Name: _____ **Date:** _____

Answer Key: Cybersecurity Ethics and Analysis for College

Student evaluate real-world infrastructure vulnerabilities and data governance policies through multi-layered analysis of modern digital threats.

---

1. A nation-state actor utilizes a 'zero-day exploit' to compromise an electrical grid. What distinguishes this specific type of vulnerability for security analysts?

Answer: B) The vulnerability is unknown to the software vendor, leaving zero days for a patch.

Zero-day exploits are particularly dangerous because they target vulnerabilities that the developers are not yet aware of, meaning no defense or patch exists at the time of the attack.

2. In a 'Man-in-the-Middle' (MitM) attack, the adversary primarily relies on compromising the physical server hardware rather than the communication channel.

Answer: B) False

MitM attacks focus on intercepting and potentially altering the communication between two parties on a network, often via ARP spoofing or rogue Wi-Fi hotspots, rather than physical server compromise.

3. An organization implements _____, a security model that requires all users, even those inside the network perimeter, to be authenticated and validated before gaining access to applications and data.

Answer: B) Zero Trust Architecture

Zero Trust operates on the principle of 'never trust, always verify,' removing the assumption of trust for users based solely on their physical or network location.

4. During a risk assessment of a cloud-based database, an analyst suggests using 'Salting' alongside hashing for stored passwords. What is the primary analytical objective of this technique?

Answer: C) To defend against pre-computed hash attacks like Rainbow Tables.

Salting adds a unique, random string to each password before hashing, which ensures that identical passwords have different hashes, rendering pre-computed Rainbow Tables useless.

5. End-to-End Encryption (E2EE) ensures that service providers like WhatsApp or Signal cannot view the contents of the messages sent through their platforms.

Answer: A) True

Name: _____ **Date:** _____

E2EE encrypts data on the sender's device and only decrypts it on the recipient's device; the service provider acts only as a conduit and lacks the cryptographic keys to read the data.

6. To analyze the integrity of a downloaded forensic image, a technician generates a _____, a unique alphanumeric string produced by an algorithm like SHA-256.

Answer: A) Cryptographic Hash

A cryptographic hash acts as a digital fingerprint; if even one bit of the original file is changed, the resulting hash will be completely different, proving a lack of integrity.

7. Which of the following describes 'Stuxnet' in the context of advanced persistent threats (APTs)?

Answer: B) A worm designed to target industrial control systems (PLCs) in a specific facility.

Stuxnet was a highly sophisticated piece of malware that target SCADA systems, demonstrating how cyber threats can cause physical damage to national infrastructure.

8. The 'Principle of Least Privilege' (PoLP) suggests that all users in a corporate environment should have administrative access to facilitate efficient troubleshooting.

Answer: B) False

PoLP states that users should only be granted the minimum level of access necessary to perform their job functions, reducing the 'attack surface' if an account is compromised.

9. In the context of the CIA Triad, ensuring that information is modified only by authorized parties is known as _____.

Answer: C) Integrity

Integrity refers to the protection of data from unauthorized deletion or modification, ensuring the information is accurate and trustworthy.

10. You are assessing a company's 'Incident Response Plan.' Which phase involves identifying how the breach occurred and removing the threat from the environment?

Answer: B) Eradication

Eradication is the stage where the root cause of the incident is eliminated and all traces of the malicious activity are removed from the system.