Vendor: CompTIA

Exam Code: JK0-022

Exam Name: CompTIA Academic/E2C Security+ Voucher Only

Version: Demo

Exam A

QUESTION 1
Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

A. 21/UDP
B. 21/TCP
C. 22/UDP
D. 22/TCP

Correct Answer: D
Explanation

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

Incorrect Answers:
A, C: FTP ,and SSH do not make use of UDP ports.
B: FTP uses TCP port 21.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.

QUESTION 2
A network administrator is asked to send a large file containing PII to a business associate.

Which of the following protocols is the BEST choice to use?

A. SSH
B. SFTP
C. SMTP
D. FTP

Correct Answer: B
Explanation

Explanation/Reference:
SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications. As a result, SFTP offers protection for both the authentication traffic and the data transfer taking place between a client and server.

Incorrect Answers:
A: SSH is employed by SFTP.
C: SMTP is the email-forwarding protocol used on the Internet and intranets.
D: Standard FTP does not provide any confidentiality protection because it sends all data in the clear.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 49, 50.

QUESTION 3
Which of the following is a difference between TFTP and FTP?

A. TFTP is slower than FTP.
B. TFTP is more secure than FTP.
C. TFTP utilizes TCP and FTP uses UDP.
D. TFTP utilizes UDP and FTP uses TCP.

Correct Answer: D
Explanation

Explanation/Reference:
FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, whereas TFTP makes use of UDP port 69.

Incorrect Answers:
A: UDP is faster than TCP is because there is no form of flow control or error correction.
B: TFTP requires no authentication, whereas FTP allows authenticated connections.
C: As stated above, FTP employs TCP ports 20 and 21 and TFTP makes use of UDP port 69.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 49, 50.
http://www.skullbox.net/tcpudp.php

QUESTION 4
Which of the following is the default port for TFTP?

A. 20
B. 69
C. 21
D. 68

Correct Answer: B
Explanation

Explanation/Reference:
TFTP makes use of UDP port 69.

Incorrect Answers:
A, C: FTP (File Transfer Protocol) uses ports 20 and 21
D: Port 68 TCP/UDP is used by Bootstrap Protocol (BOOTP) Client; as well Dynamic Host Configuration Protocol (DHCP).

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 5
A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site
B. Block port 23 on the network firewall
C. Block port 25 on the L2 switch at each remote site
D. Block port 25 on the network firewall

Correct Answer: B
Explanation

Explanation/Reference:
Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn't support transfer of fi les. Telnet uses TCP port 23. Because it's a clear text protocol and service, it should be avoided and replaced with SSH.

Incorrect Answers:
A, C: L2 switches may interconnect a small number of devices in a home or the office. They are normally used for LANs.
D: Port 25 is used by Simple Mail Transfer Protocol (SMTP) for e-mail routing between mail servers.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.
http://en.wikipedia.org/wiki/Network_switch#Layer_2
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 6
A security analyst noticed a colleague typing the following command:

`Telnet some-host 443'

Which of the following was the colleague performing?

A. A hacking attempt to the some-host web server with the purpose of achieving a distributed denial of service attack.
B. A quick test to see if there is a service running on some-host TCP/443, which is being routed correctly and not blocked by a firewall.
C. Trying to establish an insecure remote management session. The colleague should be using SSH or terminal services instead.
D. A mistaken port being entered because telnet servers typically do not listen on port 443.

Correct Answer: B
Explanation

Explanation/Reference:
B: The Telnet program parameters are: telnet <hostname> <port> <hostname> is the name or IP address of the remote server to connect to. <port> is the port number of the service to use for the connection. TCP port 443 provides the HTTPS (used for secure web connections) service; it is the default SSL port. By running the Telnet some-host 443 command, the security analyst is checking that routing is done properly and not blocked by a firewall.

Incorrect Answers:
A: The telnet command parameter used by the colleague is done to check what service is running, i.e. HTTPS, not an attempt to get a denial of service attack.
C: TCP port 443 will not allow an insecure remote session because is the default SSL port.
D: TCP port 443 is the default SSL port and SSH makes use of TCP port 22.

References:
https://support.microsoft.com/en-us/kb/290051
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 83.

QUESTION 7
A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

A. ICMP
B. BGP
C. NetBIOS
D. DNS

Correct Answer: C
Explanation

Explanation/Reference:
The LMHOSTS file provides a NetBIOS name resolution method that can be used for small networks that do not use a WINS server. NetBIOS has been adapted to run on top of TCP/IP, and is still extensively used for name resolution and registration in Windows-based environments.

Incorrect Answers:
A: Internet Control Message Protocol (ICMP) is a network health and link-testing protocol that is commonly used by tools such as ping, traceroute, and pathping. It is not include in the LMHOSTS file.
B: Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. It is not include in the LMHOSTS file.
C: Domain Name System (DNS) distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain.
It is not include in the LMHOSTS file.

References:
https://technet.microsoft.com/library/Cc977602
http://en.wikipedia.org/wiki/Border_Gateway_Protocol
http://en.wikipedia.org/wiki/Domain_Name_System

QUESTION 8
An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

A. RADIUS
B. Kerberos

C. TACACS+
D. LDAP

Correct Answer: D
Explanation

Explanation/Reference:
LDAP makes use of port 389.

Incorrect Answers:
A: RADIUS makes use of various UDP ports.
B: Kerberos makes use of port 88.
C: TACACS makes use of TCP port 49 by default.

References:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 9
A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS
C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

Correct Answer: B
Explanation

Explanation/Reference:
The question states that traffic on port 21, 69, 80, and 137-139 is blocked, while ports 22 and 443 are allowed.

Port 21 is used for FTP by default.
Port 69 is used for TFTP.
Port 80 is used for HTTP.
Ports 137-139 are used for NetBIOS.
VMM uses SFTP over default port 22.
Port 22 is used for SSH by default.
SCP runs over TCP port 22 by default.
Port 443 is used for HTTPS.

Incorrect Answers:
A: FTP uses port 21, which is blocked.
C: SFTP uses port 22, which is allowed.
D: HTTPS uses port 443, which is allowed. NetBIOS uses ports 137-139, which is blocked.

References:
https://technet.microsoft.com/en-us/library/dd548299.aspx https://technet.microsoft.com/en-us/library/hh545212(v=sc.20).aspx https://technet.microsoft.com/en-us/library/dd425238(v=office.13).aspx https://technet.microsoft.com/en-us/library/hh427328.aspx

QUESTION 10
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

Correct Answer: CD
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A, E: PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
B: TCP port 500 is used by the Internet Security Association and Key Management Protocol (ISAKMP) References:
http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 11
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

Correct Answer: B
Explanation

Explanation/Reference:
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.

Incorrect Answers:

A: SMTP makes use of port 25.
C: HTTP makes use of port 80.
D: HTTPS makes use of port 443

References:
http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 12
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

Correct Answer: B
Explanation

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

Incorrect Answers:
A: FTP uses port 20, but it is not the default port.
C: SSH uses TCP port 22.
D: Telnet uses port 23.

References:
http://compnetworking.about.com/od/tcpip/p/port-numbers-21-ftp.htm http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 13
Which of the following ports is used for SSH, by default?

A. 23
B. 32
C. 12
D. 22

Correct Answer: D
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A: Port 23 is used by the Telnet protocol, not by SSH.
B: Port 32 is an unassigned port.
C: Port 12 is an unassigned port.

References:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers http://en.wikipedia.org/wiki/Secure_Shell http://www.planetlinks.com/tec236/notes-terms/4-10-06/default-tcp-ports-list.html

QUESTION 14
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

Correct Answer: DGH
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A: FTPS stands for File Transfer Protocol Secure. FTPS is similar to SFTP in that it is used to securely transfer files. The difference between the two is the encryption protocol used. FTPS uses the SSL or TLS cryptographic protocols and therefore uses port 443.
B: STelnet stands for secure telnet. STelnet uses SSL by default and therefore uses port 443.
C: TLS (Transport Layer Security) is a successor to SSL and uses port 443.
E: SSL (Secure Sockets Layer) uses port 443.
F: HTTPS (Hypertext transfer protocol secure) is used by web sites to encrypt and security transmit data. HTTPS uses the SSL or TLS cryptographic protocols and therefore uses port 443.

References:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 15

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

Correct Answer: C
Explanation

Explanation/Reference:
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).

Incorrect Answers:
A: Telnet uses port 23.
B: Port 69 is used by TFTP.
D: Port 21 is used by FTP.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 51.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 16
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

Correct Answer: ADE
Explanation

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

Incorrect Answers:
B: SSL operates over TCP port 443.
C: TLS can operate over TCP ports 443 and 80.
F: FTPS uses ports 989 and 990.
G: SMTP uses TCP port 25.
H: SNMP makes use of UDP ports 161 and 162.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 45, 51.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 17
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

Correct Answer: A
Explanation

Explanation/Reference:
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.

Incorrect Answers:
B: Port 69 is used by TFTP.
C: NetBIOS uses port 137.
D: Port 445 is used by Microsoft-DS.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 51.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 18
Which of the following ports is used to securely transfer files between remote UNIX systems?

A. 21
B. 22
C. 69
D. 445

Correct Answer: B
Explanation

Explanation/Reference:

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.

Incorrect Answers:
A: Port 21 is used by FTP.
C: Port 69 is used by TFTP.
D: Port 445 is used by Microsoft-DS.

References:
http://www.computerhope.com/unix/scp.htm
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 19
Which of the following secure file transfer methods uses port 22 by default?

A. FTPS
B. SFTP
C. SSL
D. S/MIME

Correct Answer: B
Explanation

Explanation/Reference:
SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.
Incorrect Answers:
A: FTPS uses ports 989 and 990.
C: SSL operates over TCP port 443.
D: S/MIME is an Internet standard for encrypting and digitally signing e-mail.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 45, 51, 313.

QUESTION 20
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

Correct Answer: B
Explanation

Explanation/Reference:
DNS (Domain Name System) uses port 53.

Incorrect Answers:
A: FTP (File Transfer Protocol) uses ports 20 and 21, not port 53.
C: Email uses multiple ports depending on what aspect of `email' we're talking about. For example SMTP (Simple Mail Transfer Protocol) used for sending email uses port 25. POP3 and IMAP, two methods of accessing and downloading email use ports 110 and 143 respectively.
D: NetBIOS uses ports 137, 138 and 139.

References:
http://en.wikipedia.org/wiki/Domain_Name_System
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 21
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

Correct Answer: CE
Explanation

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

Incorrect Answers:
A: FTP uses TCP port 21.
B. D: Telnet uses port 23.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 22
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

Correct Answer: C
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A: HTTP is responsible for the transmission of HTML documents and embedded multimedia components.
B: Dynamic Host Configuration Protocol (DHCP) allows DHCP servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients.
D: NetBIOS is a program that allows applications on different computers to communicate within a local area network (LAN).

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46. https://technet.microsoft.com/en-us/library/cc896553(v=ws.10).aspx http://en.wikipedia.org/wiki/NetBIOS

QUESTION 23
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

Correct Answer: C
Explanation

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

Incorrect Answers:
A: FTP uses TCP port 21.
B: SMTP uses TCP port 25.
D: Remote Desktop Protocol (RDP) uses TCP port 3389.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.

QUESTION 24
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

Correct Answer: AF
Explanation

Explanation/Reference:
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.

Incorrect Answers:
B: Port 135 is used by Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, which is used to remotely manage services including DHCP server, DNS server and WINS.
C: NetBIOS Name Service uses TCP port 137.
D: Internet Message Access Protocol v4 (IMAP4) uses TCP port 143.
E: HTTPS uses TCP port 443

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 25
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

Correct Answer: D
Explanation

Explanation/Reference:
Remote Desktop Protocol (RDP) uses TCP port 3389.

Incorrect Answers:
A: SSH uses TCP port 22. All protocols encrypted by SSH also use TCP port 22, such as SFTP, SHTTP, SCP, SExec, and slogin.
B: NetBIOS Session service uses TCP port 139.
C: HTTPS uses TCP port 443

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.

QUESTION 26
Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP
B. IPSec
C. SCP
D. TCP

Correct Answer: C
Explanation

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

Incorrect Answers:
A: ICMP (Internet Control Message Protocol) works in the network layer (Layer 3) of the OSI model.
B: IPSec (Internet Protocol Security) works in the network layer (Layer 3) of the OSI model.
D: TCP (Transmission Control Protocol) works in the transport layer (Layer 4) of the OSI model.

References:
http://www.rhyshaden.com/osi.htm
http://en.wikipedia.org/wiki/List_of_network_protocols_%28OSI_model%29 http://en.wikipedia.org/wiki/OSI_model

QUESTION 27
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

Correct Answer: A
Explanation

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

Incorrect Answers:
B: Disabling the SSID will only hide the wireless network, and is not more secure than WPA.
C: This will increase or decrease signal strength and availability, but will not make the network secure.
D: WEP was replaced by WPA to offer a more secure solution.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 59- 62.

QUESTION 28
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

Correct Answer: C
Explanation

Explanation/Reference:
There are three steps to penetrating a WPA-protected network.
Sniffing
Parsing
Attacking
Incorrect Answers:
A: Packet sniffing is not used for an IV attack.
B: WEP provides protection from packet sniffing and eavesdropping against wireless transmissions
D: Packet sniffing is not used for the Rogue AP.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 64, 189, 192.
www.tomshardware.com/reviews/wireless-security-hack,2981-6.html

QUESTION 29
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

Correct Answer: D
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A: A token is not required on the authentication server when configuring WPA-Enterprise.
B: DHCP (Dynamic Host Configuration Protocol) does not have to be installed on the authentication server. You don't have to use DHCP at all although it is easier if you do. However, DHCP is usually configured on a dedicated device, not on the authentication server.
C: You don't install an encryption key on the authentication server when configuring WPA- Enterprise. You install a digital certificate. The private key of the certificate is then used to create secure connections.

References:
http://www.windowsnetworking.com/articles-tutorials/wireless-networking/Deploying-WPA2- Enterprise-Wi-Fi-Security-Small-Businesses.html

QUESTION 30
A security administrator must implement a wireless security system, which will require users to enter a 30 character ASCII password on their accounts. Additionally the system must support 3DS wireless encryption.

Which of the following should be implemented?

A. WPA2-CCMP with 802.1X
B. WPA2-PSK
C. WPA2-CCMP
D. WPA2-Enterprise

Correct Answer: D
Explanation

Explanation/Reference:
D: WPA-Enterprise is also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK), this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. RADIUS can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether an incoming caller is authorized. Thus the RADIUS server can perform all authentications. This will require users to use their passwords on their user accounts.

Incorrect Answers:
A & C: CCMP is a block cipher that makes use of a 128 bit key. CCMP provides the following security services: Data confidentiality; ensures only authorized parties can access the information; Authentication; provides proof of genuineness of the user; Access control in conjunction with layer management. However, WPA2 includes support for CCMP.
B: EAP-PSK is documented in an experimental RFC that provides a lightweight and extensible EAP method that does not require any public-key cryptography.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 145, 172, 182.

QUESTION 31
Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

A. WPA2-Enterprise wireless network
B. DNS secondary zones
C. Digital certificates
D. Intrusion detection system

Correct Answer: A
Explanation

Explanation/Reference:
WPA2-Enterprise is designed for enterprise networks and requires a RADIUS authentication server.

Incorrect Answers:
B: A secondary zone is merely a copy of a primary zone that is hosted on another server.
C: Digital certificates are used for proving the identity of a user or the source of an object.
D: An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

References:
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
https://technet.microsoft.com/en-us/library/cc771898.aspx Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 32
A security administrator must implement a network authentication solution which will ensure encryption of user credentials when users enter their username and password to authenticate to the network.

Which of the following should the administrator implement?

A. WPA2 over EAP-TTLS
B. WPA-PSK
C. WPA2 with WPS
D. WEP over EAP-PEAP

Correct Answer: D
Explanation

Explanation/Reference:
D: Wired Equivalent Privacy (WEP) is designed to provide security equivalent to that of a wired network. WEP has vulnerabilities and isn't considered highly secure. Extensible Authentication Protocol (EAP) provides a framework for authentication that is often used with wireless networks. Among the five EAP types adopted by the WPA/ WPA2 standard are EAP-TLS, EAP- PSK, EAP-MD5, as well as LEAP and PEAP. PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server- side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

Incorrect Answers:
A: WPA2 is a more recent version of WEP. Although many consider PEAP and EAP-TTLS to be similar options, PEAP is more secure because it establishes an encrypted channel between the server and the client. EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. With EAP TTLS the client can, but does not have to be authenticated via a CA-signed PKI certificate to the server.
B: WPA is basically a version of WEP. EAP-PSK, defined in RFC 4764, is an EAP method for mutual authentication and session key derivation using a Pre-Shared Key (PSK). EAP-PSK is documented in an experimental RFC that provides a lightweight and extensible EAP method that does not require any public-key cryptography. The EAP method protocol exchange is done in a minimum of four messages.
C: WPA2 is a more recent version of WEP but does not ensure encryption of user credentials when they enter their usernames and passwords to authenticate to the network.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 181.

QUESTION 33
Which of the following BEST describes the weakness in WEP encryption?

A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm.
   Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
B. The WEP key is stored in plain text and split in portions across 224 packets of random data.
   Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
C. The WEP key has a weak MD4 hashing algorithm used.
   A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
D. The WEP key is stored with a very small pool of random numbers to make the cipher text.
   As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D
Explanation

Explanation/Reference:
WEP is based on RC4, but due to errors in design and implementation, WEP is weak in a number of areas, two of which are the use of a static common key and poor implementation of initiation vectors (IVs). When the WEP key is discovered, the attacker can join the network and then listen in on all other wireless client communications.

Incorrect Answers:
A: RC4 itself is not crack-able, but the IV that is crack-able.
B: The initialization vector (IV) that WEP uses for encryption is 24-bit and IVs are reused with the same key. By examining the repeating result, it is easy for intruders to crack the WEP secret key, known as an IV attack.
C: WEP does not use the MD4 hashing algorithm, but RC4.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 189.

QUESTION 34
Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5
B. WEP
C. PEAP-MSCHAPv2
D. EAP-TLS

Correct Answer: C
Explanation

Explanation/Reference:
PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

Incorrect Answers:
A: MD5 has been employed in a wide selection of cryptographic applications, and is also commonly used to verify data integrity.
B: Usernames and passwords are not required for WEP authentication.
D: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.

References:
https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx http://en.wikipedia.org/wiki/MD5

QUESTION 35
Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements?

A. EAP-TLS
B. EAP-FAST
C. PEAP-CHAP
D. PEAP-MSCHAPv2

Correct Answer: D
Explanation

Explanation/Reference:
PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and

password) rather than digital certificates or smart cards. Only servers running Network Policy Server (NPS) or PEAP-MS-CHAP v2 are required to have a certificate.

Incorrect Answers:
A: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.
B: EAP-FAST does not make use of TLS, but PAC (Protected Access Credentials).
C: CHAP intermittently authenticates the identity of the client via a three-way handshake.

References:
https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx http://www.techrepublic.com/article/ultimate-wireless-security-guide-a-primer-on-cisco-eap- fast-authentication/ http://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol

QUESTION 36
Which of the following means of wireless authentication is easily vulnerable to spoofing?

A. MAC Filtering
B. WPA - LEAP
C. WPA - PEAP
D. Enabled SSID

Correct Answer: A
Explanation

Explanation/Reference:
Each network interface on your computer or any other networked device has a unique MAC address. These MAC addresses are assigned in the factory, but you can easily change, or "spoof," MAC addresses in software.
Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. This isn't a great security tool because people can spoof their MAC addresses.
Incorrect Answers:
B: WPA LEAP (Wifi Protected Access Lightweight Extensible Authentication Protocol) combine to ensure a secure wireless authentication method. WPA LEAP is not easily vulnerable to spoofing.
C: WPA PEAP (Wifi Protected Access Protected Extensible Authentication Protocol) combine to ensure a secure wireless authentication method. WPA PEAP is not easily vulnerable to spoofing.
D: Enabling SSID broadcasting makes the wireless network visible to clients. It is not a means of wireless authentication.

References:
http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows- linux-and-mac/ http://www.tech-faq.com/eap-leap-peap-and-eap-tls-and-eap-ttls.html

QUESTION 37
Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/password combination. Upon disconnecting from the wireless network, she attempted to connect her personal tablet computer to the same wireless network and could not connect.
Which of the following is MOST likely the reason?

A. The company wireless is using a MAC filter.
B. The company wireless has SSID broadcast disabled.
C. The company wireless is using WEP.
D. The company wireless is using WPA2.

Correct Answer: A
Explanation

Explanation/Reference:
MAC filtering allows you to include or exclude computers and devices based on their MAC address.

Incorrect Answers:
B: because she could connect to the wireless with the first device, the SSID must be broadcasting.
C, D: Both WEP and WPA2 require a password or phrase.

References:
https://technet.microsoft.com/en-us/magazine/ff521761.aspx Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 38
After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network:
PERMIT 0A: D1: FA. B1: 03: 37
DENY 01: 33: 7F: AB: 10: AB

Which of the following is preventing the device from connecting?

A. WPA2-PSK requires a supplicant on the mobile device.
B. Hardware address filtering is blocking the device.
C. TCP/IP Port filtering has been implemented on the SOHO router.
D. IP address filtering has disabled the device from connecting.

Correct Answer: B
Explanation

Explanation/Reference:
MAC filtering allows you to include or exclude computers and devices based on their MAC address.

Incorrect Answers:
A: WPA2-PSK is used to encrypt a network using a plain-English passphrase between 8 and 63 characters long. C, D: The information entered into the SOHO wireless router are MAC addresses, therefore these options are not valid.

References:
https://technet.microsoft.com/en-us/magazine/ff521761.aspx http://www.webopedia.com/TERM/W/WPA2_PSK.html

QUESTION 39
A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up. Which of the following BEST allows the analyst to restrict user access to approved devices?

A. Antenna placement
B. Power level adjustment
C. Disable SSID broadcasting
D. MAC filtering

Correct Answer: D
Explanation

Explanation/Reference:
A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

Incorrect Answers:
A, B: This will increase or decrease signal strength and availability, but will not restrict user access.
C: Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence. Removing the presence will affect both authorized and unauthorized devices.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 40
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

Correct Answer: B
Explanation

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

Incorrect Answers:
A: macconfig is not a valid command-line utility.
C: To find MAC address of a Windows-based workstation, use ipconfig.
D: config on its own will not solve the problem.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 60.

QUESTION 41
An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access points?

A. SSID broadcast
B. MAC filter
C. WPA2
D. Antenna placement

Correct Answer: A
Explanation

Explanation/Reference:
Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence.

Incorrect Answers:
B: A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices. It does not, however, make finding the wireless network name any easier.
C: WPA2 deals with encryption, not the wireless network name.
D: This will increase or decrease signal strength and availability, but has nothing to do with the wireless network name being discovered.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 183. Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 42
A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

A. Disabling SSID broadcasting
B. Implementing WPA2 - TKIP
C. Implementing WPA2 - CCMP
D. Filtering test workstations by MAC address

Correct Answer: A
Explanation

Explanation/Reference:
Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

Incorrect Answers:
B: WPA2 makes use of CCMP, not TKIP.
C: WPA2 is an encryption scheme, but it will not make discovering the network difficult.

D: This will block devices not included in the MAC address list from accessing the network, but it will not make discovering the network difficult.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 60, 61.

QUESTION 43
While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

A. no longer used to authenticate to most wireless networks.
B. contained in certain wireless packets in plaintext.
C. contained in all wireless broadcast packets by default.
D. no longer supported in 802.11 protocols.

Correct Answer: B
Explanation

Explanation/Reference:
The SSID is still required for directing packets to and from the base station, so it can be discovered using a wireless packet sniffer.

Incorrect Answers:
A, D: The SSID is still used as a unique identifier for a wireless LAN. It is therefore still valid for authentication, and also still supported in 802.11 protocols.
C: Devices which are configured to connect to a network which does not broadcast its SSID may try to connect to the network by broadcasting for the network. This results in the SSID being revealed to wireless snoopers in the vicinity of the device. It is not included by default.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61. http://en.wikipedia.org/wiki/Service_set_(802.11_network)

QUESTION 44
A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

A. The SSID broadcast is disabled.
B. The company is using the wrong antenna type.
C. The MAC filtering is disabled on the access point.
D. The company is not using strong enough encryption.

Correct Answer: A
Explanation

Explanation/Reference:
When the SSID is broadcast, any device with an automatic detect and connect feature is able to see the network and can initiate a connection with it. The fact that they cannot access the network means that they are unable to see it.

Incorrect Answers:
B: The antenna type deals with signal strength and direction. It will not have a bearing on whether technology is older.
C: The network information is being given to the vendors, therefore MAC filtering is not the issue.
D: The network information is being given to the vendors, therefore encryption is not the issue.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 45
Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering
B. UseWPA2-PSK
C. Disable SSID broadcast
D. Power down unused WAPs

Correct Answer: C
Explanation

Explanation/Reference:
Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.
Incorrect Answers:
A: A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices. It does not, however, increase the difficulty of finding a wireless network.
B: WPA-Personal, also referred to as WPA-PSK (Pre-shared key) mode, is designed for home and small office networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase. Using this option will not decrease the chances of discovering the wireless network.
D: Using this option will not decrease the chances of discovering the wireless network in use.

References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

QUESTION 46
Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

A. Disable the wired ports
B. Use channels 1, 4 and 7 only
C. Enable MAC filtering
D. Disable SSID broadcast
E. Switch from 802.11a to 802.11b

Correct Answer: CD
Explanation

Explanation/Reference:
Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.
A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

Incorrect Answers:
A: Disabling the wired ports will not prevent outsiders from connecting to the AP and gaining unauthorized access.
B: Selecting the correct channels will prevent interference, not unauthorized access.
E: Doing this will decrease the bandwidth and increase the risk of interference.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61. https://technet.microsoft.com/en-us/library/cc783011(v=ws.10).aspx

QUESTION 47
Which of the following wireless security technologies continuously supplies new keys for WEP?

A. TKIP
B. Mac filtering
C. WPA2
D. WPA

Correct Answer: A
Explanation

Explanation/Reference:
TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it.
Incorrect Answers:
B: Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. It does not continuously supply new keys for WEP.
C: WPA2 makes use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and is a more secure standard that WEP or WPA.
D: WPA replaces WEP, and also uses TKIP.
References:
http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows- linux-and-mac/ Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 172, 173.

QUESTION 48
A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

A. WPA2 CCMP
B. WPA
C. WPA with MAC filtering
D. WPA2 TKIP

Correct Answer: A
Explanation

Explanation/Reference:
CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the WEP protocol and TKIP protocol of WPA. CCMP provides the following security services:
Data confidentiality; ensures only authorized parties can access the information Authentication; provides proof of genuineness of the user Access control in conjunction with layer management

Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 264 steps of operation.

Incorrect Answers:
B: The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP. WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2.
C: WPA even with the added security of MAC filtering is still inherently less secure than WPA2.
D: CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the TKIP protocol of WPA.

References:
http://en.wikipedia.org/wiki/CCMP
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

QUESTION 49
An access point has been configured for AES encryption but a client is unable to connect to it. Which of the following should be configured on the client to fix this issue?

A. WEP
B. CCMP
C. TKIP
D. RC4

Correct Answer: B
Explanation

Explanation/Reference:
CCMP is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC

(CCM) of the AES standard.

Incorrect Answers:
A: WEP is based on RC4, and does not use AES.
C: TKIP is a basis for WPA.
D: RC4 is the basis of WEP.

References:
http://en.wikipedia.org/wiki/CCMP
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 59, 60.

QUESTION 50
A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

A. Change the encryption from TKIP-based to CCMP-based.
B. Set all nearby access points to operate on the same channel.
C. Configure the access point to use WEP instead of WPA2.
D. Enable all access points to broadcast their SSIDs.

Correct Answer: A
Explanation

Explanation/Reference:
CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Incorrect Answers:
B: Wireless APs with overlapping signals should use unique channel frequencies to reduce interference between them.
C: WEP is not a secure encryption protocol.
D: This will make the network visible, and open for attacks.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 178.
https://technet.microsoft.com/en-us/library/cc783011(v=ws.10).aspx

QUESTION 51
The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

A. WEP
B. WPA2 CCMP
C. Disable SSID broadcast and increase power levels
D. MAC filtering

Correct Answer: B
Explanation

Explanation/Reference:
CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Incorrect Answers:
A: WEP is not a secure encryption protocol.
C: This will only cloak the network, and increase the signal strength.
D: MAC filtering is vulnerable to spoof attacks.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 178.

QUESTION 52
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

Correct Answer: D
Explanation

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

Incorrect Answers:
A, B, C: These are not used by CCMP

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 250.

QUESTION 53
Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

A. Placement of antenna
B. Disabling the SSID
C. Implementing WPA2
D. Enabling the MAC filtering

Correct Answer: A
Explanation

Explanation/Reference:

You should try to avoid placing access points near metal (which includes appliances) or near the ground. Placing them in the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

Incorrect Answers:
B: This option would "cloak" the network, not limit its signal strength.
C: This deals with authentication and would not make sure that the network is inaccessible from the parking area.
D: This would require clients to furnish the security administrator with their device's MAC address.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 177, 178, 183.

QUESTION 54
A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

A. Antenna placement
B. Interference
C. Use WEP
D. Single Sign on
E. Disable the SSID
F. Power levels

Correct Answer: AF
Explanation

Explanation/Reference:
Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot.
Incorrect Answers:
B: Interference could disrupt the signal in the building as well.
C: WEP is not a secure encryption protocol.
D: This allows users access to all the applications and systems they need when they log on.
E: This option would "cloak" the network, not limit its signal strength.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 149, 171, 177, 183.

QUESTION 55
Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

A. Implement TKIP encryption
B. Consider antenna placement
C. Disable the SSID broadcast
D. Disable WPA

Correct Answer: B
Explanation

Explanation/Reference:
Cinderblock walls, metal cabinets, and other barriers can reduce signal strength significantly.
Therefore, antenna placement is critical.

Incorrect Answers:
A: This option deals with encryption, not signal strength.
C: This option would "cloak" the network, not limit its signal strength.
D: This option deals with authentication, not signal strength.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 173, 177, 183.

QUESTION 56
Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be.
Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients?

A. Enable MAC filtering on the wireless access point.
B. Configure WPA2 encryption on the wireless access point.
C. Lower the antenna's broadcasting power.
D. Disable SSID broadcasting.

Correct Answer: C
Explanation

Explanation/Reference:
Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

Incorrect Answers:
A: This would require clients to furnish the security administrator with their device's MAC address.
B: This would require clients to ask for Wi-Fi access.
D: Clients would not be able to detect the Wi-Fi network.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 177, 178, 183.

QUESTION 57
After reviewing the firewall logs of her organization's wireless APs, Ann discovers an unusually high amount of failed authentication attempts in a particular segment of the building. She remembers that a new business moved into the office space across the street. Which of the following would be the BEST option to begin addressing the issue?

A. Reduce the power level of the AP on the network segment

B. Implement MAC filtering on the AP of the affected segment
C. Perform a site survey to see what has changed on the segment
D. Change the WPA2 encryption key of the AP in the affected segment

Correct Answer: A
Explanation

Explanation/Reference:
Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

Incorrect Answers:
B: MAC filtering is an option further down the line. If reducing the amount of output resolves the issue, the administrative effort will be much less that have to compile a list of the MAC addresses associated with users' computers and then entering those addresses.
C: A site survey is recommended when laying out a network.
D: The fact that Ann has found failed authentication attempts shows that the WPA2 encryption is not the real issue.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 177, 178.

QUESTION 58
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

Correct Answer: B
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A: The 15 cm long vertical element you see on most Wi-Fi equipment is actually a dipole antenna. It consists of two elements and is popular because of its omnidirectional radiation pattern.
C: A sector antenna is a type of directional microwave antenna with a sector-shaped radiation pattern. The word "sector" is used in the geometric sense; some portion of the circumference of a circle measured in degrees of arc. 60? 90?and 120?designs are typical, often with a few degrees 'extra' to ensure overlap and mounted in multiples when wider or full-circle coverage is required.
D: An omnidirectional antenna is designed to provide a 360-degree pattern and an even signal in all directions

References:
http://en.wikipedia.org/wiki/Yagi-Uda_antenna
http://www.techrepublic.com/blog/data-center/80211-time-to-clear-up-some-antenna- misconceptions/ http://en.wikipedia.org/wiki/Sector_antenna#See_also
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 178.

QUESTION 59
A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

A. The old APs use 802.11a
B. Users did not enter the MAC of the new APs
C. The new APs use MIMO
D. A site survey was not conducted

Correct Answer: D
Explanation

Explanation/Reference:
To test the wireless AP placement, a site survey should be performed.

Incorrect Answers:
A: 802.11a operates in the 5 GHz frequency spectrum, and is therefore less likely to have disconnections and slow network connectivity.
B: Entering the MAC address will not prevent disconnections, or speed up network connectivity.
C: This cannot be the cause because MIMO would increase network availability.

References:
https://technet.microsoft.com/en-us/library/dd348467(v=ws.10).aspx http://en.wikipedia.org/wiki/MIMO http://en.wikipedia.org/wiki/IEEE_802.11a-1999

QUESTION 60
Three of the primary security control types that can be implemented are.

A. Supervisory, subordinate, and peer.
B. Personal, procedural, and legal.
C. Operational, technical, and management.
D. Mandatory, discretionary, and permanent.

Correct Answer: C
Explanation

Explanation/Reference:
The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical.

Incorrect Answers:
A: Supervisory, subordinate and peer are not primary security control types.

B: Personal, procedural and legal controls are subsections of managerial control types.
D: Mandatory, discretionary and permanent control types are methods of access control that can be implemented.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 26-27 http://www.professormesser.com/security-plus/sy0-401/control-types-2/

QUESTION 61
Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?

A. Authentication
B. Blacklisting
C. Whitelisting
D. Acceptable use policy

Correct Answer: C
Explanation

Explanation/Reference:
White lists are closely related to ACLs and essentially, a white list is a list of items that are allowed.
Incorrect Answers:
A: Authentication is always required when applications are installed and uninstalled and to log in to an application.
B: Black lists are exactly the opposite of white lists in that it is essentially a list of items that are not allowed.
D: Acceptable use policy describe how the employees in an organization can use company systems and resources, both software and hardware.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 24, 221 http://searchsecurity.techtarget.com/definition/application-whitelisting

QUESTION 62
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management
B. Administrative
C. Technical
D. Operational

Correct Answer: C
Explanation

Explanation/Reference:
controls such as preventing unauthorized access to PC's and applying screensavers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection.

Incorrect Answers:
A: Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment.
B: Administrative tools are used when applying technical control types.
D: Operational control types include Personnel Security, Physical and Environmental Protection, Contingency planning, Configuration Management, Maintenance, System and Information Integrity, Media Protection, Incident Response and Awareness and Training.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 27

QUESTION 63
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Correct Answer: B
Explanation

Explanation/Reference:
Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category.

Incorrect Answers:
A: Logon banners are configuration management which is an operational control type.
C: SYN attack prevention is done by exercising technical control measures.
D: ACLs are technical control measures.

References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 27

QUESTION 64
Which of the following can result in significant administrative overhead from incorrect reporting?

A. Job rotation
B. Acceptable usage policies
C. False positives
D. Mandatory vacations

Correct Answer: C
Explanation

Explanation/Reference:
False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: