

NPTEL ASSIGNMENT WEEK :-7
Cyber Security and privacy

1. _____ is a comprehensive system comprising software, encryption techniques, protocols, legal arrangements, and third-party services that facilitate secure communication among users by utilizing digital certificates.

a. Registration authority

b. Public key infrastructure

c. Digital signature

d. Certificate authority

2. Which ring does the kernel, the core of the operating system, typically operate?

a. Ring 2

b. Ring 1

c. Ring 0

d. Ring 3

3. Which of the following statements is not true?

a. Hash functions are one-way.

b. It is possible to attach a message authentication code (MAC) to allow only specific recipients to access the message digest.

c. Hashing functions require the use of keys.

d. Hash functions are used in password verification systems to confirm the identity of the user.

4. Which of the following is not related to defense against rainbow cracking?

a. Password hash salting

b. key stretching

c. Key strengthening

d. Private key encryption

5. Which of the following statements is/are correct?

a. TCP is a connection-oriented protocol, while UDP is connectionless.

b. TCP is comparatively faster than UDP.

c. TCP provides reliable data delivery, while UDP does not.

d. Both a and c.

6. WhichWhich of the following statements about Virtual Private Networks (VPN) are true? of the following statements is/are correct?

NPTEL ASSIGNMENT WEEK :-7
Cyber Security and privacy

- a. A VPN is an encrypted connection over the Internet from a device to a network.
- b. A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic.
- c. A VPN protects its users by masking their IP address.

d. All the above.

7. Endpoint Detection and Response (EDR) solutions are primarily focused on:

- a. Securing network perimeters and firewalls.

b. Protecting individual user devices from threats.

- c. Monitoring and analyzing network traffic for malicious activity.
- d. Providing vulnerability assessments for servers and applications.

8. Cryptojacking is a cyber attack that leverages a victim's computer resources for the attacker's financial gain. Which of the following best describes the attacker's activity in a cryptojacking attack?

- a. Encrypting the victim's data and demanding a ransom payment.
- b. Gaining unauthorized access to the victim's personal information for resale.

c. Silently using the victim's processing power to solve complex mathematical problems for financial reward.

- d. Disrupting the normal operation of the victim's system to cause inconvenience.

9. What kind of infrastructure Advanced Persistent Threat (APT) groups are typically known for targeting?

- a. Personal computers of home users.

b. Critical infrastructure essential for national security (e.g., power grids, communication networks).

- c. Public Wi-Fi networks at cafes or airports.
- d. Outdated operating systems on personal devices of insignificant value

10. Which of the following is NOT one of the stages in the Intrusion Kill Chain framework?

- a. Reconnaissance
- b. Exploitation

c. Cleanup

- d. Command and Control

NPTEL ASSIGNMENT WEEK :-7
Cyber Security and privacy