

ii. Define applocker and the technique to bypass it. 6 3 5 1

(OR)

b.i. Explain the objective of applocker in windows operating systems and how it can be circumvented in offensive security testing. 6 4 5 1

ii. Explain mimikatz and its function of offensive security testing. 6 4 5 1

* * * * *