28. a.	Explain the different types of security policies that can be used to control, who can get into computer systems and see the information they hold.	10	2	3	1
	(OR)				
b.	Describe the accepted design principles for security measures to safeguard computer systems form various threats?	10	2	3	1
29. a.	What are the techniques used in network to obtain the information. Describe any four Kali OS information gathering tools.	10	2	4	1
	(OR)				
b.	As a penetration testers, explain how penetration testing is done and also discuss how data is protected during and after penetration testing.	10	2	4	1
30. a.	Explain buffer overflow attack with a C program. Discuss, how a stack buffer overflow attack is implemented.	10	2	5	1
	(OR)				
b.	With a C program, explain exec ( ) system call for executing the process. Illustrate the exec ( ) s/m call with output execution.	10	2	5	1

* * * * *

Reg. No.															

B.Tech. DEGREE EXAMINATION, NOVEMBER 2022
Sixth/ Seventh Semester

18CSE478T – OPERATION SYSTEM SECURITY
(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

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** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

PART – A (25 × 1 = 25 Marks)
Answer **ALL** Questions

		Marks	BL	CO	PO
1.	System that permits untrusted processes to modify protection state. (A) Discretionary access control (B) C-list (C) Access control list (D) Protection domain	1	1	1	1
2.	The model that defines the set of software and data upon which the system depends for correct enforcement of security goals (A) SSH model (B) Trust model (C) Thrust model (D) Threat model	1	1	1	1
3.	The operation that determine what subjects can modify on associated objects. (A) Modify (B) Change (C) Own (D) Add	1	1	1	1
4.	_____ take interfaces inputs and converts these to query for the reference monitors policy store. (A) Process identity (B) Object references (C) Authorization module (D) Reference monitor	1	1	1	1
5.	The state that enables a secure operating system to change the label of a process or a system resource. (A) Labeling state (B) Transition state (C) Protection state (D) Access state	1	1	1	1
6.	Which is not true about storage management? (A) Storage allocation (B) Free space management (C) Disk scheduling (D) Offers the user access to various resources the network shares	1	1	2	1
7.	Which statement is false about the need of thread? (A) Context switching is faster when working with threads (B) Threads cannot share the common data (C) Takes less time to create a new thread than a process (D) Takes less time to terminate a thread than a process	1	1	2	1

8. In which of the memory allocation techniques internal fragmentation can rise — 1 1 2 1
   (A) Segmentation (B) Paging
   (C) Fragmentation (D) Memory allocation

9. Which one is not a "Attack replication vector". — 1 1 2 1
   (A) Virus (B) DMA
   (C) Mass mail (D) SNMP

10. Misuse of system services and network connections to put user in trouble — 1 1 2 1
   (A) System threats (B) Program threats
   (C) Process threats (D) DoS attack

11. Requires that a computer system be able to verify the identity of a user. — 1 1 3 1
   (A) Integrity (B) Authenticity
   (C) Confidentiality (D) Availability

12. Which is not true about segmentation? — 1 1 3 1
   (A) Lends itself to the implementation of protection and sharing policies
   (B) An entity capable of accessing objects
   (C) Gives user view of the process which paging does not give
   (D) A memory management technique

13. The user can change the access rights granted to other users. — 1 1 3 1
   (A) Execution mode (B) User mode
   (C) Changing protection mode (D) Rewrite mode

14. Access can be provided to the individual users who are designated by user is — 1 1 3 1
   (A) Specific user (B) User groups
   (C) All (D) Owner

15. When multiple categories or levels of data are defined, the requirement is referred to as — 1 1 3 1
   (A) Multiple security (B) Multilevel security
   (C) Single level (D) Hierarchical security

16. The security rules are enforced on every access, not just, for example, when a file is opened — 1 1 4 1
   (A) Reference monitor (B) Verifiability
   (C) Isolation (D) Complete mediation

17. A mapping range of roughly 6500 vulnerabilities is included in the vulnerability tool. — 1 1 4 1
   (A) Arachni (B) Acunetix
   (C) Netsparker (D) Nmap

18. The exploitation tool used to test web applications for bugs, errors, and vulnerabilities related to command injection attacks. — 1 1 4 1
   (A) Commix (B) Cisco-ocs
   (C) Cisco-torch (D) Crackle

19. Which one is forensic tool in kali linux? — 1 1 4 1
   (A) Pdf-parser (B) Wire shark
   (C) Xplico (D) Guymager

20. The command used to list out all hidden files of a directory. — 1 1 4 1
   (A) ls (B) ls -l
   (C) ls -k (D) ls -h

21. Which of the following is used to crack the security of a system and gain access for stealing data? — 1 1 5 1
   (A) Online attack (B) System hacking
   (C) Offline attack (D) Port scamming

22. Where are user crontab files stored? — 1 1 5 1
   (A) /etc/crontab (B) /var/spool
   (C) ~/.cron (D) /var/spool/cron

23. To avoid attacks like SQL injection, vulnerability scanning is implemented on _____. — 1 1 5 1
   (A) Cloud (B) Host
   (C) Database (D) Network

24. An approach is to allow a user to lock the entire file when it is to be updated. — 1 1 6 1
   (A) Saltzer and Schroeder (B) Brute-force
   (C) Open source (D) Racing

25. Which is not the mode of ring protection approach? — 1 1 6 1
   (A) Kernel (B) Executive
   (C) Supervisor (D) Object

PART – B (5 × 10 = 50 Marks) — Marks BL CO PO
Answer **ALL** Questions

26. a. Assume that you have been assigned as a trusted administrator and you have given with the task of changing the required protection system. With illustration, explain different state representation. — 10 2 1 1

(OR)

   b. It is your responsibility as an operating system developer to plan and build a secure OS what are the evaluation standard to be taken into account, and explain how the system is evaluated. — 10 2 1 1

27. a. Explain memory management strategies. Illustrate how memory protection is done in operating system. — 10 2 2 1

(OR)

   b. Explain the ways in which the hardware and architecture supports the OS security. — 10 2 2 1