Name _____ Date _____

Module 16 – Network Security Fundamentals

Introduction to Networks – Semester 1

Student Version

Module 16 Sections:

16.0 Introduction
16.1 Security Threats and Vulnerabilities
16.2 Network Attacks
16.3 Network Attack Mitigation
16.4 Device Security
16.5 Module Practice and Quiz

Required Materials:

Reading Organizer

Packet Tracer Activities: 16.4.6 - Configure Secure Passwords and SSH
16.5.1 - Secure Network Devices

Labs: 16.2.6 - Research Network Security Threats
16.4.7 - Configure Network Devices with SSH
16.5.2 - Secure Network Devices

Module's 16 – 17 Exam

Page intentionally left blank.

Points_____ / __98___

Name_____ Date _____

Module 16 – Network Security Fundamentals

Introduction to Networks – Semester 1
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 chapter, you should be able to:

- Explain why basic security measure are necessary on network devices.
- Identify security vulnerabilities.
- Identify general mitigation techniques.
- Configure network devices with device hardening features to mitigate security threats.

16.1 Security Threats and Vulnerabilities

1. List and describe the four types of threats may arise after a threat actor gains access to the network.

a. _____ -

b. _____ -

c. _____ -

d. _____ -

2. What are three primary vulnerabilities or weaknesses in network devices?

a.

b.

c.

3. List and describe the four classes of physical threats.

a. _____ -

b. _____ -

c. _____ -

d. _____ -

4. Describe three steps you can use to Implement physical security to limit damage to the equipment.

Step 1.

Step 2.

Step 3.

16.2 Network Attacks

5. Explain what malware is.

6. List and describe three types of malware.

a. _____ -

b. _____ -

c. _____ -

7. Network attacks can be classified into three major categories. List and describe each of the three.

a. _____ -

b. _____ -

c. _____ -

8. List and describe three types of reconnaissance attack tools.

a. _____ -

b. _____ -

c. _____ -

9. List and describe four types of access attacks.

a. _____ -

b. _____ -

c. _____ -

d. _____ -

10. _____ attacks are the most publicized form of attack and among the most difficult to eliminate.

11. Describe the following attacks.

a. DoS Attack –

b. DDoS Attack –

16.3 Network Attack Mitigation

12. in order to mitigate network attacks organizations employ a _____ approach (also known as a _____ to security.

13. List the security devices and services that can be implemented to protect an organization's users and assets against TCP/IP threats.

a.

b.

c.

d.

e.

14. Backing up device configurations and data is one of the most effective ways of protecting against data loss. List the things to consider when choosing a backup method.

a.

b.

c.

d.

15. What is the most effective way to mitigate a worm attack?

16. List and describe what each of the "A's" mean in the AAA or triple A.

a. _____ -

b. _____ -

c. _____ -

17. A _____protects computers and networks by preventing undesirable traffic from entering internal networks.

18. A _____could allow outside users controlled access to specific services.

19. List the different techniques firewalls use to determine what will be permitted or denied access to a network.

a.

b.

c.

d.

20. Securing _____ devices is one of the most challenging jobs of a network administrator because it involves human nature.

16.4 Device Security

21. For Cisco routers, the Cisco _____ feature can be used to assist securing the system.

22. Describe some simple steps to increase security that should be taken that apply to most operating systems?

a.

b.

c.

23. On Cisco routers, leading spaces are _____ for passwords, but spaces _____ the first character are not.

24. What steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch?

a.

b.

c.

d.

25. The _____ global configuration command prevents unauthorized individuals from viewing plaintext passwords in the configuration file.

26. Telnet simplifies remote device access, but it is not secure. Why is telnet not secure?

27. What remote software is recommended for better security?

28. What command can you use to see which ports are open on a Cisco router?