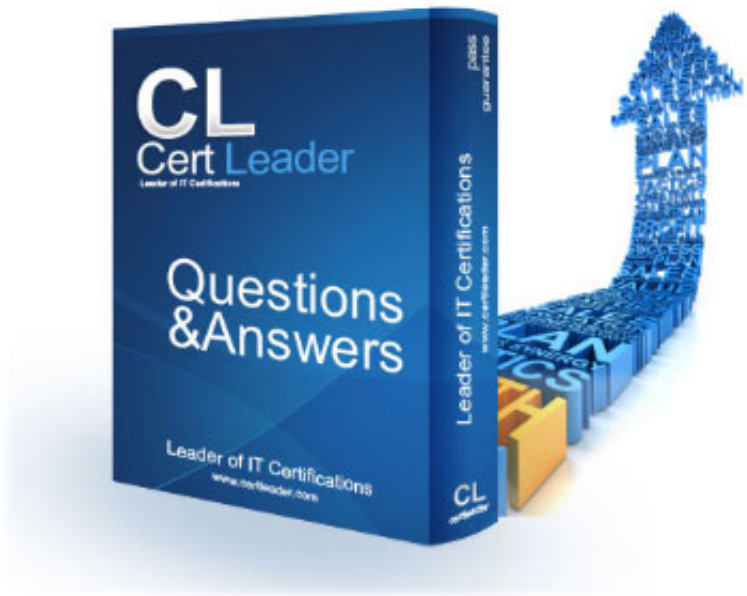
SY0-401 - CompTIA Security+ Certification

http://www.certleader.com/SY0-401-dumps.html



1. A company has implemented PPTP as a VPN solution. Which of the following ports would need to be opened on the firewall in order for this VPN to function properly? (Select TWO).

A. UDP 1723

B. TCP 500

C. TCP 1723

D. UDP 47

E. TCP 47

Answer: C,D

Explanation:

A PPTP tunnel is instantiated by communication to the peer on TCP port 1723. This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer. The PPTP GRE packet format is non-standard, including an additional acknowledgement field replacing the typical routing field in the GRE header. However, as in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47.

2. After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25

B. 68

C. 80

D. 443

Answer: B

Explanation:

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for distributing IP addresses for interfaces and services. DHCP makes use of port 68.

3. A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20

B. 21

C. 22

D. 23

Answer: B

Explanation:

When establishing an FTP session, clients start a connection to an FTP server that listens on TCP port 21 by default.

4. Which of the following ports is used for SSH, by default?

A. 23

B. 32

C. 12

D. 22

Answer: D

Explanation:

Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

5. By default, which of the following uses TCP port 22? (Select THREE).

A. FTPS

B. STELNET

C. TLS

D. SCP

E. SSL

F. HTTPS

G. SSH

H. SFTP

Answer: D,G,H

Explanation:

G: Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

D: SCP stands for Secure Copy. SCP is used to securely copy files over a network. SCP uses SSH to secure the connection and therefore uses port 22.

H: SFTP stands for stands for Secure File Transfer Protocol and is used for transferring files using FTP over a secure network connection. SFTP uses SSH to secure the connection and therefore uses port 22.

6. Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

A. TCP 23

B. UDP 69

C. TCP 22

D. TCP 21

Answer: C

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

7. Which of the following uses port 22 by default? (Select THREE).

A. SSH

B. SSL

C. TLS

D. SFTP

E. SCP

F. FTPS

G. SMTP

H. SNMP

Answer: A,D,E

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

8. Which of the following ports should be used by a system administrator to securely manage a remote server?

A. 22

B. 69

C. 137

D. 445

Answer: A

Explanation:

Secure Shell (SSH) is a more secure replacement for Telnet, rlogon, rsh, and rcp. SSH can be called a remote access or remote terminal solution. SSH offers a means by which a command-line, text-only interface connection with a server, router, switch, or similar device can be established over any distance. SSH makes use of TCP port 22.

9. Which of the following ports is used to securely transfer files between remote UNIX systems?

A. 21

B. 22

C. 69

D. 445

Answer: B

Explanation:

SCP copies files securely between hosts on a network. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH. Unlike RCP, SCP will ask for passwords or passphrases if they are needed for authentication.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

10. Which of the following secure file transfer methods uses port 22 by default?

A. FTPS

B. SFTP

C. SSL

D. S/MIME

Answer: B

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

11. During the analysis of a PCAP file, a security analyst noticed several communications with a remote server on port 53. Which of the following protocol types is observed in this traffic?

A. FTP

B. DNS

C. Email

D. NetBIOS

Answer: B

Explanation:

DNS (Domain Name System) uses port 53.

12. A security technician needs to open ports on a firewall to allow for domain name resolution.

Which of the following ports should be opened? (Select TWO).

A. TCP 21

B. TCP 23

C. TCP 53

D. UDP 23

E. UDP 53

Answer: C,E

Explanation:

DNS uses TCP and UDP port 53. TCP port 53 is used for zone transfers, whereas UDP port 53 is used for queries.

13. A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

A. HTTP

B. DHCP

C. DNS

D. NetBIOS

Answer: C

Explanation:

DNS links IP addresses and human-friendly fully qualified domain names (FQDNs), which are made up of the Top-level domain (TLD), the registered domain name, and the Subdomain or hostname.

Therefore, if the DNS ports are blocked websites will not be reachable.

14. Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

A. 21

B. 25

C. 80

D. 3389

Answer: C

Explanation:

Port 80 is used by HTTP, which is the foundation of data communication for the World Wide Web.

15. A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

A. 22

B. 135

C. 137

D. 143

E. 443

F. 3389

Answer: A,F

Explanation:

A secure remote administration solution and Remote Desktop protocol is required.

Secure Shell (SSH) is a secure remote administration solution and makes use of TCP port 22.

Remote Desktop Protocol (RDP) uses TCP port 3389.

16. Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

A. 22

B. 139

C. 443

D. 3389

Answer: D

Explanation:

Remote Desktop Protocol (RDP) uses TCP port 3389.

17. Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP

B. IPSec

C. SCP

D. TCP

Answer: C

Explanation:

SCP (Secure Copy) uses SSH (Secure Shell). SSH runs in the application layer (layer 7) of the OSI model.

18. Which of the following allows Pete, a security technician, to provide the MOST secure wireless

implementation?

A. Implement WPA

B. Disable SSID

C. Adjust antenna placement

D. Implement WEP

Answer: A

Explanation: Of the options supplied, WiFi Protected Access (WPA) is the most secure and is the replacement for WEP.

19. A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key. Which of the following attacks is taking place?

A. IV attack

B. WEP cracking

C. WPA cracking

D. Rogue AP

Answer: C

Explanation:

There are three steps to penetrating a WPA-protected network. Sniffing Parsing Attacking

20. Which of the following is a step in deploying a WPA2-Enterprise wireless network?

A. Install a token on the authentication server

B. Install a DHCP server on the authentication server

C. Install an encryption key on the authentication server

D. Install a digital certificate on the authentication server

Answer: D

Explanation:

When setting up a wireless network, you'll find two very different modes of Wi-Fi Protected Access (WPA) security, which apply to both the WPA and WPA2 versions. The easiest to setup is the Personal mode,

technically called the Pre-Shared Key (PSK) mode. It doesn’t require anything beyond the wireless router or access points (APs) and uses a single passphrase or password for all users/devices. The other is the Enterprise mode —which should be used by businesses and organizations—and is also known as the RADIUS, 802.1X, 802.11i, or EAP mode. It provides better security and key management, and supports other enterprise-type functionality, such as VLANs and NAP.

However, it requires an external authentication server, called a Remote Authentication Dial In User Service (RADIUS) server to handle the 802.1X authentication of users.

To help you better understand the process of setting up WPA/WPA2-Enterprise and 802.1X, here's the basic overall steps:

Choose, install, and configure a RADIUS server, or use a hosted service.

Create a certificate authority (CA), so you can issue and install a digital certificate onto the RADIUS server, which may be done as a part of the RADIUS server installation and configuration.

Alternatively, you could purchase a digital certificate from a public CA, such as GoDaddy or Verisign, so you don't have to install the server certificate on all the clients. If using EAP-TLS, you'd also create digital certificates for each end-user.

On the server, populate the RADIUS client database with the IP address and shared secret for each AP.

On the server, populate user data with usernames and passwords for each end-user.

On each AP, configure the security for WPA/WPA2-Enterprise and input the RADIUS server IP address and the shared secret you created for that particular AP.

On each Wi-Fi computer and device, configure the security for WPA/WPA2-Enterprise and set the 802.1X authentication settings.

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-401 Exam with Our Prep Materials Via below:

http://www.certleader.com/SY0-401-dumps.html