Name: _____ **Date:** _____

Answer Key: Sophisticated Security: Stuxnet to Social Engineering 9th Grade Quiz

Learners develop critical defense intuition by analyzing complex attack vectors like APTs, zero-day vulnerabilities, and behavioral psychology used in modern breaches.

---

1. A threat actor uses a previously unknown vulnerability in a major operating system to bypass security. Because the developer has zero days to fix it, this is called a:

Answer: B) Zero-day exploit

A zero-day exploit targets a software flaw that is unknown to the vendor, leaving no time for a patch to be created before exploitation.

2. The primary goal of an Advanced Persistent Threat (APT) is typically to cause immediate system crashes rather than long-term data exfiltration.

Answer: B) False

APTs are characterized by their stealth and longevity; they aim to remain undetected for long periods to steal sensitive information.

3. Which specific tactic involves an attacker following an authorized person into a secure building without scanning their own badge?

Answer: C) Tailgating

Tailgating is a physical social engineering technique where an unauthorized person gains access to a restricted area by following closely behind someone with legitimate access.

4. In the context of the 'Stuxnet' worm, which infrastructure component was specifically targeted to cause physical damage through digital manipulation?

Answer: B) Programmable Logic Controllers (PLCs)

Stuxnet targeted industrial PLCs to sabotage centrifuges, demonstrating how digital code can impact physical infrastructure.

5. An attacker creates a fake LinkedIn profile of a recruiter to build trust with an employee before sending a malicious file. This manipulation is known as:

Name: _____ **Date:** _____

Answer: B) Social Engineering

Social engineering focuses on psychological manipulation of individuals into divulging confidential information or performing actions that compromise security.

6. Salting a password involves adding random data to the password before hashing it to protect against rainbow table attacks.

Answer: A) True

Salting ensures that even if two users have the same password, their hashes will look different, making precomputed hash tables (rainbow tables) ineffective.

7. Which cryptographic principle ensures that a sender cannot later deny having sent a specific digital message?

Answer: C) Non-repudiation

Non-repudiation, often achieved through digital signatures, provides proof of the origin and integrity of data so the sender cannot deny it.

8. What is the name for the 'White Hat' practice of searching for vulnerabilities in a system with the owner's permission to improve security?

Answer: B) Penetration Testing

Penetration testing (or pen testing) is a simulated cyberattack against your computer system to check for exploitable vulnerabilities.

9. Using a Virtual Private Network (VPN) encrypts the data between your device and the VPN server, effectively preventing your ISP from seeing the specific content of your traffic.

Answer: A) True

VPNs create an encrypted tunnel for your data, hiding your browsing activity from your Internet Service Provider (ISP) and others on the local network.

10. In a 'Man-in-the-Middle' (MitM) attack, what is the primary method the attacker uses to compromise the target?

Answer: B) Intercepting and potentially altering communication between two parties

Name: _____ Date: _____

A MitM attack occurs when a perpetrator positions themselves in a conversation between a user and an application to eavesdrop or impersonate one of the parties.