Network Security Fundamentals / Module Practice and Quiz

Module Practice and Quiz

16.5.1

Packet Tracer - Secure Network Devices

In this activity you will configure a router and a switch based on a list of requirements.

Secure Network Devices

Secure Network Devices

16.5.2

Lab - Secure Network Devices

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure Basic Security Measures on the Router
- Part 3: Configure Basic Security Measures on the Switch

Secure Network Devices

16.5.3

What did I learn in this module?

Security Threats and Vulnerabilities

Attacks on a network can be devastating and can result in a loss of time and money due to damage or theft of important information or assets. Intruders who gain access by modifying software or exploiting software vulnerabilities are threat actors. After the threat actor gains access to the network, four types of threats may arise: information theft, data loss and manipulation, identity theft, and disruption of service. There are three primary vulnerabilities or weaknesses: technological, configuration, and security policy. The four classes of physical threats are: hardware, environmental, electrical, and maintenance.

Network Attacks

Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict "bad" or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojan horses are types of malware. Network attacks can be classified into three major categories: reconnaissance, access, and denial of service. The four classes of physical threats are: hardware, environmental, electrical, and maintenance. The three types of reconnaissance attacks are: internet queries, ping sweeps, and port scans. The four types of access attacks are: password (brute-force, Trojan horse, packet sniffers), trust exploitation, port redirection, and man-in-the-middle. The two types of disruption of service attacks are: DoS and DDoS.

Network Attack Mitigation

To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. This requires a combination of networking devices and services working together. Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats: VPN, ASA firewall, IPS, ESA/WSA, and AAA server. Infrastructure devices should have backups of configuration files and IOS images on an FTP or similar file server. If the computer or a router hardware fails, the data or configuration can be restored using the backup copy. The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems. To manage critical security patches, to make sure all end systems automatically download updates. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and what actions they perform while accessing the network (accounting). Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access. Servers accessible to outside users are usually located on a special network referred to as the DMZ. Firewalls use various techniques for determining what is permitted or denied access to a network including: packet filtering, application filtering, URL filtering and SPI. Securing endpoint devices is critical to network security. A company must have well-documented policies in place, which may include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

Device Security

The security settings are set to the default values when a new OS is installed on a device. This level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system. For most OSs default usernames and passwords should be changed immediately, access to system resources should be restricted to only the individuals that are authorized to use those resources, and any unnecessary services and applications should be turned off and uninstalled when possible. To protect network devices, it is important to use strong passwords. A pass phrase is often easier to remember than a simple password. It is also longer and harder to guess. For routers and switches, encrypt all plaintext passwords, setting a minimum acceptable password length, deter brute-force password guessing attacks, and disable an inactive privileged EXEC mode access after a specified amount of time. Configure appropriate devices to support SSH, and disable unused services.

16.5.4

Module Quiz - Network Security Fundamentals

1. Which component is designed to protect against unauthorized communications to and from a computer?

○ antivirus
○ security center
● firewall
○ port scanner
○ antimalware

2. Which command will block login attempts on RouterA for a period of 30 seconds if there are 2 failed login attempts within 10 seconds?

○ RouterA(config)# **login block-for 2 attempts 30 within 10**
○ RouterA(config)# **login block-for 30 attempts 10 within 2**
○ RouterA(config)# **login block-for 10 attempts 2 within 30**
● RouterA(config)# **login block-for 30 attempts 2 within 10**

3. What is the purpose of the network security accounting function?

○ to require users to prove who they are
○ to provide challenge and response questions
● to keep track of the actions of a user
○ to determine which resources a user can access

4. What type of attack may involve the use of tools such as nslookup and fping**?**

○ denial of service attack
○ access attack
● reconnaissance attack
○ worm attack

5. Which benefit does SSH offer over Telnet for remotely managing a router?

○ connections via multiple VTY lines
○ authorization
○ TCP usage
● encryption

6. What is one of the most effective security tools available for protecting users from external threats?

○ router that run AAA services
○ patch servers
● firewalls
○ password encryption techniques

7. Which type of network threat is intended to prevent authorized users from accessing resources?

● DoS attacks
○ reconnaissance attacks
○ access attacks
○ trust exploitation

8. Which three services are provided by the AAA framework? (Choose three.)

☐ automation
☑ authentication
☐ autoconfiguration
☐ autobalancing
☑ accounting
☑ authorization

9. Which malicious code attack is self-contained and tries to exploit a specific vulnerability in a system being attacked?

● worm
○ Trojan horse
○ virus
○ social engineering

10. Some routers and switches in a wiring closet malfunctioned after an air conditioning unit failed. What type of threat does this situation describe?

● environmental
○ electrical
○ maintenance
○ configuration

11. What does the term vulnerability mean?

○ a method of attack to exploit a target
○ a computer that contains sensitive information
○ a potential threat that a hacker creates
○ a known target or victim machine
● a weakness that makes a target susceptible to an attack

12. What three configuration steps must be performed to implement SSH access to a router? (Choose three.)

☑ an IP domain name
☐ an enable mode password
☐ an encrypted password
☐ a password on the console line
☑ a unique hostname
☑ a user account

13. What is the objective of a network reconnaissance attack?

○ unauthorized manipulation of data
○ disabling network systems or services
○ denying access to resources by legitimate users
● discovery and mapping of systems

14. For security reasons a network administrator needs to ensure that local computers cannot ping each other. Which settings can accomplish this task?

● firewall settings
○ smartcard settings
○ file system settings
○ MAC address settings

15. A network administrator establishes a connection to a switch via SSH. What characteristic uniquely describes the SSH connection?

○ remote access to the switch through the use of a telephone dialup connection
○ out-of-band access to a switch through the use of a virtual terminal with password authentication
● remote access to a switch where data is encrypted during the session
○ on-site access to a switch through the use of a directly connected PC and a console cable
○ direct access to the switch through the use of a terminal emulation program

Check

Show Me

Reset

16.4 Device Security

17.0 Introduction