Homework Assignment: Chapter 8 & 9 – Infrastructure Threats and Security

Please answer each questions in about 2-3 sentences.

1. What is a man-in-the-middle (MITM) attack, and how does it compromise secure communication?

2. How does a replay attack differ from a session hijacking attack?

3. Explain what a man-in-the-browser (MITB) attack is and how it typically begins.

4. What are DNS poisoning and DNS hijacking, and what is the key difference between them?

5. Define a DDoS attack and describe how attackers typically carry it out.

6. How can PowerShell be misused by attackers during a network attack?

7. What is the purpose of using macros in VBA, and why are they a common security concern?

8. Describe what ARP poisoning is and its role in Layer 2 attacks.

9. What is a MAC flooding attack, and how does it impact a network switch?

10. Define a credential relay attack and how it is used to gain unauthorized access.

11. Compare and contrast anomaly-based and signature-based monitoring methodologies.

12. What is the goal of heuristic monitoring, and how does it differ from behavior-based monitoring?

13. Explain the concept of data loss prevention (DLP) and how it protects organizational data.

14. What is a Security Information and Event Management (SIEM) tool, and what are its primary functions?

15. How do SOAR platforms assist in improving security operations?

16. Explain the role of email headers in monitoring and securing email communications.

17. What are SPF, DKIM, and DMARC, and how do they enhance email security?

18. Describe the principle of least privilege and how it applies to infrastructure security.

19. What are network segmentation and isolation, and how do they improve security?

20. Explain the security risks and defenses related to MAC address spoofing.

21. How does a router use access control lists (ACLs) to improve network security?

22. What are the benefits of using a load balancer for security?

23. Distinguish between a policy-based and rule-based firewall.

24. What is the difference between a forward proxy and a reverse proxy?

25. Describe the purpose and function of a honeypot and a honeynet.

26. Explain the difference between an IDS and an IPS.

27. What are the challenges of using file integrity monitoring (FIM)?

28. Define Extended Detection and Response (XDR) and how it expands on endpoint protection.

29. What is a demilitarized zone (DMZ), and why is it used in network architecture?

30. Describe the Zero Trust Architecture (ZTA) and how it changes traditional network security models.

31. What is the function of a jump server within a DMZ?

32. Explain how network access control (NAC) restricts endpoint access to a network.

33. What is a Virtual LAN (VLAN) and how does it provide logical segmentation?

34. Describe two differences between VPNs and NAC as access technologies.

35. Why is it important to remove unnecessary software from infrastructure devices?