Name: _____ **Date:** _____

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?

A. Implicit trust for all users within the physical perimeter
B. Continuous verification of every device and user regardless of location
C. Focusing exclusively on external firewall strength
D. Granting all employees administrative access to streamline workflow

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

A. DDoS Attacking
B. Script Kiddie
C. Whaling
D. Salting

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.

A. True
B. False

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

A. Brute-force attack
B. Zero-day exploit
C. Cross-site scripting (XSS)
D. Buffer overflow

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

A. Pepper
B. Token
C. Salt
D. Cookie

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

A. True

Name: _____ Date: _____

B. False

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

A. SQL Injection
B. Packet Sniffing
C. Trojan Horse
D. Ransomware

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.

A. DDoS
B. Phishing
C. Rootkit
D. Spyware

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

A. Implementing an Intrusion Detection System (IDS)
B. Requiring employees to wear ID badges
C. Creating an acceptable use policy (AUP)
D. Installing security cameras in the server room

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

A. True
B. False