CompTIA

Exam SY0-401

CompTIA Security+ Certification

Version: 36.0

[Total Questions: 1776]

Topic break down

Topic	No. of Questions
Topic 1: Network Security	203
Topic 2: Compliance and Operational Security	289
Topic 3: Threats and Vulnerabilities	231
Topic 4: Application, Data and Host Security	137
Topic 5: Access Control and Identity Management	141
Topic 6: Cryptography	131
Topic 7: Mixed Questions	644

Topic 1, Network Security

Question No : 1 - (Topic 1)

An administrator wants to establish a WiFi network using a high gain directional antenna with a narrow radiation pattern to connect two buildings separated by a very long distance. Which of the following antennas would be BEST for this situation?

A. Dipole
B. Yagi
C. Sector
D. Omni

Answer: B

Explanation:
A Yagi-Uda antenna, commonly known simply as a Yagi antenna, is a directional antenna consisting of multiple parallel dipole elements in a line, usually made of metal rods. It consists of a single driven element connected to the transmitter or receiver with a transmission line, and additional parasitic elements: a so-called reflector and one or more directors. The reflector element is slightly longer than the driven dipole, whereas the directors are a little shorter. This design achieves a very substantial increase in the antenna's directionality and gain compared to a simple dipole.

Question No : 2 - (Topic 1)

Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete’s access to this site?

A. Internet content filter
B. Firewall
C. Proxy server
D. Protocol analyzer

Answer: A

Explanation:
Web filtering software is designed to restrict or control the content a reader is authorised to access, especially when utilised to restrict material delivered over the Internet via the Web,

e-mail, or other means.

Question No : 3 - (Topic 1)

Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP
B. SNMP
C. SFTP
D. SCP
E. TFTP

Answer: C,D

Explanation:
Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks. SFTP is a secured alternative to standard FTP.
Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Question No : 4 - (Topic 1)

An administrator needs to secure RADIUS traffic between two servers. Which of the following is the BEST solution?

A. Require IPSec with AH between the servers
B. Require the message-authenticator attribute for each message
C. Use MSCHAPv2 with MPPE instead of PAP
D. Require a long and complex shared secret for the servers

Answer: A

Explanation:
IPsec is used for a secure point-to-point connection traversing an insecure network such as the Internet. Authentication Header (AH) is a primary IPsec protocol that provides authentication of the sender's data.

Question No : 5 - (Topic 1)

A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

A. Bind server
B. Apache server
C. Exchange server
D. RADIUS server

Answer: A

Explanation:
BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. It includes the DNS server component contracted for name daemon. This is the only option that directly involves DNS.

Question No : 6 - (Topic 1)

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.

Question No : 7 - (Topic 1)

A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

A. RC4
B. DES
C. 3DES
D. AES

Answer: D

Explanation:
Cipher Block Chaining Message Authentication Code Protocol (CCMP) makes use of 128-bit AES encryption with a 48-bit initialization vector.

Question No : 8 - (Topic 1)

Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS
B. Firewall
C. NIPS
D. Spam filter

Answer: C

Explanation:
Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

Question No : 9 - (Topic 1)

Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

A. Subnetting
B. NAT
C. Quality of service
D. NAC

Answer: C

Explanation:
Quality of Service (QoS) facilitates the deployment of media-rich applications, such as video conferencing and Internet Protocol (IP) telephony, without adversely affecting network throughput.

Question No : 10 - (Topic 1)

A security analyst is reviewing firewall logs while investigating a compromised web server. The following ports appear in the log:

22, 25, 445, 1433, 3128, 3389, 6667

Which of the following protocols was used to access the server remotely?

A. LDAP
B. HTTP
C. RDP
D. HTTPS

Answer: C

Explanation:

RDP uses TCP port 3389.

Question No : 11 - (Topic 1)

A security engineer, Joe, has been asked to create a secure connection between his mail server and the mail server of a business partner. Which of the following protocol would be MOST appropriate?

A. HTTPS
B. SSH
C. FTP
D. TLS

Answer: D

Explanation: Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

Question No : 12 - (Topic 1)

A small company can only afford to buy an all-in-one wireless router/switch. The company has 3 wireless BYOD users and 2 web servers without wireless access. Which of the

following should the company configure to protect the servers from the user devices? (Select TWO).

A. Deny incoming connections to the outside router interface.
B. Change the default HTTP port
C. Implement EAP-TLS to establish mutual authentication
D. Disable the physical switch ports
E. Create a server VLAN
F. Create an ACL to access the server

Answer: E,F

Explanation:

We can protect the servers from the user devices by separating them into separate VLANs (virtual local area networks).

The network device in the question is a router/switch. We can use the router to allow access from devices in one VLAN to the servers in the other VLAN. We can configure an ACL (Access Control List) on the router to determine who is able to access the server.

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN.
This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs.
Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The network described in this question is a DMZ, not a VLAN.

Question No : 13 - (Topic 1)

If you don’t know the MAC address of a Linux-based machine, what command-line utility can you use to ascertain it?

A. macconfig
B. ifconfig
C. ipconfig
D. config

Answer: B

Explanation:

To find MAC address of a Unix/Linux workstation, use ifconfig or ip a.

Question No : 14 - (Topic 1)

Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

A. Redundant systems.
B. Separation of duties.
C. Layered security.
D. Application control.

Answer: C

Explanation:

Layered security is the practice of combining multiple mitigating security controls to protect resources and data.

Question No : 15 - (Topic 1)

A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

A. SNMP
B. SNMPv3
C. ICMP
D. SSH

Answer: B

Explanation: