Final Review

Chapter 8

1. What is the primary goal of a man-in-the-middle (MITM) attack?

2. What type of attack captures a legitimate transmission and reuses it later?

3. How does a Man-in-the-Browser (MITB) attack usually begin?

4. Give examples of consequences of a successful DNS attack?

5. What describes a MAC flooding attack?

6. What monitoring methodology compares current activity to a secure baseline to detect deviations?

7. What tool is used for capturing and analyzing packets via a command-line interface?

8. What is the function of a Data Loss Prevention (DLP) system?

9. What email authentication method validates content through a digital signature?

10. What type of attack involves intercepting and reusing a user's authentication credentials?

Chapter 9

1. What is the purpose of network segmentation in infrastructure security?

2. Which device is most vulnerable to a MAC flooding attack?

3. What is the main function of an Access Control List (ACL) on a router?

4. What firewall type allows more flexible and generic rule statements?

5. What is the role of a reverse proxy?

6. What is a honeynet?

7. Describes the Zero Trust model?

8. What does a VPN allow users to do?

9. What is a demilitarized zone (DMZ) in network infrastructure?

10. What does Network Access Control (NAC) primarily do?

Chapter 10

1. What is the main difference between Bluejacking and Bluesnarfing?

2. Which of the following is a security concern with NFC in crowded places?

3. What is a rogue access point (AP)?

4. What vulnerability exists in MAC address filtering?

5. Which Wi-Fi security protocol introduced Simultaneous Authentication of Equals (SAE)?

6. What is a fat AP?

7. What encryption protocol is used by WPA2 for data confidentiality?

8. Which attack uses fake deauthentication frames to disconnect clients from an AP?

9. Which authentication method uses digital certificates and is part of EAP?

10. What is the purpose of a wireless site survey?

Chapter 11

1. Name benefits of cloud computing?

2. What type of cloud is open only to specific organizations with shared concerns?

3. What is the purpose of a CASB in cloud environments?

4. Which service model allows consumers to run their own applications on a cloud platform?

5. Which cloud computing characteristic allows users to provision resources without human interaction?

6. Which cloud model includes both public and private cloud elements?

7. What is the function of a thin client in cloud computing?

8. Which virtualization type allows entire OS environments to be simulated?

9. Which of the following describes a Type I hypervisor?

10. What is a major security risk with virtual machines?

Chapter 12

1. What is the main purpose of vulnerability scanning?

2. What scan type does not send test traffic but listens to network data?

3. List of tools is used for web application vulnerability scanning?

4. What does OSINT refer to?

5. Which component defines the devices or areas to be scanned?

6. What is a CVSS score used for?

7. What is a major drawback of internal penetration testing?

8. Which term refers to scanning from within the network perimeter?

9. What is a false negative in vulnerability scanning?

10. Which agency is responsible for AIS?

Chapter 13

1. What is the purpose of a Business Continuity Plan (BCP)?

2. What type of site has all the necessary equipment but no internet connectivity or current backups?

3. What is the main purpose of a Business Impact Analysis (BIA)?

4. Which component of forensics involves identifying where evidence has been and who handled it?

5. What is the most volatile data source in the order of volatility?

6. What type of RAID offers both striping and mirroring?

7. Which device ensures power continues during an outage?

8. What is the difference between an audit and an assessment?

9. What is the purpose of Wireshark?

10. What does RTO stand for?

Chapter 14

1. What is the primary purpose of governance within an organization?

2. What is the role of a Data Privacy Officer (DPO)?

3. Name a few of type of governance body?

4. What does an acceptable-use policy (AUP) define?

5. What does an acceptable-use policy (AUP) define?

6. What does an acceptable-use policy (AUP) define?

7. What does an acceptable-use policy (AUP) define?

8. What is an example of artificial intelligence in cybersecurity?

9. What is a key risk of AI in cybersecurity?

10. What is adversarial AI?

Chapter 15

1. What is considered a high-value asset in cybersecurity?

2. What does CAM stand for?

3. What is the first step in an asset's lifecycle?

4. What is the goal of change management?

5. What does risk analysis aim to do?

6. Which bias involves making decisions based on easily remembered information?

7. What is the formula for Annualized Loss Expectancy (ALE)?

8. Give a few of risk response strategy?

9. What is a common third-party risk mitigation technique?

10. What is the purpose of phishing simulations in awareness training?