Homework Assignment: Chapters 11–13

Chapter 11: Cloud and Virtualization Security

1. Explain the key characteristics of cloud computing and how they benefit organizations.
2. Compare and contrast the four types of cloud deployment models (public, private, community, and hybrid). Provide an example of an appropriate use case for each.
3. Describe how a cloud access security broker (CASB) and secure web gateway (SWG) contribute to cloud security.
4. What are the main security concerns related to virtualization, and how can these risks be mitigated?
5. Explain the difference between monolithic and microservices application architecture. Why might a company prefer one over the other in a cloud-native environment?

Chapter 12: Vulnerability Management

6. What is vulnerability scanning, and why is it a critical part of cybersecurity? Describe at least two challenges organizations face when conducting scans.
7. Differentiate between active and passive vulnerability scanning. When might each be used?
8. Explain the role of Open Source Intelligence (OSINT) in threat intelligence. What are its strengths and limitations?
9. Why is it important to prioritize vulnerabilities after a scan? Briefly describe how CVSS and CWE scores help in this process.
10. Imagine you're a security analyst conducting a vulnerability scan. What steps would you take from defining the scan scope to reporting results?

Chapter 13: Incident Preparation and Investigation

11. Define business continuity planning (BCP) and describe the key components that should be included in a BCP.
12. What is a Business Impact Analysis (BIA), and how does it influence decisions in disaster recovery planning?
13. Describe the difference between a hot site, warm site, and cold site in disaster recovery. What are the pros and cons of each?
14. Explain the order of volatility in digital forensics. Why is it important to follow this order during an investigation?
15. Outline the steps involved in a digital forensics investigation following a cybersecurity incident. What procedures are essential to preserve the integrity of evidence?