Name: _____ **Date:** _____

Answer Key: Mr. Robot's Challenge: Your 11th Grade Cybersecurity Logic Quest

Sophisticated threat modeling and cryptographic analysis prepare students for high-stakes digital defense and ethical hacking scenarios in professional environments.

---

1. A network administrator implements a 'Zero Trust' architecture. Which principle best evaluates the core logic of this security model?

Answer: B) Continuous verification of every device and user regardless of location

Zero Trust operates on the principle of 'never trust, always verify,' requiring strict identity verification for every person and device trying to access resources on a private network.

2. A specialized form of 'Social Engineering' that targets high-profile executives through highly customized, deceptive communication is known as _____.

Answer: C) Whaling

Whaling is a specific type of spear-phishing aimed at senior executives (the 'big fish') to steal sensitive corporate data or high-level credentials.

3. In asymmetric encryption, the 'Private Key' is used by the sender to encrypt the message, while the 'Public Key' is used by the recipient to decrypt it.

Answer: B) False

In asymmetric encryption (RSA), the Public Key is used to encrypt data, and only the corresponding Private Key held by the recipient can decrypt it.

4. Analyze the scenario: An attacker exploits a software vulnerability that the developer is not yet aware of. This is categorized as a _____.

Answer: B) Zero-day exploit

A zero-day exploit targets a vulnerability for which no patch or fix exists because the developers have had 'zero days' to address the threat.

5. To protect stored passwords from 'Rainbow Table' attacks, developers add a unique, random string of characters to the password before hashing, called a _____.

Name: _____ **Date:** _____

Answer: C) Salt

Salting involves adding unique data to a password input so that two identical passwords produce different hashes, significantly complicating mass decryption attempts.

6. A 'Honey Pot' is a decoy system designed to lure cyber-attackers to detect, deflect, or study their hacking methods.

Answer: A) True

Honeypots are defensive tools used by security professionals to observe hacker behavior and gather intelligence on new exploit techniques without risking the main production network.

7. Which of the following describes a 'Man-in-the-Middle' (MitM) attack specifically performed via an unencrypted public Wi-Fi access point?

Answer: B) Packet Sniffing

Packet sniffing on unsecured networks allows attackers to intercept and read data packets traveling between a user's device and the internet.

8. When an attacker floods a server with an overwhelming volume of traffic from multiple compromised systems (botnets), it is referred to as a _____ attack.

Answer: A) DDoS

Distributed Denial of Service (DDoS) attacks use multiple sources to crash a service, making it unavailable to legitimate users.

9. In the context of 'Defense in Depth,' which strategy represents a technical/logical control rather than a physical or administrative control?

Answer: A) Implementing an Intrusion Detection System (IDS)

Technical controls use software and hardware (like IDS, firewalls, and encryption) to protect data, whereas badges are physical and policies are administrative.

10. Stuxnet is a historically significant example of malware specifically designed to sabotage industrial control systems (SCADA) rather than just stealing consumer data.

Answer: A) True

Name: _____ **Date:** _____

Stuxnet was a highly complex worm discovered in 2010 that targeted programmable logic controllers used in uranium enrichment facilities, marking a shift toward cyber-physical warfare.