Name _____ Date _____

Module 10 - LAN Security Concepts

Switching, Routing, and Wireless Essentials – Semester 2

Student Version

Module 10 Sections:

10.0 Introduction
10.1 Network Attacks Today
10.2 Access Control
10.3 Layer 2 Security Threats
10.4 MAC Address Table Attack
10.5 LAN Attacks
10.6 Module Practice and Quiz

Required Materials:

Reading Organizer

Packet Tracer Activities: None

Labs: None

Module's 10 - 13 Exam

Page intentionally left blank.

Points_____ / ___163___

Name_____ Date _____

Module 10 - LAN Security Concepts
Reading Organizer
Student Version

Note: The Reading Organizer has weighted scoring. Any question with the word **explain**, **define, or describe** in it is expected to have a longer answer and is worth two points each.

After completion of this module, you should be able to:

- Explain how to use endpoint security to mitigate attacks.
- Explain how AAA and 802.1X are used to authenticate LAN endpoints and devices.
- Identify Layer 2 vulnerabilities.
- Explain how a MAC address table attack compromises LAN security.
- Explain how LAN attacks compromise LAN security.

10.1 Network Attacks Today

1. Describe the following attacks.

a. Distributed Denial of Service (DDoS) –

b. Data Breach –

c. Malware –

2. List and describe the devices that can protect the network perimeter from outside access.

a. _____–

b. _____–

c. _____–

3. Describe endpoints.

4. List the traditional host-based security features endpoints have typically used.

a.

b.

c.

5. Endpoints are best protected today by a combination of Network Access Control (NAC) solutions. What is typically included with NAC?

a.

b.

c.

d.

6. According to the Cisco's Talos Intelligence Group, in June 2019, _____ of all email sent was spam.

7. What is an email security appliance or ESA designed to monitor?

8. Threat intelligence data is pulled by the Cisco ESA every _____.

9. What are some of the functions of an ESA?

a.

b.

c.

d.

e.

10. A Web Security Appliance (WSA) is a mitigation technology for web-based threats. What protections does WSA combine and provide?

a.

b.

c.

d.

10.2 Access Control

11. What is the simplest method of remote access authentication?

12. SSH is a more secure form of remote access. Describe the three ways it is more secure.

a.

b.

c.

13. describe the limitations to a local database method.

a.

b.

14. What does AAA stands for?

15. AAA provides the primary framework to set up access control on a network device. Explain what each of the three A's does.

a.

b.

c.

16. List and describe the two common methods of implementing AAA authentication.

a. _____–

b. _____–

17. Explain what the attributes Authorization uses operate.

18. AAA accounting collects and reports usage data. What might the collected data include?

a.

b.

c.

d.

19. The IEEE 802.1X standard is a port-based access control and authentication protocol. Describe what this protocol restricts.

20. List and describe the specific device roles offered for 802.1X port-based authentication devices.

a. _____–

b. _____–

c. _____–

10.3 Layer 2 Security Threats

21. Security is only as strong as the weakest link in the system. What is the weak link in the OSI model?

22. Describe the following layer 2 attacks.

a. MAC Table Attacks –

b. VLAN Attacks –

c. DHCP Attacks –

d. ARP Attacks –

e. Address Spoofing Attacks –

f. STP Attacks –

23. Describe the following attack mitigations.

a. Port Security –

b. DHCP Snooping –

c. Dynamic ARP Inspection (DAI) –

d. IP Source Guard (IPSG) –

24. Layer 2 mitigation solutions will not be effective if the management protocols are not secured. Explain the recommended strategies to secure management protocols.

a.

b.

c.

d.

10.4 MAC Address Table Attack

25. MAC address tables are stored in _____ and are used to more efficiently _____ frames.

26. All MAC tables have a fixed size and consequently, a switch can run out of resources in which to store MAC addresses. Explain in detail what occurs during a MAC address flooding attack.

27. Explain what happens if a MAC address flooding attack is discovered and stopped.

28. What makes tools such as _____ so dangerous is that an attacker can create a MAC table overflow attack very quickly.

29. A reason attack tools are dangerous is because they not only affect the local switch, they can also affect other connected Layer 2 switches. Explain why this is a problem.

30. To mitigate MAC address table overflow attacks, network administrators must implement port security. Explain how port security can help.

10.5 LAN Attacks

31. Describe a VLAN hopping attack.

32. Explain the three steps in a double-tagging attack.

Step 1:

Step 2:

Step 3:

33. List how VLAN hopping and VLAN double-tagging attacks can be prevented.

a.

b.

c.

34. List the IP configuration information DHCP servers dynamically provide to hosts.

a.

b.

c.

d.

35. List and describe two types of DHCP attacks.

a. _____–

b. _____–

36. Describe how Gobbler works.

37. List and describe what misleading information a rogue server can provide.

a. _____–

b. _____–

c. _____–

38. According to the ARP RFC, a client is allowed to send an unsolicited ARP Reply called a “gratuitous ARP.” Explain what happens during this process.

39. List and describe the attacks that can occur during a DHCP spoofing attack.

a. _____–

b. _____–

c. _____–

40. List some of the tools available on the internet to create ARP man-in-the-middle attacks.

a.

b.

c.

d.

41. Explain in detail what happens during a MAC address spoofing attack.

42. Explain how network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack.

43. How can STP attacks be mitigated?

44. The Cisco Discovery Protocol (CDP) is a proprietary _____ link discovery protocol.

45. What information is included in CDP updates?

a.

b.

c.

d.

e.

46. CDP broadcasts are sent _____ and _____.

47. To disable CDP globally on a device what command do you use?

48. To enable CDP globally what command do you use?

49. To disable CDP on a port what command can you use?

50. To enable CDP on a port what command can you use?

52. Link Layer Discovery Protocol (LLDP) is a vendor-neutral version of Cisco's CDP. It is also vulnerable to reconnaissance attacks. What command can you use to disable LLDP globally?

53. To disable LLDP on the interface what two commands can you use?

a.

b.