Cyber Security and Privacy, IIT Madras
Prof. Saji K Mathew

Week 7 Quiz
(All questions carry 1 point each)

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

Ans: b. Public key infrastructure
Explanation: PKI, or public key infrastructure, encompasses everything used to establish and manage public key encryption.

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

Ans: c.Ring 0
Explanation: The kernel requires the highest level of privilege to manage hardware and system resources directly. Therefore, it usually operates in Ring 0, the innermost and most privileged ring.

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.

Ans: c. Hashing functions require the use of keys.
Explanation: Cryptographic hash functions do not require a key. Hashing functions take an input message and produce a fixed-length hash value.

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

Ans: d. Private key encryption
Explanation: Rainbow is a technique used to crack password hashes by precomputing hash values and storing them in a table for quick lookup. Private key encryption is not related to this process.

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.

Ans: d. Both a and c.
Explanation: TCP is reliable, ensures data delivery, and is suitable for applications where accuracy and sequencing are crucial. On the other hand, UDP is faster and suitable for real-time applications that prioritize speed over reliability.

6. Which of the following statements about Virtual Private Networks (VPN) are true?

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.

Ans: d. All the above.
Explanation: VPN is a mechanism for creating secure connections between computing devices and networks.

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.

Ans: b.Protecting individual user devices from threats.
Explanation : EDR specializes in detecting and responding to threats on endpoints like laptops, desktops, mobile devices, ioTs etc.

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.

Ans: c.Silently using the victim's processing power to solve complex mathematical problems for financial reward.
Explanation : Cryptojacking involves secretly using the victim's computer's processing power (CPU or GPU) to solve complex mathematical problems associated with cryptocurrency mining. These computations generate cryptocurrency for the attacker, providing them with financial gain without the victim's knowledge or consent.

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

Ans: b.Critical infrastructure essential for national security (e.g., power grids, communication networks).
Explanation : APT groups typically target high-value targets with significant impact, not personal devices or public Wi-Fi.

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

Ans: c.Cleanup
Explanation : The stages of the Intrusion Kill Chain typically include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. "Cleanup" is not one of the recognized stages.