Name: _____ **Date:** _____

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?

A. It is a brute-force method targeting outdated legacy hardware.
B. The vulnerability is unknown to the software vendor, leaving zero days for a patch.
C. It is a social engineering tactic requiring no technical code execution.
D. It relies on a 24-hour window where servers are rebooting for maintenance.

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

A. True
B. False

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.

A. Discretionary Access Control
B. Zero Trust Architecture
C. Open Systems Interconnection
D. Network Address Translation

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?

A. To compress the data size for faster authentication.
B. To prevent unauthorized users from viewing the clear-text passwords.
C. To defend against pre-computed hash attacks like Rainbow Tables.
D. To ensure the database is compliant with physical security standards.

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.

A. True
B. False

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.

A. Cryptographic Hash
B. Digital Watermark
C. Metadata Tag

Name: _____ Date: _____

D. Symmetric Key

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

A. A simple phishing script targeting university students.
B. A worm designed to target industrial control systems (PLCs) in a specific facility.
C. A ransomware strain used to extort small businesses.
D. A legitimate administrative tool used for network monitoring.

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

A. True
B. False

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

A. Availability
B. Authenticity
C. Integrity
D. Confidentiality

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?

A. Preparation
B. Eradication
C. Recovery
D. Lessons Learned