

ADVANCED CERTIFICATE IN INFORMATION SECURITY (ACISE)

Term-End Examination

December, 2022

OSEI-044 : SERVER SECURITY

Time : 2 hours

Maximum Marks : 50

Note :

*Section A : Answer **all** the objective type questions.*

*Section B : Answer **all** the very short answer type questions.*

*Section C : Answer any **two** out of three short answer type questions.*

*Section D : Answer any **two** out of three long answer type questions.*

SECTION A

*Attempt **all** the questions.*

$10 \times 1 = 10$

1. There are _____ major ways of stealing email information.

- (a) 2
- (b) 3
- (c) 4
- (d) 5

2. _____ is a famous technological medium for the spread of malware, facing problems of spam and phishing attacks.
- (a) Cloud
 - (b) Pen drive
 - (c) Website
 - (d) Email
3. Which of the following is **not** an appropriate method of defacing web server ?
- (a) Fetching credentials through MiTM
 - (b) Brute-Forcing Admin Password
 - (c) IP address spoofing
 - (d) DNS attack through cache poisoning
4. Which of the following is **not** an appropriate method of defacing web server ?
- (a) Mail server intrusion
 - (b) Web application bugs
 - (c) Web share misconfiguration
 - (d) Sessions Hijacking
5. Which among them has the strongest wireless security ?
- (a) WEP
 - (b) WPA
 - (c) WPA2
 - (d) WPA3
6. _____ is an old IEEE 802.11 standard from the year 1999.
- (a) WPA2
 - (b) WPA3
 - (c) WEP
 - (d) WPA

- 7.** What is life cycle risk assessment ?
- (a) Risk assessment before the system has been deployed
 - (b) Risk assessment while the system is being developed
 - (c) All
 - (d) None
- 8.** A system resource that has a value and has to be protected is known as
- (a) Asset
 - (b) Control
 - (c) Vulnerability
 - (d) None
- 9.** _____ passwords are next level of security.
- (a) BIOS
 - (b) CMOS
 - (c) SMOS
 - (d) DOS
- 10.** Find out, select and uninstall all _____ programs from your computer.
- (a) useful
 - (b) pre-installed
 - (c) unwanted
 - (d) utility

SECTION B

*Attempt all **five** very short answer type questions. $5 \times 2 = 10$*

- 11.** What is Kerberos ?
- 12.** How secure is WEP ?
- 13.** What is Cross-Site Request Forgery (CSRF) ?
- 14.** What is SQL Injection ?
- 15.** Why is Spam bad ?

SECTION C

*Attempt any **two** out of three short answer type questions.*

$$2 \times 5 = 10$$

- 16.** What is email spoofing and spamming ?
- 17.** What do you see as challenges to successfully deploying/monitoring web intrusion detection ?
- 18.** How can one Block ports on Linux with Iptables ?

SECTION D

*Attempt any **two** out of three long answer type questions.* $2 \times 10 = 20$

- 19.** How does one implement wireless security measures ?
 - 20.** What are the different security extensions available for Linux ?
 - 21.** Write the types of security attacks. Explain in detail about various types of attacks.
-