Network security

Technology, Information Technology

Network security s of Learning Discuss the term confidentiality as it applies to data. How can data confidentiality be assured on a network?

Data confidentiality entails allowing authorized users to access particular data, while preventing unauthorized access of data by intruders. When access eavesdrops into particular data, the principle of confidentiality will not hold. In networks, encryption is the principle techniques of maintain data confidentiality. This process is achieved using encryption algorithms that are used to generate keys for encrypting and decrypting data.

2. Explain the concept of technical security controls. What are some the major components that make up technical control?

Technical security controls are used to provide control mechanisms within systems to as to mitigate potential security risks that may affect the network. Technical security controls are made of three components: detective, corrective and preventive, which all work to mitigate risks within a system.

3. Ad Type the global configuration mode and line configuration mode commands that are

required to secure the vty lines 0 through 15 to use the local username admin with the

encrypted password adminpass for remote telnet or ssh logins to the Cisco router.

a) Secure line 0 through 15

Switch(config)#line vty 0 15

Switch(config-line)#password admin

Switch(config-line)# login

Switch(config-line)#exit

b) Secure telnet

Switch(config)#line console 0

Switch(config-line)#password adminpass

Switch(config-line)#login

Switch(config-line)#exit

4. Type in the global configuration mode commands that will cause a user to be blocked for

10 minutes when 3 unsuccessful attempts are made to log in to the router within a time

period of 2 minutes.

routerOne(config)# login block-for 600 attempts 3 within

routerOne(config)#login on-failure log every 2

5. Describe the steps you can take on your personal mode Wireless network to protect your network and prevent unauthorized users from using your Internet connection.

The first step I will access the router through the web interface. This will allow me to configure encryption using the WPA2 or the pre-shared key. This will ensure that anyone who all devices must provide this key before joining the network.

I will also configure the number of addresses to a defined number as well as allow the DHCP server to provide dynamic addresses based on certain main address.

After doing these configurations, I will also enable no broadcast of the SSID and save the configurations, and exit the router.

6. Ads access-list 100 permit tcp any any eq 80 established

int s0/0

ip access-group 100 in

Given the commands shown above and assuming S0/0 is the outside (Internet-facing)

interface, explain what this ACL does.

The access list will permit traffic from outside network to reach the inside network through port 80.

7. Ad Discuss the advantages and disadvantages of TACACS+ and RADIUS. Include in your

discussion transport protocols, encryption, multiple protocol support, and accounting

reports

-TACACS uses TCP protocol which is more reliable than User Data Protocol used by RADIUS.

-RADIUS only encrypts password section of an access-request packet. On the other hand, the TACACS+ encrypt the entire message thus offering a better security.

- RADIUS offers better extension for IPSec compared to TACACS+ which does not.

-RADIUS is well developed compared to TACACS that is not very well developed.

8. Discuss the three IKE policy choices for data encryption algorithms. Discuss the key

Lengths, and rank the algorithms in order of best security.

There are three IKE policy choices message encryption, message integrity hash algorithm and peer authentication method. The policies are satisfied by various encryption methods that are dependent on a number of factors such as type of hardware in place. The key length available when using encryption algorithm allows the definition of key length used in terms of bits. When it comes to choosing message encryption algorithm, 3des is the strongest when compared to DES. The sha encryption offers a better encryption type as compared to md5 when it comes to message integrity has algorithm. For the peer authentication method, the rsa-sig offers a stronger encryption.

9. Explain the differences between and an Intrusion Detection System (IDS) and an

Intrusion Prevention System. Include the terms promiscuous mode and in-line mode in your

explanation.

An intrusion detection system has powerful features that provide notification when an attack occurs. On the other hand, a detective prevention system only uses limited functions to thwart attacks from taking place.

Detection system is also limited because it relies on copies of network packets, which must be received from another switch. This makes sensors operating in intrusion mode to be said as running in promiscuous mode.

Compared to detection system, intrusion prevention is more robust and has better features because it operate in inline mode where it checks as packets flows in teatime. Therefore, it can prevent traffic from entering a given network in real-time.