Name: _____ **Date:** _____

Answer Key: Operation Zero Day: Cyber Logistics for 11th Grade Technologists

Calculate risks and weigh the ethical dilemmas of state-sponsored exploits and zero-trust architecture in this high-stakes digital defense simulation.

---

1. An organization adopts a 'Zero Trust' architecture. What is the fundamental guiding principle of this security model?

Answer: C) Continuous verification of every request as if it originates from an open network

Zero Trust operates on the assumption that threats exist both outside and inside the network; therefore, no request is automatically trusted regardless of its origin.

2. In the context of cryptology, the process of 'hashing' converts data into a fixed-length string of characters. Unlike encryption, hashing is specifically designed to be _____.

Answer: B) One-way

Hashing is a one-way function used for data integrity; you cannot mathematically reverse a hash to retrieve the original plaintext.

3. A 'Zero-Day' vulnerability refers to a security flaw that has been known to the software vendor for at least one month but remains unpatched.

Answer: B) False

A Zero-Day vulnerability is one that is unknown to the vendor or for which no patch exists, meaning the developer has had 'zero days' to fix it.

4. Which of the following describes a 'Man-in-the-Middle' (MitM) attack specifically occurring via ARP Spoofing?

Answer: B) Linking an attacker's MAC address with the IP address of a legitimate server on a local network

ARP Spoofing redirects network traffic intended for a gateway or server to the attacker's machine by manipulating the Address Resolution Protocol.

5. When an attacker uses a massive list of previously compromised username and password pairs to gain unauthorized access to different websites, the technique is known as _____.

Name: _____ **Date:** _____

Answer: C) Credential stuffing

Credential stuffing exploits the common habit of password reuse across multiple platforms using automated tools and leaked databases.

6. Which security protocol is primarily responsible for establishing an encrypted link between a web server and a browser, replacing its predecessor SSL?

Answer: B) TLS

Transport Layer Security (TLS) is the modern, more secure version of SSL used to secure HTTPS traffic.

7. Sandboxing is a cybersecurity practice where suspicious programs are executed in an isolated virtual environment to observe their behavior without risking the host system.

Answer: A) True

Sandboxing provides a safe 'container' to analyze potentially malicious software while preventing it from accessing the local file system or network.

8. An attacker targets a specific high-ranking executive using a highly customized and researched phishing email. This specialized form of social engineering is called _____.

Answer: B) Whaling

Whaling is a specific subset of spear-phishing that targets 'big fish' like CEOs or CFOs to steal high-value data or authorize large wire transfers.

9. What is the primary purpose of a ‘Salting’ technique in password storage?

Answer: B) To add a unique, random string of bits to each password before hashing to defeat rainbow table attacks

Salting ensures that even if two users have the same password, their hashes will look completely different, making it much harder for hackers to use pre-computed tables to crack them.

10. A 'Cold Boot Attack' involves a hacker physically accessing a computer to retrieve encryption keys that remain briefly in the RAM after the power is turned off.

Answer: A) True

Data in DRAM takes seconds to minutes to degrade; by cooling the modules and restarting the machine, an attacker can dump the memory contents and find sensitive keys.

Name: _____ Date: _____