

Chapter 1

1. Define confidentiality in the CIA triad?
2. What is the primary trade-off when increasing security measures?
3. Name all of the three A's related to access control?
4. What is the main motivation behind a nation-state actor's cyberattacks?
5. What is "shadow IT"?
6. Which type of threat actor is motivated primarily by ideology?
7. What is a zero-day vulnerability?
8. Give an example of data exfiltration?
9. Which cybersecurity resource defines policies and procedures for implementing security controls?
10. What is another name for an attack surface?

Chapter 2

1. What is social engineering primarily based on?
2. What distinguishes spear phishing from regular phishing?
3. What is the purpose of a Faraday cage?
4. What social engineering attack that uses fake websites to harvest information?
5. What type of sensor uses high-frequency radio waves to detect motion?
6. What best defines data minimization?
7. What is the goal of a mantrap in physical security?
8. What data classification would apply to technical specifications of a product still in development?
9. What is the main concern addressed by data sovereignty?
10. Give an example of human-readable data?

Chapter 3

1. What is the main purpose of steganography?
2. What term refers to the unreadable output of encryption?
3. What cryptographic algorithm type uses two different keys?
4. What is the purpose of a digital signature?
5. What does a hash function primarily provide?
6. Which symmetric encryption algorithm is widely used and considered very secure?
7. What is a self-encrypting drive (SED)?
8. What is the primary limitation of cryptography in low-power devices?
9. What type of cryptographic attack attempts to find two inputs with the same hash value?
10. What is the purpose of post-quantum cryptography?

Chapter 4

1. What is the primary purpose of a digital certificate?
2. Which entity is responsible for verifying a user's identity before issuing a digital certificate?
3. What is a Certificate Revocation List (CRL)?
4. Which protocol provides real-time certificate status checking?
5. Describe a root digital certificate?
6. What is a wildcard digital certificate used for?
7. What format are most digital certificates structured in?
8. In the bridge trust model, what is the function of the central CA?
9. What does IPSec provide that TLS does not?
10. Which block cipher mode is designed to provide both confidentiality and authentication?

Chapter 5

1. What is the primary action performed by locking ransomware?
2. Which type of malware silently records every key a user types?
3. What differentiates a fileless virus from a file-based virus?
4. A Remote Access Trojan (RAT) is?
5. What is the role of a bot in a botnet?
6. What is a common characteristic of a rootkit?
7. What kind of attack takes advantage of input not being validated in a web application?
8. What is a NULL pointer dereference likely to cause?
9. What type of tool is Host Intrusion Detection System (HIDS)?
10. Which method helps protect an OS by preventing unapproved software from running?

Chapter 6

1. Which method helps protect an OS by preventing unapproved software from running?
2. Which mobile device deployment model allows employees to use their personally owned phones for work?
3. Give benefits of containerization on mobile devices?
4. What mobile device feature can take a picture of a thief after failed login attempts?
5. What is a security risk of connecting to public hotspots?
6. What type of embedded hardware allows users to program logic operations into a chip?
7. What legislation addresses federal cybersecurity standards for IoT devices?
8. Which tool allows organizations to manage apps on mobile devices?
9. What is the key challenge in implementing cryptography on IoT devices?
10. What is dynamic code analysis also known as?

Chapter 7

1. Name examples of “something you have” as an authentication factor?
2. What type of attack attempts to log in to many accounts using a few common passwords?
3. What biometric method uses eyes for authentication?
4. What is the primary purpose of salting a password?
5. Which authentication protocol is used for enabling single sign-on across different web domains?
6. In the Attribute-Based Access Control (ABAC) model, access decisions are based on:
7. What is a disadvantage of Discretionary Access Control (DAC)?
8. What stores all authentication credentials in one place for multiple app access?
9. Which key stretching algorithm is typically used for securing password hashes?
10. Behavioral biometrics include which of the following?