Name: _______________ Date: _______________

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:

A. Ransomware blockade
B. Zero-day exploit
C. Distributed Denial of Service (DDoS)
D. Brute force attack

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

A. True
B. False

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

A. Baiting
B. Pretexting
C. Tailgating
D. Vishing

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

A. Cloud Database Servers
B. Programmable Logic Controllers (PLCs)
C. Consumer Smart Home Hubs
D. Graphics Processing Units (GPUs)

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:

A. DNS Hijacking
B. Social Engineering
C. Buffer Overflow
D. SQL Injection

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

A. True

B. False

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

A. Confidentiality
B. Availability
C. Non-repudiation
D. Redundancy

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?

A. Data Mining
B. Penetration Testing
C. Packet Sniffing
D. Cryptanalysis

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.

A. True
B. False

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

A. Exhausting server resources with traffic
B. Intercepting and potentially altering communication between two parties
C. Guessing simple passwords using a dictionary file
D. Physically stealing a hard drive from a data center