Vendor: CWNA

Exam Code: PW0-204

Exam Name: Certified Wireless Security Professional (CWSP)

Version: Demo

Question Set 1

QUESTION 1
In an effort to optimize WLAN performance ABC Company has already upgraded their infrastructure from 802 11b/g to 802 11n. ABC has always been highly security conscious but they are concerned with security threats introduced by incompatibilities between 802.11n and 802.11a/g in the past. ABC has performed manual and automated scans with products that were originally designed for use in 802 11a/g networks. Including laptop- based spectrum and protocol analyzers as well as an overlay 802 11a/g WIPS solution. ABC has sought your input to understand and respond to potential security threats.

In ABC's network environment, what type of devices would be capable of identifying rouge APs that use HT Greenfield 40 MHZ channels? (Choose 3)

A. 802.11n WPS sensor with a single 2x2 radio
B. The company's current laptop-based protocol analysis tools
C. WIPS solution that is integrated in the company's AP infrastructure
D. The company's current overlay WIPS solution
E. The company's current laptop-based spectrum analysis tools

Correct Answer: ABC
Explanation

Explanation/Reference:

QUESTION 2
Given: A new Access point is connected to an authorized network segment and is detected wirelessly by a WIPS.
By what method does the WIPS apply a security classification to newly discovered AP?

A. According to the location service profile
B. According to the SNMP MIB table
C. According to the RADIUS rectum attribute
D. According to the site survey template
E. According to the default security policy

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 3
What elements should be addressed by a WLAN security policy? (Choose 2)

A. Verification that administrative passwords are unique to each infrastructure device
B. Enabling encryption to prevent MAC addresses from being sent in clear text
C. Security policy details should be safeguarded from non IT employees to prevent vulnerability exposure
D. End user training for password selection and acceptable network use
E. Social engineering recognition and mitigation technique.

Correct Answer: DE
Explanation

Explanation/Reference:

QUESTION 4
Role-based access control (RBAC) allows a WLAN administrator to perform that network function?

A. Allows access to specific files and applications based on the user's WMM AC.
B. Provide admission control to VoWiFi clients on selected access points.
C. Allows one user group to access an internet gateway while denying internet access gateway to another group
D. Provide differing levels of management access to a WLAN controller based on the user account.
E. Allow simultaneous support of multiple EAP types on a single Access point.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 5
The following numbered items show the contents of the four frames exchanged during the 4-way handshake.

1. Encrypted GTK sent
2. Confirmation of temporal key installation
3. Announce sent from authenticator to supplicant, unprotected by MIC
4. Snonce sent from applicant to authenticator, protected by MIC. Arrange the frames in the correct sequence beginning with the start of the 4-way handshake

A. 3, 4, 1, 2
B. 2, 3, 4, 1
C. 1, 2, 3, 4
D. 4, 3, 1, 2

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 6
What 802 11 WLAN security problem is addressed by 802.1X/EAP mutual authentication.

A. Disassociation attacks
B. Weak initialization vectors
C. Offline dictionary attacks
D. Weak password policies
E. MAC spoofing
F. Wireless hijacking attacks

Correct Answer: F
Explanation

Explanation/Reference:

QUESTION 7
What disadvantage does EAP-TLS have when compared with PEAPvO EAP/MSCHAPv2 as an 802. 11 WLAN security solution?

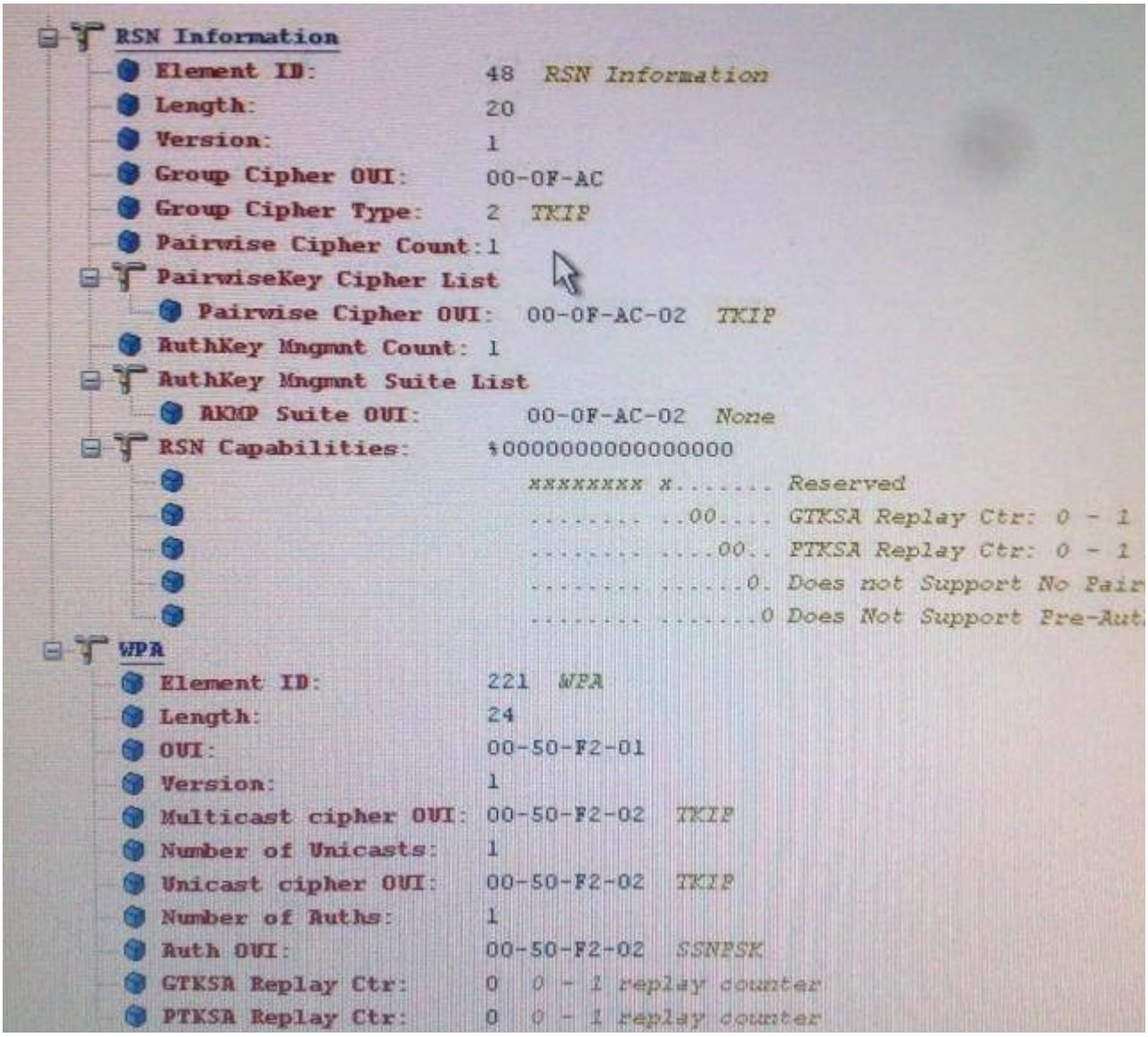
A. EAP-TLS requires a PKI to create X509 certificates for both the server and client, which increases administrative overhead.
B. EAP-TLS does not use SSL to establish a secure tunnel for internal EAP authentication.
C. Fast/secure roaming in an 802 11 RSN is significantly longer when EAP-TLS is use.

D. EAP-TLS does not protect the client's username and password in side an encrypted tunnel.
E. Though more secure EAP-TLS is not widely supported by wireless infrastructure or client vendors.
F. Initially mobility authentication with EAP-TLS is significantly longer due to X509 certificate verification.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 8
Exhibit



Given: The illustration shows a WLAN protocol analyzer decoding an 802.11 beacon frame.
What statement about the access points BSS is true and can be confirmed with this illustration?

A. This is a TSN and stations may use only the TKIP chiper suit.
B. The BSS's group key chiper will be rotated by the access point after two more beacon frames.
C. The BSS supports both CCMP and TKIP chiper suit simultaneously.
D. There is currently one wireless client associated with the AP using TKIP chiper suit within the BSS.
E. The BSS is an RSN, but the only chiper suit supported in BSS is TKIP.

Correct Answer: E
Explanation

Explanation/Reference:

QUESTION 9
Given: You manage a wireless network that services 200 wireless users. Your facility requires 20 access points and you have installed an IEEE 802.1X LEAP with AES CCMP as an authentication and encryption solution.

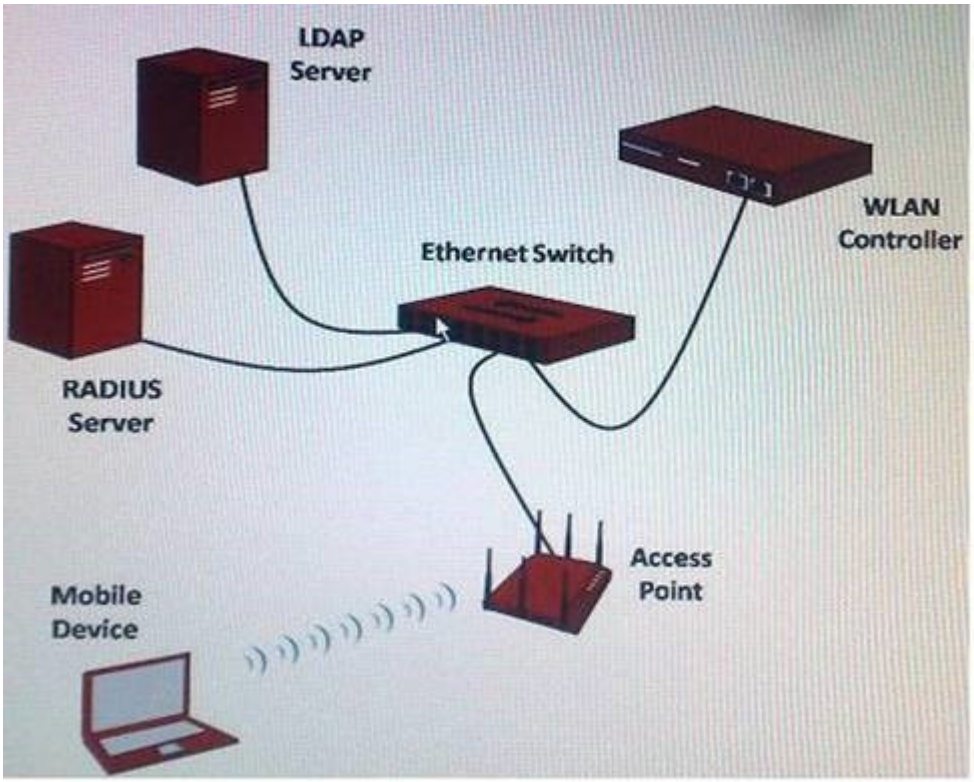
In this configuration the wireless network is initially susceptible to what type of attacks? (Choose 2)

A. Eavesdropping
B. Offline dictionary
C. Layer 1 DoS
D. Session hijacking
E. Man-in-the-middle
F. Layer 3 peer-to-peer

Correct Answer: BE
Explanation

Explanation/Reference:

QUESTION 10
Exhibit



Given: The network in this diagram implements an 802.1X/EAP-based wireless security solution. What device functions as EAP authenticator?

A. Ethernet switch
B. Mobile device
C. LDAP server
D. Access point
E. WLAN controller

F. RADIUS server

Correct Answer: E
Explanation

Explanation/Reference:

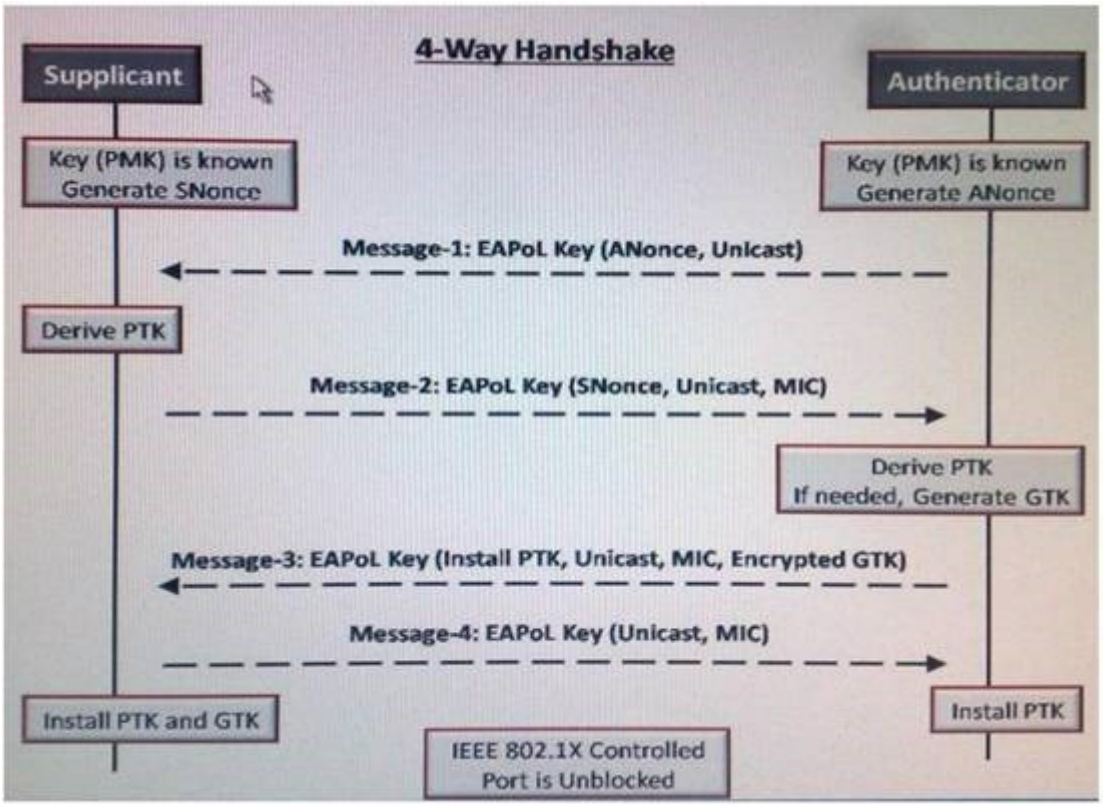
QUESTION 11
What one advantage of using EAP-TTLS instead of EAP-TLS as an authentication mechanism in 802.11WLAN?

A. EAP-TTLS does not require the use of PKI.
B. EAP-TTLS does not require an authenticator server.
C. EAP-TTLS sends encrypted supplicant credentials to the authentication server.
D. EAP-TTLS supports mutual authentication between supplicants and authentication servers.
E. EAP-TTLS supports smart card clients.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 12
Exhibit



In this diagram illustrating an example of IEEE 802.11standard's4-Way handshake what is the purpose of ANonce and Snonce?

A. There are values used in the derivation of the pairwise Transient key.
B. The IEEE 802.11 standard requires that all crypto graphic frames contain a nonce for security purposes.
C. They are used to pad message 1 and message 2 so each frame contains the same number of bytes.

D. They are added together and used as the GMK, from which the GTK is derived.
E. They allow the participating STAs to avoid sending unicast encryption keys across the wireless medium

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 13
You own a coffee shop and have recently installed a 802.11g wireless hot spot for the benefit of your customers. For legal reasons you want to minimize your network and avoid liability related to the operations of hot spots.

What option specifies the best approach to achieve this goal at your public hot-spot?

A. Allow only trusted patrons to use the WLAN
B. Use a WIPS to deauthenticate the malicious stations
C. Require clients STAs to have updated firewall and antivirus software
D. Disable the WLAN during non business hours
E. Use the captive portal to force users to agree to an acceptable use disclaimer
F. Configure WPA2-personal security on your access point
G. Block TCP port 25out bound on the internet router

Correct Answer: E
Explanation

Explanation/Reference:

QUESTION 14
Given: XYZ company has recently installed a controller based WLAN and is using a RADIUS server to proxy authenticate request to an LDAP server user based across controls and would like to use the RADIUS server to facilitate network authorization

What RADIUS features could be used by XYZ to assign the proper network permissions to users during authentication? (Choose 3)

A. The RADIUS server can support vendor-specific attributes in the ACCESS- ACCEPT response which can be used for ASL or firewall assignment.
B. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignments to users.
C. According to database entries, RADIUS can reassign client 801.11assosiations to proper SSID by referring a user name to SSID mapping
D. RADIUS return list attributes can be used to assign permission level, such as read only permission, to users of particular network source.
E. RADIUS can send a VLAN assignment for each authorized user to the VLAN controller in a return list attribute.

Correct Answer: ABE
Explanation

Explanation/Reference:

QUESTION 15
Given: ABC company is developing an IEEE 802.11 complaint wireless security solution using 802.1X/EAP authentication. According to company policy the security should prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security solution features play a role in adhering to this policy requirement? (Choose 2)

A. Group temporal key
B. Message integrity check (MIC)
C. Multi-factor authentication
D. Encrypted passphrase
E. Integrity check value
F. 4-Way handshake

Correct Answer: AF
Explanation

Explanation/Reference:

QUESTION 16
Given: John smith uses a coffee shop's internet hot spot to transfer funds between his checking and saving accounts at his bank's website. The bank's website uses HTTPS protocol to protect sensitive account information. A hacker was able to obtain john's bank account user ID and password and transfers john's money to another account. How did the hacker obtain john's bank Account user ID and password?

A. John uses same username and password for banking that he does for email. John used a pop3 email client at the wireless hot-spot to check the email and the user ID and password were not encrypted.
B. The bank's web server is using anX509 certificate that is no signed by a root CA, causing the user ID and password to be sent unencrypted
C. John's bank is using an expiredX509 certificate on there web server. The certificate is on john's certificate Revocation list (CRL), causing the user ID and password to be sent unencrypted.
D. Before connecting to the banks website, johns association to the AP was hijacked.
The Attacker interrupted the HTTPS public encryption key from the bank's web server and has decrypted john's login credentials in real time.
E. John accessed his corporate network with the IPSec VPN software at the wireless hot-spot. An IPSec VPN only encrypts data, so the user ID and password were sent in clear text. John uses the same username and password for banking that he does for his IPSec VPN software.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 17
What statement accurately describes the functions of the IEEE 802.1X standard?

A. Port-based access control with support for EAP authentication and AES-CCMP encryption only
B. Port-based access control with encryption key management and distribution
C. Port-based access control with support for authenticated-user VLANs only
D. Port-based access control with 802.3 and 802.11 LANs
E. Port-based access control with permission for three frame types: EAP, DHCP, DNS.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 18
Company's 500 employees use ABC's dual band HT 802.11 WLAN extensively general data traffic, VoWiFi, and guest access internet-only data. Size and network applications, what solution effects common and recommended security practices for this type of network?

A. His high security requirements, support EAT-TLS for corporate data and VoWiFi, require WPA or WPA2-personal as well as MAC address filtering for all guest solutions. Segment each data type using a separate data type SSID, frequently band, and VLAN.
B. WPA2-Personal for corporate data and VoWiFi application with a long passphrase. For guest access, implementation open authentication. Configure two and VLAN-one for corporate access and one for guest access-and support WMM on the corporate network. For ease-of-use and net work discovery hide the corporate broad cast to the guest SSID.
C. PEAPvO/EAP-MSCHAPv2 for corporate data end VoWiFi, use open authentication with captive portal on the guest network. If the VoWiFi phones can not support, use WPA2-personal with a string passphrase. Segment the three types of traffic by using separate SSIDs and VLANs.
D. WPA2 enterprise for all types of network access. For added configuration simplicity, authenticate all users from a single VLAN but apply filtering with IP ACLs by giving each user to group using RADIUS group attributes. Configure the IPACLs so that each group can only access the necessary resources.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 19
Given: A VLAN consultant has just finished installing a WLAN controller with 15 controller based APs. Two SSIDs with separate VLANs are configured for this network and LANs are configured to use the same RADIUS server. The SSIDs are configured as follows

SSID Blue -VLAN 10-lightweight EAP (LEAP) authentication-CCMP cipher suit SSID Red - VLAN 20-802.1X/PEAPv0 authentication-TKIP cipher suit

The consultants computer can successfully authenticate and browse the internet when using the Blue SSID. The same computer can authenticate when using the Red SSID.
What is most likely cause of problem

A. The consultant does not have a valid Kerberos ID on the Blue VLAN.
B. The TKIP cipher suit is not a valid option for 802.1 X/PEAPv0 authentications.
C. The clock on the consultant's computer post dates the RADIUS server's certificate expiration date/time.
D. PEAPv0 authentication is not supported over controller based access points.
E. The red VLAN does not support certificate based authentication traffic.

Correct Answer: E
Explanation

Explanation/Reference:

QUESTION 20
After completing the installation of new overlay WIPS, what baseline function MUST be performed?

A. Approved 802.1X/EAP methods need to be selected and confirmed.
B. Configure specifications for upstream and down stream throughout thresholds.
C. Classify the authorized, neighbor, and rogue WLAN devices.
D. Configure profiles for operation among different regularity domains.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 21
What different security benefits are provided by endpoint security solution software? (Choose 3)

A. Can collect statistics about a user's network use and monitor network threats while they are connected.
B. Must be present for support of 802.11k neighbor reports, which improves fast BSS transitions.
C. Can be use to monitor and prevent network activity from nearby rogue clients or APs.
D. Can prevent connections to networks with security settings that do not confirm to company policy.
E. Can restrict client connections to network with specific SSIDs and encryption types.

Correct Answer: ADE
Explanation

Explanation/Reference:

QUESTION 22
What software and hardware tools are used together to hijack a wireless station from the authorized wireless network in to an unauthorized wireless networks? (Choose 2)

A. A low-gain patch antenna and terminal emulation software
B. Narrow band RF jamming devices and wireless radio card
C. DHCP server software and access point software
D. A wireless work group bridge and protocol analyzer
E. MAC spoofing software and MAC DOS software

Correct Answer: BC
Explanation

Explanation/Reference:

QUESTION 23
Given: ABC company is implementing a secure 802.11WLAN at there head quarters building in New York and at each of the 10 small, remote branch offices around the country 802.1X/EAP is ABC's preferred security solution. Where possible

At all access points (at the headquarters building and all branch offices) connect to single WLAN controller located at the head quarters building, what additional security considerations should be made? (Choose 2)

A. An encrypted connection between the WLAN controller and each controller-based AP should be used or all branch offices should be connected to the head quarters building a VPN.
B. Remote WIPS sensors should be installed at the headquarters building and at all branch office to monitor and enforce wireless security.
C. RADIUS service should always be provided at branch offices so that user authentication is kept on the local network.
D. Remote management via telnet, SSH, HTTP, HTTPs should be permitted across the WLAN link.

Correct Answer: AB
Explanation

Explanation/Reference:

QUESTION 24
ABC Company uses the wireless network for highly sensitive network traffic. For that reason they intend to protect there network in all possible ways. They are continually researching new network threats and new preventative measure. They are interested in the security benefits of 802.11w, but would like to know its limitations.

What types of wireless attacks are protected by 802.11w? (Choose 2)

A. NAV-based DoS attacks
B. RF DoS attacks
C. Layer 2 Disassociation attacks
D. Robust management frame replay attacks
E. EAPoL flood attacks

Correct Answer: CD
Explanation

Explanation/Reference:

QUESTION 25
The IEEE 802.11 pairwise transient key (PTK) is derived from what cryptographic element?

A. Phase shift key (PSK)
B. Group master key (GMK)
C. Peerkey (PK)
D. Group temporal key (GTK)
E. Pairwise master key (PMK)

Correct Answer: E
Explanation

Explanation/Reference:

QUESTION 26
What wireless authentication technologies build a TLS-encrypted tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)

A. EAP-TTLS
B. EAP-FAST
C. LEAP
D. EAP-MD5
E. MS-CHAPv2
F. PEAPv1/EAP-GTC

Correct Answer: ABF
Explanation

Explanation/Reference:

QUESTION 27
Given: ABC Company has recently installed a WLAN controller and configured it to support WPA2-Enterprise security. The administrator has confirmed a security profile on the WLAN controller for each group within the company (manufacturing, sales, and engineering)

How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller?

A. The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication.
B. The RADIUS server forwards a request for a group attribute to an LDAP database service, and LDAP sends the group attribute to the WLAN controller.
C. The RADIUS server sends a group name return list attribute to the WLAN controller during every

successful user authentication.

D. The RADIUS server sends the list of authenticated users and groups to the WLAN controller as a part of a 4-way handshake prior to user authentication.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 28
Given: Jane Smith works primarily from home and public wireless hot spot rather than commuting to the office. She frequently accesses the office network frequently from her laptop using the 802.11 WLAN.

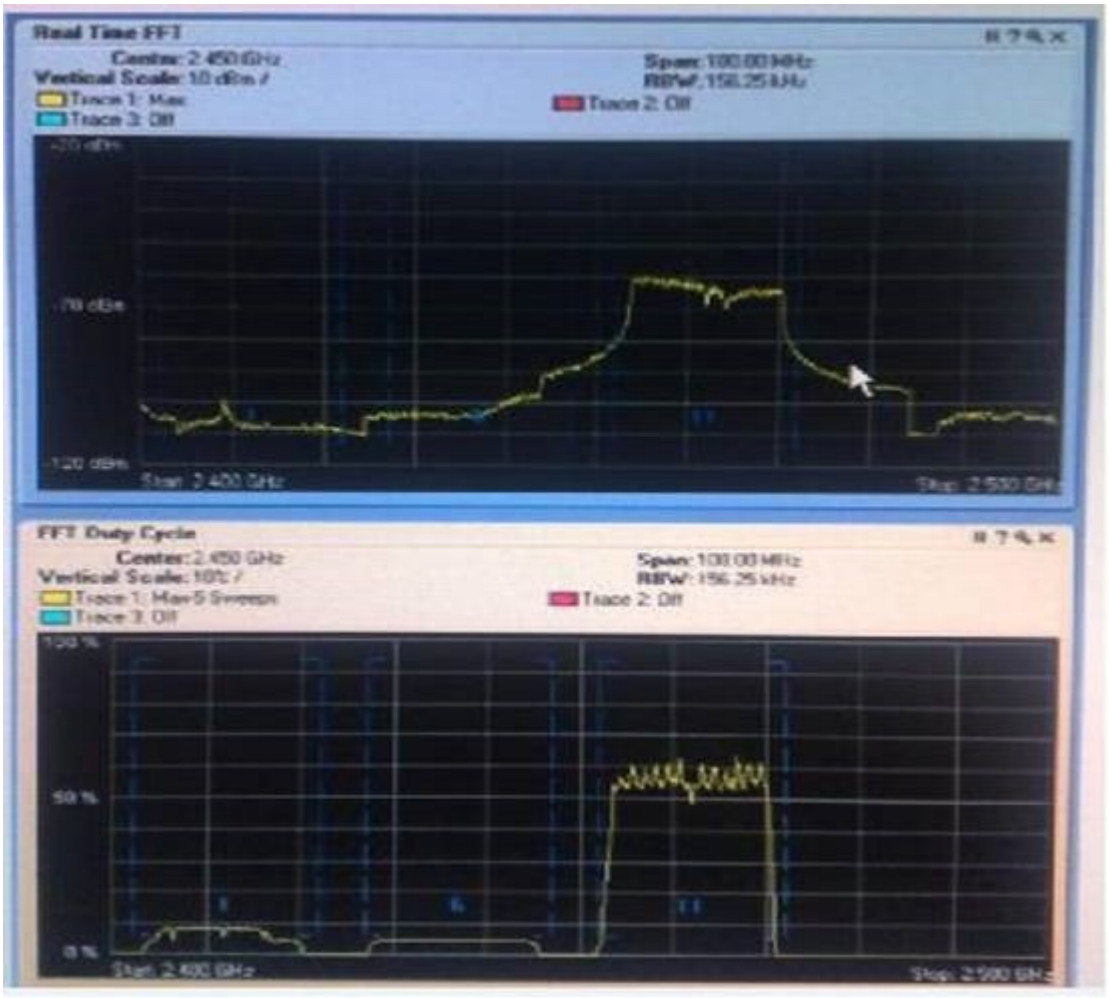
To safeguard her data, what wireless security policy items should be implemented? (Choose 2)

A. Use 802.1X/PEAPv0 to connect to the corporate office network.
B. Use secure protocols, such as FTP, for remote file transfer with encryption.
C. Use an IPSec VPN for connectivity to the office network.
D. Use an HTTPS captive portal for authent6ication at hot spots.
E. Use WIPS sensor software to monitor for risks.
F. Use personal firewall software on her laptop.

Correct Answer: CF
Explanation

Explanation/Reference:

QUESTION 29
Exhibit



What is illustrated on the RF spectrum analyzer?

A. A low-power narrow band RF attacks is in progress on channel 11, causing significant 802.11 interference.
B. A frequency hoping device is being used as a signal jammer on channel 11 only.
C. An HR/DSSS AP and an ERP AP are both operating on channel 11 simultaneously.
D. An ERP AP operating normally on channel 11.

Correct Answer: A
Explanation

Explanation/Reference:

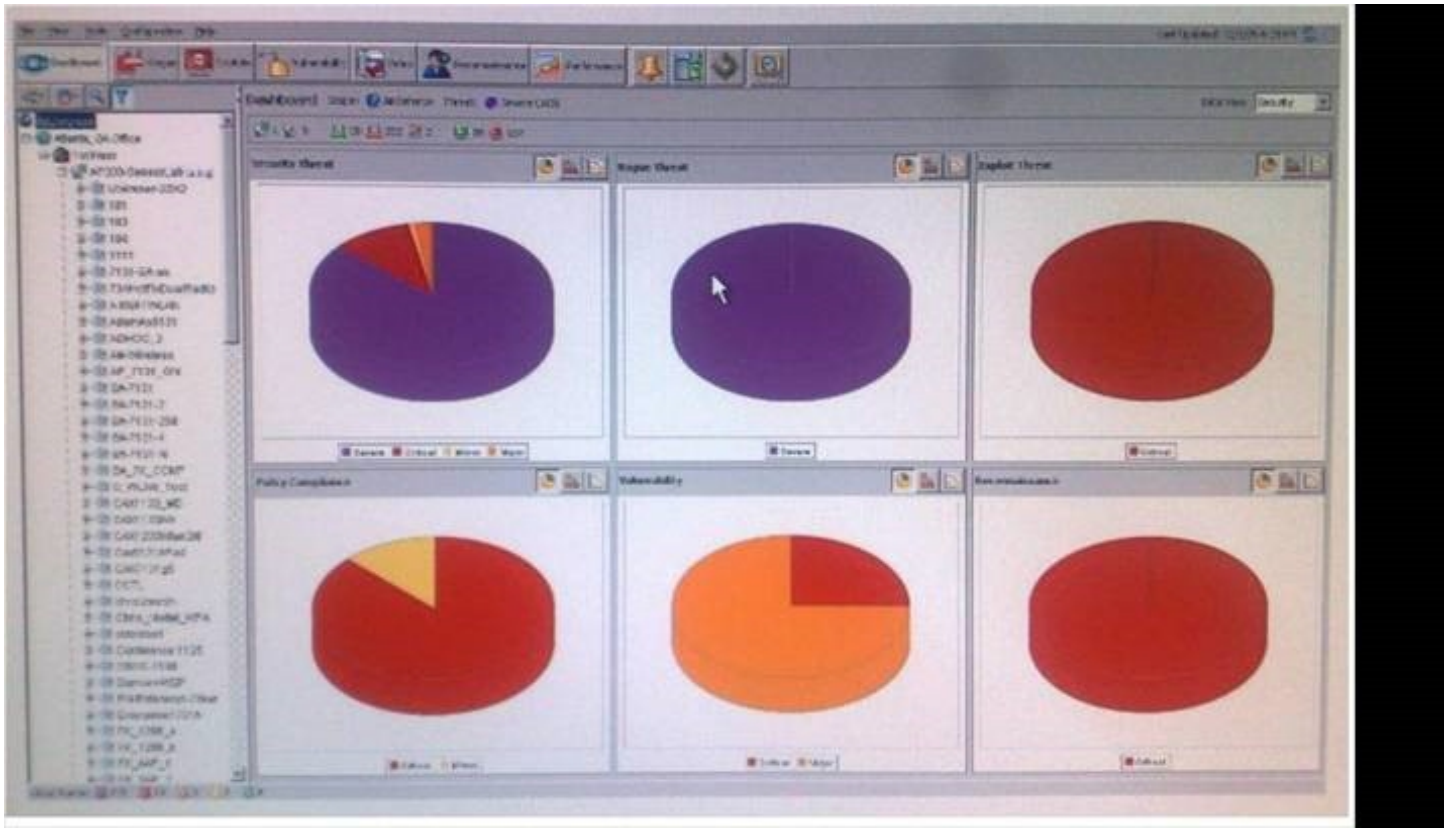
QUESTION 30
What security weakness is presented in pre-RSNA system using 802.1X with dynamic WEP?

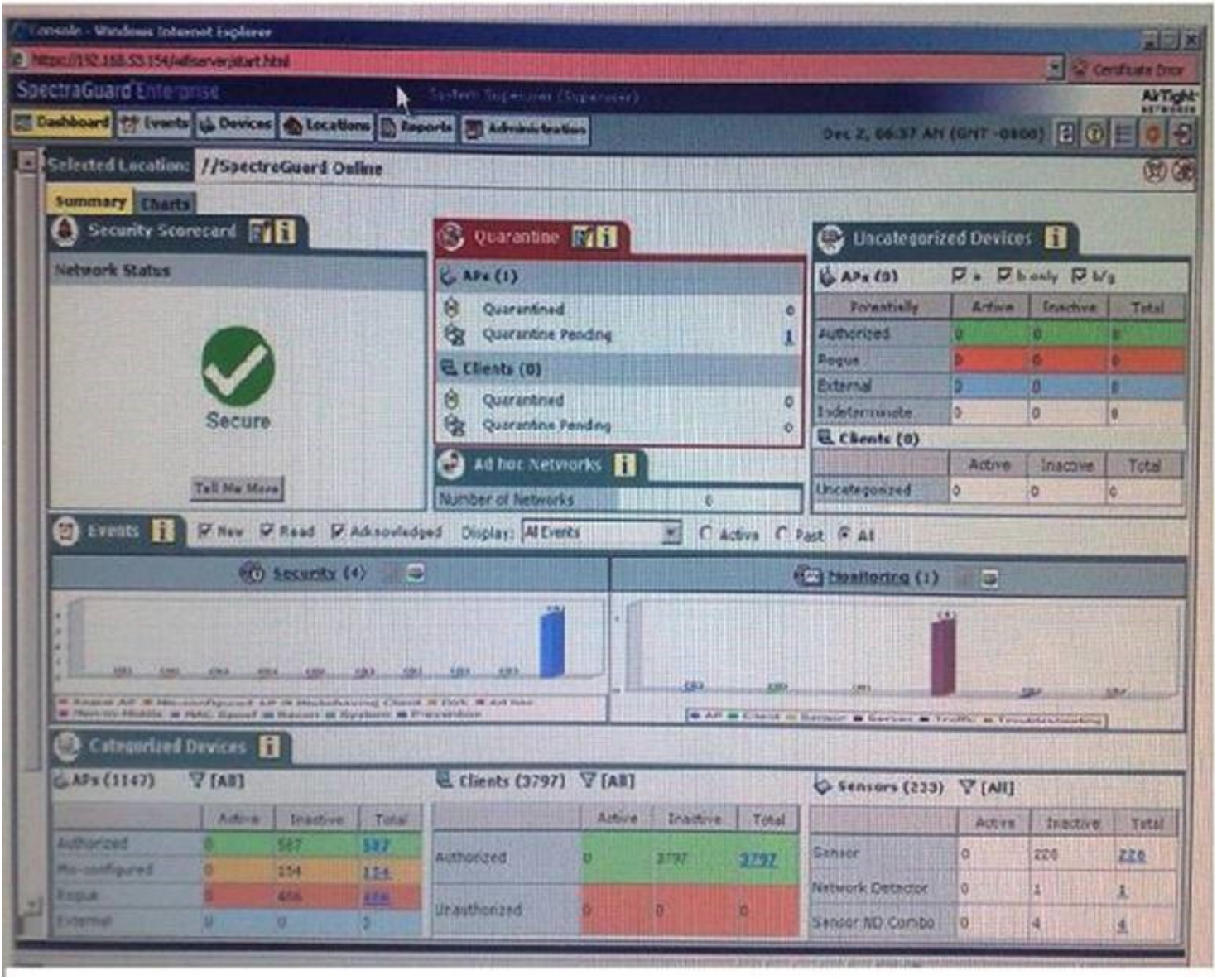
A. There is support for authentication of individual users.
B. All version of EAP used with dynamic WEP pass the user name across the wireless medium in clear text.
C. The session key is crackable if enough traffic is transmitted using the key.
D. With out notification, APs downgrade the security mechanism to 104-bit static WEP when the client device does not support dynamic WEP.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 31
Exhibit





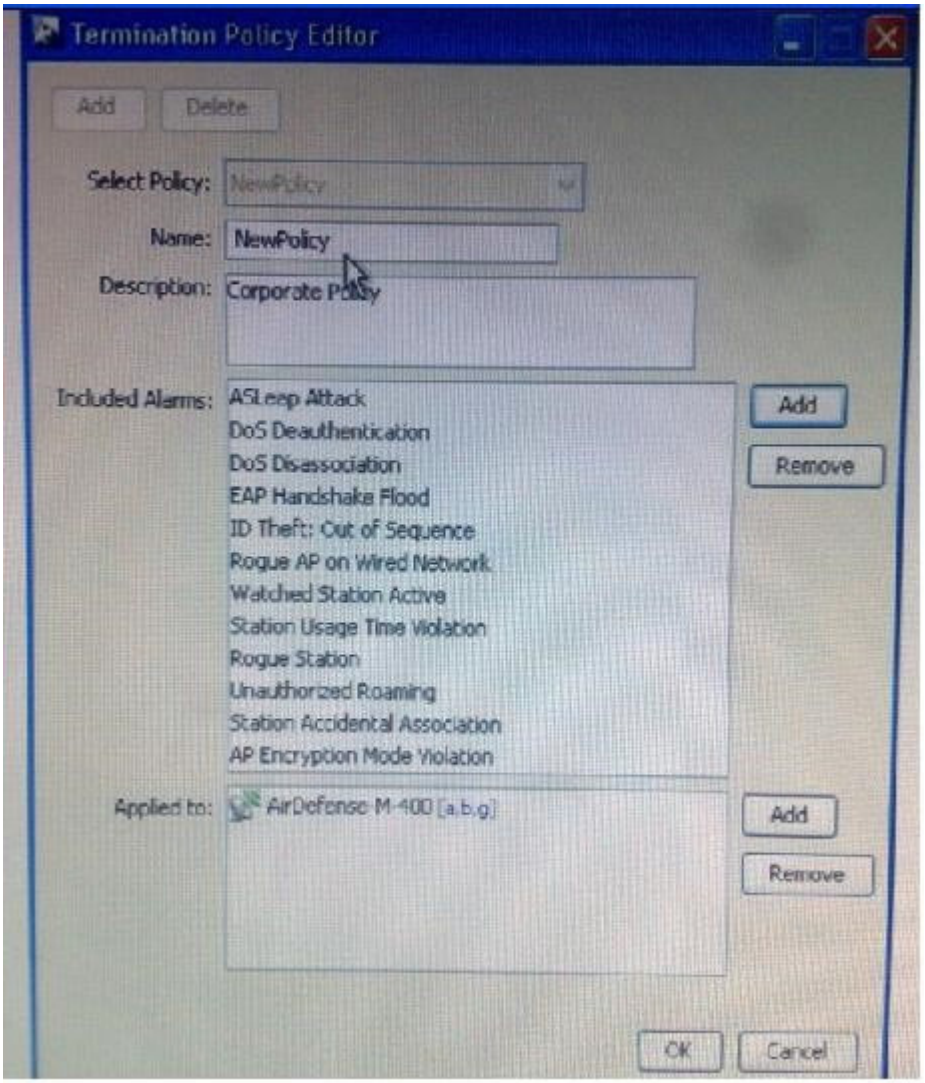
What type of system is installed in graphics?

A. Distributed RF spectrum analyzer
B. Wireless Intrusion Prevention System
C. WLAN Controller Device Monitors
D. WLAN Emulation System
E. Wireless VPN Management System

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 32
Exhibit



Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAP PEAPv0. The company's wireless network action network administrator assured Joe that his laptop was authorized in the WIPS for connectivity to all marketing department APs before it was given to him yesterday the WIPS terminations given to him yesterday. The WIPS termination policy is shown in exhibit.

What is a possible reason that Joe can not connect to the network?

A. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.
B. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. This WIPS responded by disabling the APs.
C. Joe's 802.11radio sending too many probe request and EAPoL start frame due to corrupted driver.
D. Joe configured his 802.11 radio card to transmit at 100mW to increase his SNR.
The WIPS is detecting his much out put power as a DoS attack.
E. Joe changed the system limit on his computer, and WIPS is detecting this as usage time violation.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 33
Given: Many corporations have guest VLANs configured on their WLAN controller that allow visitors to have wireless internet access only.

What risks are associated with implementing the guest VLAN without any protocol filtering features enabled? (Choose 2)

A. Unauthorized users can perform internet based network attacks through the WLAN.
B. Intruders can send spam to the internet through the guest VLAN.
C. Peer-to-peer attacks between the guest users can not be prevented without protocol filtering.
D. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.
E. Guest users can reconfigure APs in the guest VKAN unless unsecure network management protocols (e.g. Telnet, HTTP) are filtered.

Correct Answer: AC
Explanation

Explanation/Reference:

QUESTION 34
What limitations are present with PMK caching (or PMKSA caching) when 802.1X/EAP authentication is in use?

A. PMK caching may only be supported when the authentication server (SA) is collocated with the authenticator, as with WLAN controllers using an internal RADIUS server.
B. PMK caching has a maximum PMKSA storage threshold of five keys, which limits the fast roaming capability to a mobility group of five APs.
C. PMK caching allows to fast roaming between APs when they are managed by a single controller, but it does not support inter-controller handoffs
D. PMK caching can only retain PMKSAs once they are present, but it can not create new PMKSAs without a full 802.1X/EAP authentication nor can it distribute an existing PMKSA to other APs.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 35
In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking?

A. In home networks in which file and pointer sharing is enabled
B. In corporate VoWiFi is networks with push to talk multicast capabilities
C. At public hot-spots in which many clients use diverse application
D. In university environment with multicast training

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 36
As a primary security engineer for a large corporate network you have been asked to author a new security policy for the wireless network while most clients devices support 802.11X authentication some legacy devices still passphrase. When writing the 802.11 security policy, what password related items should be addressed?

A. Password should include a combination of upper and lower case latter, numbers, and special characters.

B. Certificate should always by recommended instead of passwords for 802.11 client authentication.
C. Password complexity should be maximized so that the weak IV attacks are prevented.
D. Password creation process should be defined to maximize the strength of PSK based authentication.
E. MSCHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2=PSK passphrase.

Correct Answer: AD
Explanation

Explanation/Reference:

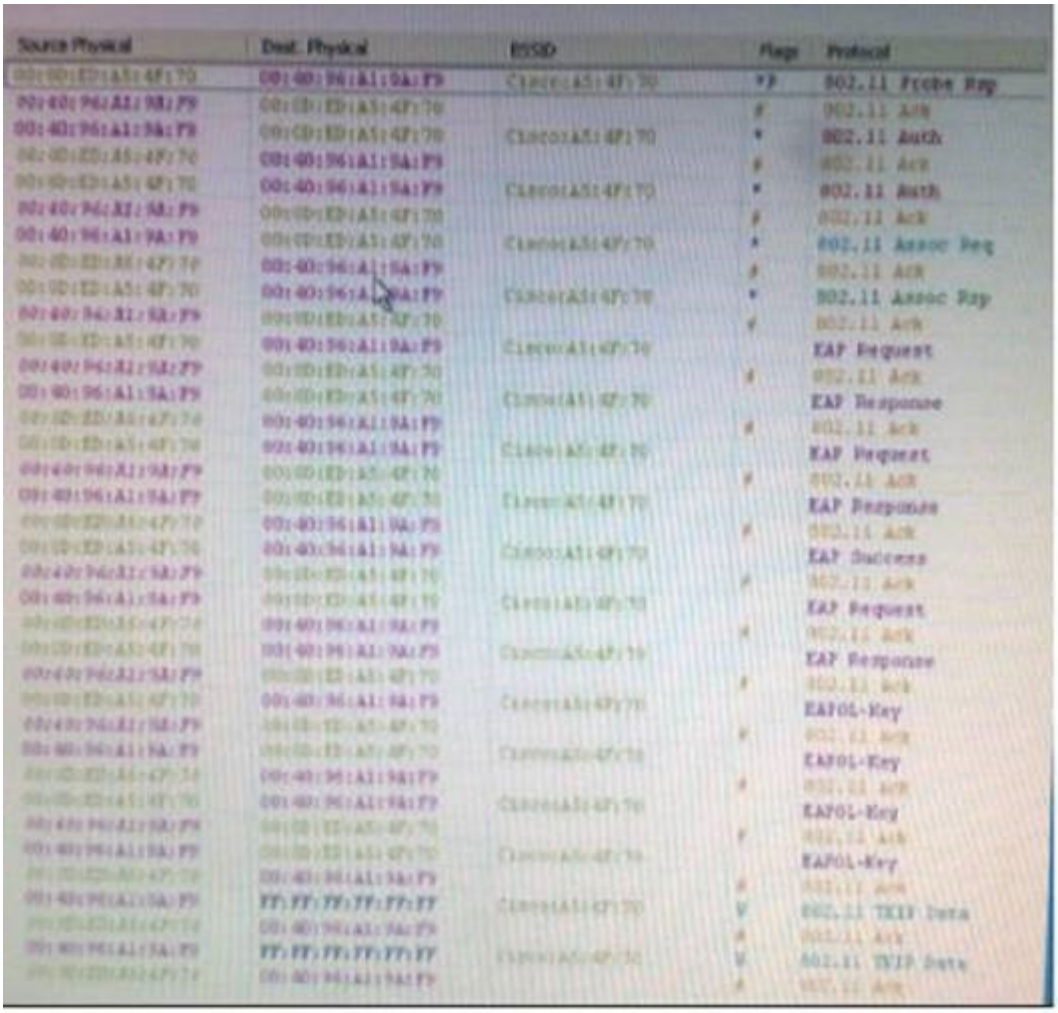
QUESTION 37
When opportunistic key caching (OKC) is supported on the wireless network, what steps must occur before a successful roam is completed? (Choose 2)

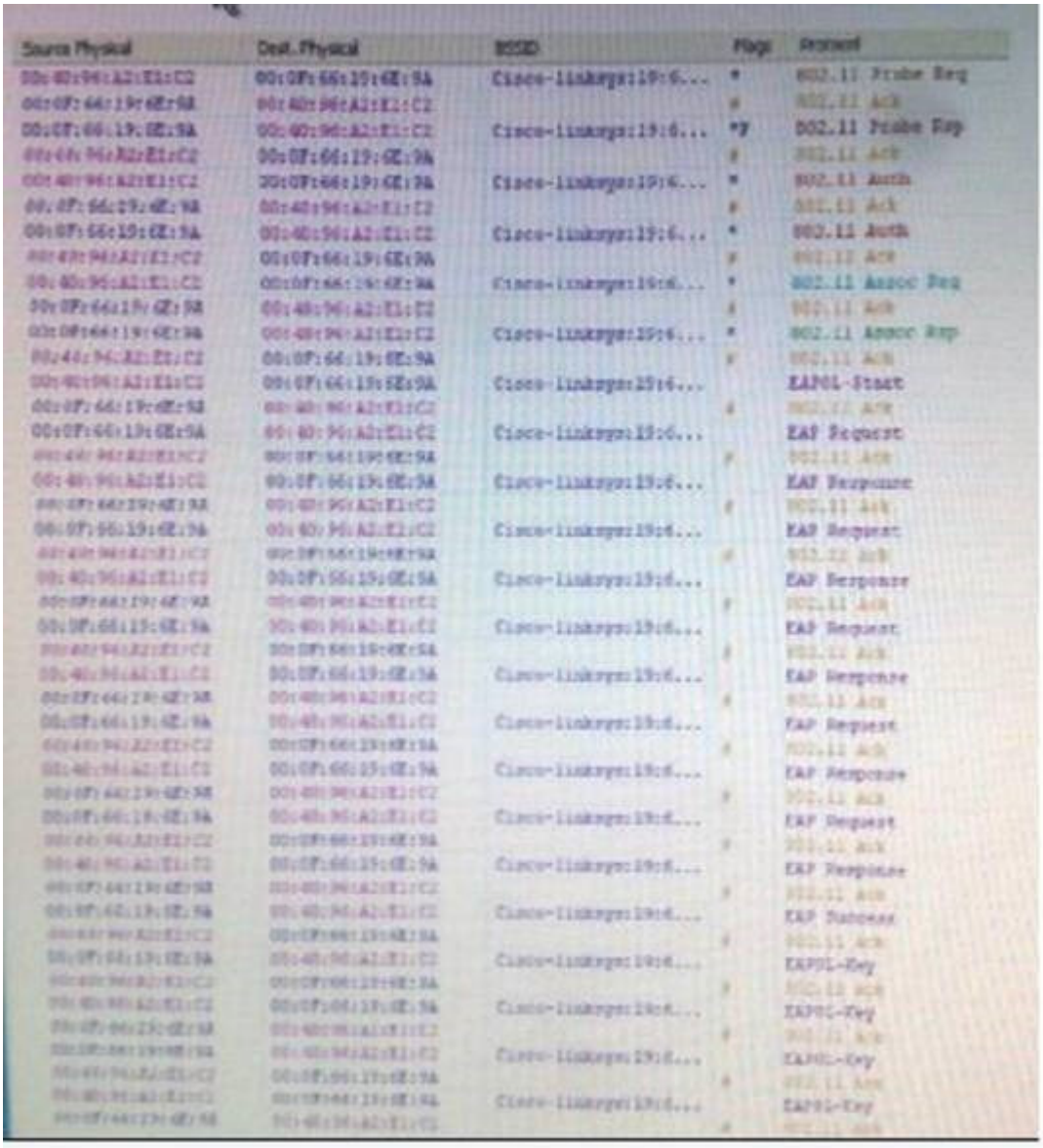
A. EAP authentication must be conducted between the supplicant and AS
B. The AS must be queried for derivation of new PMK
C. The authenticator must query the RADIUS server to validate the supplicant
D. New open system authentication must be performed
E. Supplicant and authenticator must establish a new PTK

Correct Answer: AC
Explanation

Explanation/Reference:

QUESTION 38
Exhibit


Source Physical
Dest. Physical
BSSID
Flags
Protocol
802.11 Probe Req
802.11 Auth
802.11 Assoc Req
802.11 Assoc Rsp
EAP Request
EAP Response
EAP Request
EAP Response
EAP Success
EAP Request
EAP Response
EAPOL-Key
EAPOL-Key
EAPOL-Key
802.11 TKIP Data
802.11 TKIP Data



Choose the statement that explains that why the frame exchanged from Exhibit -1 took more frames than the frames exchanged from Exhibit-2 when both authentication were successful.

A. Exhibit-1 and Exhibit -2 are using different EAP types.
B. Exhibit-2 has transmission of EAP frames.
C. Exhibit-1 is a TSN, and Exhibit-2 is an RSN
D. Exhibit-1 is association and Exhibit-2 is an initial association.
E. Exhibit-1 and Exhibit-2 are using different cipher suits.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 39
What TKIP features prevent attacks against the known weaknesses of WEP? (Choose 3)

A. 32 bit ICV (CRC 32)
B. Sequence counters

C. Michael
D. RC5 stream cipher
E. Block cipher support
F. Increased IV length

Correct Answer: BCF
Explanation

Explanation/Reference:

QUESTION 40
Given: The ABC corporation currently utilizes a public key infrastructure (PKI) to allow employees to securely access network resources using smart cards. The wireless network will use WPA2-Enterprise as its primary security solution. You have been hired to recommend a Wi-Fi alliance tested EAP method

What solutions will require the least change in how users are currently authenticated and still integrate with there existing PKI?

A. PEAPv0/EAP-MSCHAPv2
B. EAP-TLS
C. EAP-TTLS/MSCHAPv2
D. PEAPv0/EAP-TLS
E. LEAP

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 41
Given: Many travelling business users connect to internet at airports, which often have 802.11g access points with a captive portal for authentication.

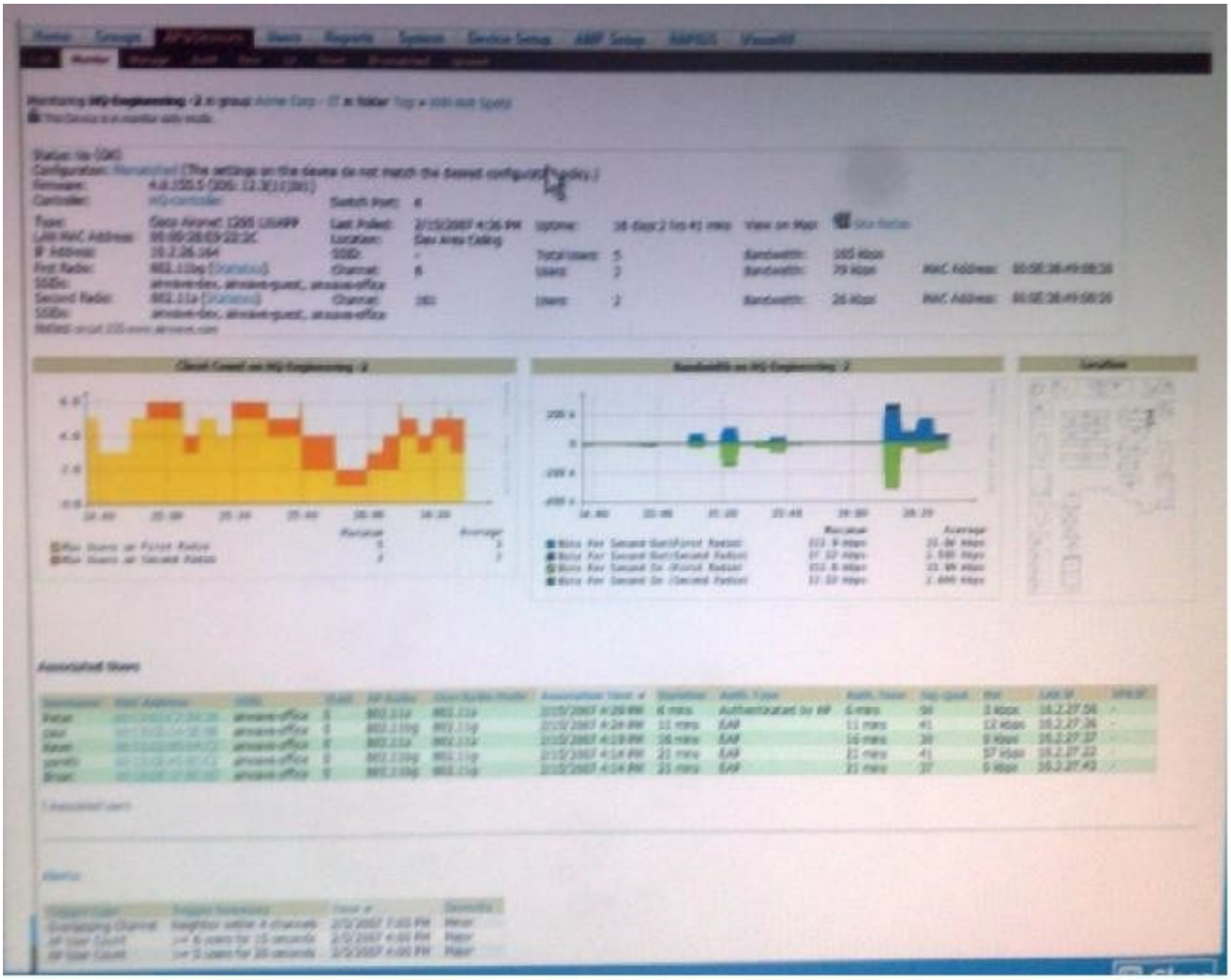
While using an airport hot spot with this security solution, to what type of wireless attack is user susceptible? (Choose 2)

A. IGMP-snooping
B. Man-in-middle
C. Wi-Fi ARP poising
D. Management interface exploits
E. Wi-Fi phishing

Correct Answer: AE
Explanation

Explanation/Reference:

QUESTION 42
Exhibit



Review the exhibit and answer the following question. When monitoring APs within A LAN using a wireless network management system (WNMS, what secure protocol may be used by the WNMS to issue configuration change to APs?

A. TFTP
B. SNMPv3
C. 802.1X/EAP
D. PPTP
E. IPSec/ESP

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 43
What penetative measures are performed by a WIPS against intrusions?

A. Uses SNMP to disable the switch port to which rogue APs connect
B. Deauthentication attack against a classified neighbor AP
C. Evil twin attack against a classified neighbor AP
D. Evil twin attack against a rogue AP
E. EAPoL reject frame flood against AP

Correct Answer: AB
Explanation

Explanation/Reference:

QUESTION 44
Exhibit

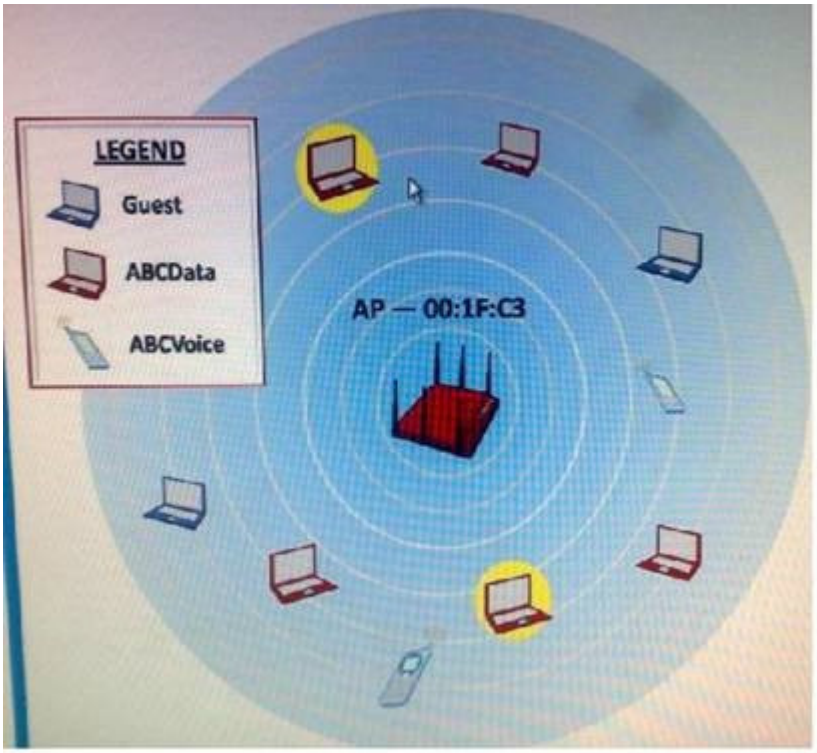
What WLAN security function can be performed by the illustrated software utility? (Choose 3)

A. Generating PMKs that can be imported into 802.11 RSN systems
B. Generating passphrases for WLAN system secured with WPA2-personal
C. Generating random EAP-TTLS session keys
D. Generating passwords for WLAN infrastructure equipment logins
E. Generating high-entropy EAP-TLS passphrase for client authentication
F. Generating secret keys for RADIUS server and WLAN infrastructure devices

Correct Answer: BDF
Explanation

Explanation/Reference:

QUESTION 45
Exhibit



The exhibit shows one of the ABC Company's APs and its associated clients. AP-00:1F:C3is configured with three separate WLAN profile, as follows

1. SSID: guestVLAN90-security: Open with captive portal authentication-2 current clients
2. SSID: ABCData-VLAN 10-security. PEAPv0/EAP\MSCH with AES-CCMP-5 current clients
3. SSID: ABC voice VLAN 10-security:WPA2-personal-2 current clients

Two of the clients stations that are connected via the ABCData SSID are corporate executives. Theses executives are the part of multicast group that is used to share sensitive videos among executive users.

What client stations possess the key that are necessary to decrypt the multicast data packets charring theses sensitive videos?

A. Only the members of executive team that are the part of the multicast group
B. All clients that are associated to AP-00:IF:C3 using the ABCData SSID
C. All clients that are associated to AP:00:IF:C:3 with shared GTK, which includes ABCData and ABC voice
D. All clients that are associated to AP-00:IF:C3 using any SSID

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 46
Given: ABC hospital wishes to create a strong security policy as a first step in securing there 802.11 WLAN
What are the appropriate sections of a WLAN security policy? (Choose 3)

A. Attack classification
B. Physical security of the RF medium
C. Acceptable use of the network
D. SSID broadcasting regulations
E. End-user and administrator training
F. Network audits

Correct Answer: ACE
Explanation

Explanation/Reference:

QUESTION 47
What impact may 802.11w have on the efforts of rogue device containment with an overlay WIPS?

A. 802.11w introduces data integrity protection for some management and action frames, which may limits the methods used by WIPS to disconnect, and mitigate the impact of, rogue AP or client communications
B. 802.11w introduces new mechanisms by which unassociated clients can refuse Deauthentication frames that can not be rejected by APs. This introduces new security concerns for WIPS containing Deauthentication attacks
C. 802.11 introduces a mechanism to Encrypt MAC headers in management and control frames, which have traditionally have been used by WIPS to detect network threats such as hijacking attacks and MAC spoofing
D. 802.11w inadvertently exposes new methods for attacks to exploit TKIP countermeasure using spoofed management frames of legitimate stations. WIPS solutions are in capable of preventing this type of attack

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 48
In An IEEE 802.11-complaint WLAN, when is 802.1X controlled port placed into the unblocked state?

A. After open system authentication
B. After any group handshake
C. After the 4-way handshake
D. After RADIUS authentication

Correct Answer: C
Explanation

Explanation/Reference:

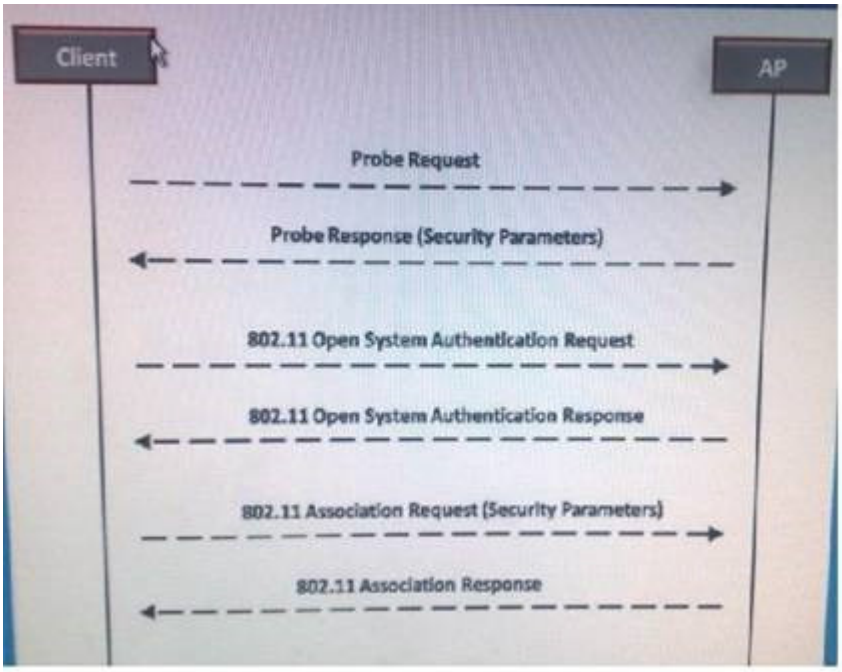
QUESTION 49
When using a tunneled EAP type, what is protected from clear text across the wireless medium?

A. X.509 certificates
B. User credentials
C. EAPoL keys
D. Pairwise Master keys
E. Server credentials

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 50
Exhibit



The illustration shows the 802.11 association procedure from the IEEE 802.11 standard. In a WPA2-Enterprise network what process immediately flows the 802.11 association procedure?

A. 802.1X EAP authentication
B. 4-way handshake
C. Group key handshake
D. RADIUS shared secret lookup
E. DHCP request
F. EAP Passphrase-to-PSK mapping

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 51
Given: WLAN protocol analyzers can read and reject many wireless frame parameters.

What parameter is needed to physically locate rogue APs with a protocol analyzer?

A. signal strength
B. RSNE
C. RSSI
D. IP address
E. Noise Flow

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 52
802.11r introduces new frame exchange protocol to support key management during fast secure transitions. Two of the new exchange protocols are the Over-the air protocol and the other-DS FT protocol.

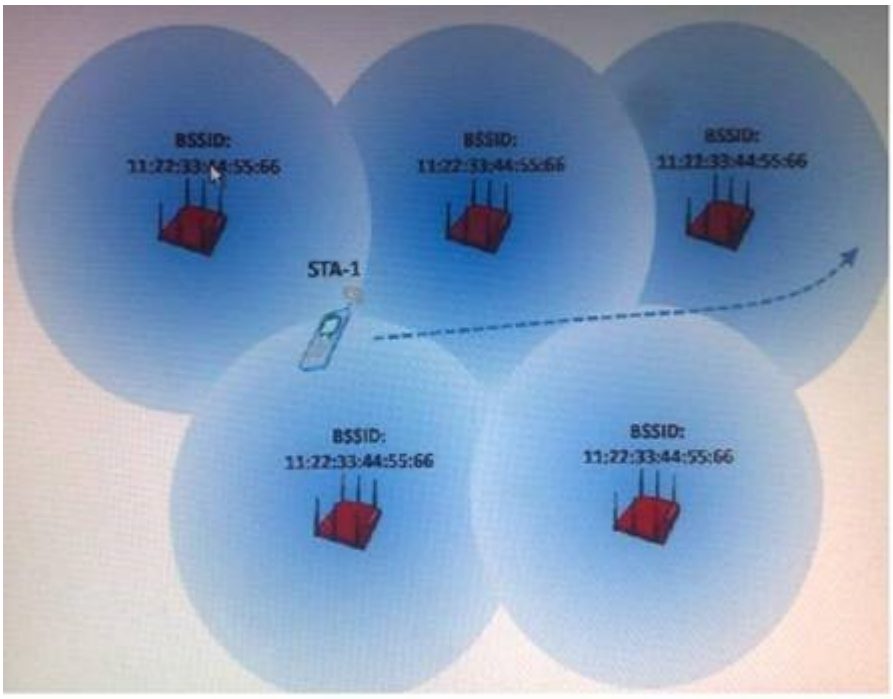
In what ways do these frames exchange protocols differ from each other?

A. In Over-the air protocol sends frames directly to new AP, while the other the DS FT protocol used the old AP to forward the frames to the New AP via the wired network.
B. Over-the air FT protocol uses the 4 way handshake to establish encryption keys, while the over the DS ft protocol does not.
C. Over-the air FT protocol is used during a layer 2 roam, while the over-the-DS FT protocol does not.
D. Over-the air FT protocol used during layer 2 raom, while the over-the-DS FT protocol is used when layer 3 rams are occurring
E. Over-the air FT protocol rules ion 802.11k neighbor reports to initiate roaming decisions, while the other-the DS FT protocol does not.

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 53
Exhibit



ABC Company has deployed single channel architecture (SCA) solution to help overcome some of the common problems with the client roaming. The figure shows the overlapping coverage area of multiple APs in ABC's network. In this network all APs are configured with the same channel and BSSID. PEAPv0/ EAP-MSCHAPv2 is only supported authentication mechanism.
As the VoWiFi client move through out this network, what events are occurring?

A. STA-1 controls when and where to roam by using signal and performance matrices in accordance with the chipset drivers.
B. The WLAN controller is querying the RADIUS server for authentication before STA-1's association is moved from one AP to the next.
C. STA-1 initiates open authentication and 802.11 associations with each AP prior to Roaming.
D. The WLAN controller controls the AP to which STA-1 is associated and transparently moves this association in accordance with STA-1's physical location.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 54
As part of large organization's security policy how should a wireless security professional address to problem of rogue access points?

A. Use a WPA-2 Enterprise complaint security solution with strong mutual authentication and encryption.
B. Hide the SSID of legitimate APs on the network so that intruders cannot copy this parameter on rogue APs.
C. All authorized APs should have there wired ports quarantined to specific VLAN for threat neutralization and analysis.
D. A trained employee should install and monitor and WIPS rogue detection and response measures.
E. Conduct through mutual facility scans with spectrum analyzers to detect rogue AP RF signature.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 55
Given: ABC corporation is selecting a security solution for there new WLAN. Two of there considered solutions PPTP VPN and 802.1XEAP. They have considered a PPTP VPN and because it is included with both server and desktop operating system. With both solutions are considered strong enough to adhere to corporate security police, the company is worried about security weakness of MS-CHAPv2 authentication.

As a consultant what do you tell ABC Corporation about implementing MS-CHAPv2 authentication? (Choose 2)

A. MS-CHAPv2 is secure when implemented with AES-CCMP encryption.
B. MS-CHAPv2 is complaint with WPA-personal, not WPA-2-Enterprise.
C. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS- encrypted tunnel.
D. MS-CHAPv2 uses anonymous differ-Helliman authentication, and therefore secure.
E. MS-CHAPv2 is only secure when combined with WEP.
F. MS-CHAPv2 is subject to offline dictionary attacks.

Correct Answer: CF
Explanation

Explanation/Reference:

QUESTION 56
Given: ABC Corporation's 802.11 WLAN is comprised of a redundant WLAN controller paid and 30-access points. ABC implemented WEP encryption with IPSec VPN technology to secure there wireless communication because it was the strongest security solution available at the time it was implemented. IT management has had decided to upgrade the WLAN infrastructure and implement VoWiFi and is connected with security because most VoWiFi phones do no support IPSec.
As the wireless network administrator, what new security solution would be best for protecting ABC's data?

A. Migrate to a new multi=factor security solution using WPA-2 personal, MAC filtering, SSID holding, stateful packet inspection and RBAC.
B. Migrate corporate data clients to WPA-Enterprise and segment VoWiFi phone by assigning them to a different frequency band.
C. Migrate corporate data and VoWiFi devices to WPA-2 Enterprise with OKC support, and segment VoWiFi data on separate VLAN.
D. Migrate all 802.11 data and devices to WPA-personal, and implement a secure DHCP server to allocate addresses from a segment subnet for the VoWiFi phones.
E. Migrate corporate data clients to WPA-2-Enterprise, and use the RADIUS server to implement MAC-base authentication of VoWiFi phones.

Correct Answer: E
Explanation

Explanation/Reference:

QUESTION 57
Select the answer option that arranges the numbered events in correct time sequence for a client associating to BSS using EAP-PEAPv0/MSCHAPv2.
1) Installation of PTK
2) Installation of 4-way handshake
3) 802.11 association
4) 802.1X uncontrolled port is opened for data traffic
5) Client validates server certificate

A. 1-2-4-2-5
B. 5-3-1-2-4
C. 3-4-2-1-5
D. 5-3-4-2-1
E. 4-3-2-1-5

Correct Answer: C
Explanation

Explanation/Reference:

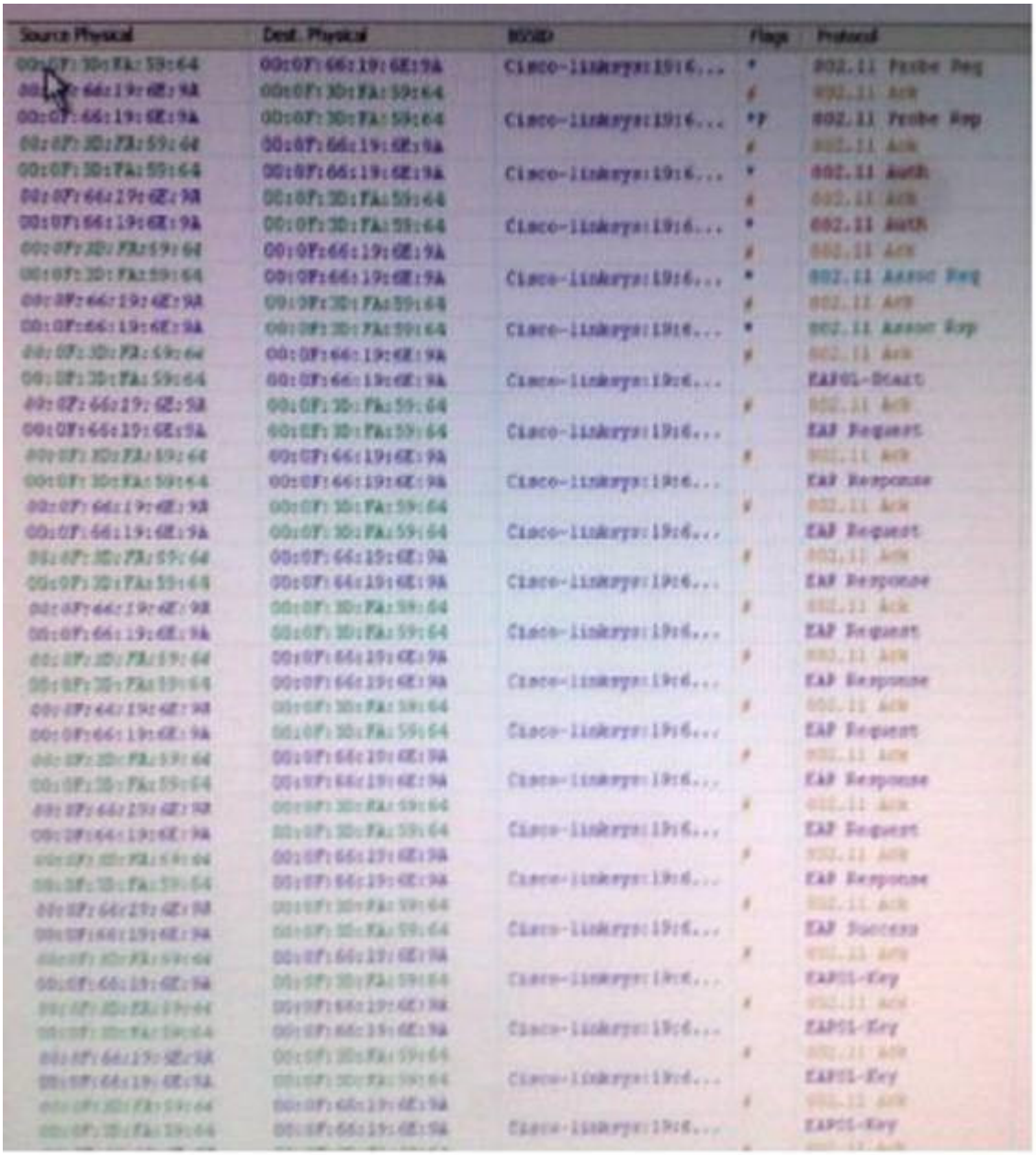
QUESTION 58
When used as portal of WLAN authentication solution, what is rule of LDAP?

A. An authentication server (AS) that communicates directly with, and provide authentication for supplicant.
B. A SQL complaint authentication service capable of encryption key generation and distribution.
C. AnX500 standard compliant database that participates in the 802.1X port-based access control process
D. A data retrieval protocol used by an authentication server such as RADIUS.
E. A role-based access control mechanism for filtering data to/from authenticated stations

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 59
Exhibit



Given:A WLAN protocol analyzer captured the illustrated frame trace of an 802.11g (ERP) client station connecting to an 802.11g access point.

What is shown in included frame trace? (Choose 4)

A. Active scanning
B. WPA2-enterprise authentication
C. 802.11 open system authentication
D. 802.1X with dynamic WEP
E. 4-way handshake

Correct Answer: ABCE
Explanation

Explanation/Reference:

QUESTION 60
What WLAN client device behavior is exploited by an attacker during a hijacking attack?

A. After the initial association and 4-way handshake, client stations and access points do not need to perform another 4-way handshake even if connectivity is lost.
B. When the RF signal between a client and an access point is lost, the client will seek to reassociate with another access point with a different SSID and stronger high quality signal.
C. Client drivers typically scan for a connect to access points in the 22.4GHz band before scanning the 5GHz band.
D. When the RF signal between a client and in an access point is disrupted for more than a few seconds, the client device will repeatedly attempt the reestablish both layer 2 and layer 3 connections.
E. As specified by 802.11 standard, clients using open system authentication must allow direct client-to-client connections, even in infrastructure mode

Correct Answer: D
Explanation

Explanation/Reference:

Question Set 2

QUESTION 1
Which of the following protocols is used to provide on-demand authentication within an ongoing data transmission?

A. LEAP
B. EAP
C. PPTP
D. CHAP

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:
The Challenge Handshake Authentication Protocol (CHAP) is used to provide on-demand authentication within an ongoing data transmission. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost all PPP servers. Answer option A is incorrect. LEAP (Lightweight Extensible Authentication Protocol) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication between a wireless client and a RADIUS server. LEAP allows clients to re-authenticate frequently. The clients get a new WEP key upon each successful authentication. Answer option C is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a remote access protocol. It is an extension of the Point-to- Point Protocol (PPP). PPTP is used to securely connect to a private network by a remote client using a public data network, such as the Internet Virtual private networks (VPNs) use the tunneling protocol to enable remote users to access corporate networks securely across the Internet. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection. Answer option B is incorrect. Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one- time passwords, public keys, etc. It is an extension to Point-to-Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection.

QUESTION 2
Which of the following is a common Windows authentication protocol used by the IEEE 802.1X security standard?

A. TACACS
B. LDAP
C. RADIUS
D. SSL/TLS

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service. When a person or device connects to a network often authentication is required. RADIUS is commonly used by ISPs and corporations managing access to the Internet or internal networks employing a variety of networking technologies, including modems, DSL, wireless and VPNs. It is a common Windows authentication protocol used by the IEEE 802.1X security standard. Answer option A is incorrect. Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon. It uses UDP port 49 as the default port. Answer option B is incorrect. Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services. Answer option D is incorrect. The Secure

Sockets Layer (SSL) and the Transport Layer Security (TLS) protocols are used to provide transport level security for Web services applications.

QUESTION 3
Which of the following authentication processes are specified by the IEEE 802.11 standards? Each correct answer represents a complete solution. Choose all that apply.

A. Open System authentication
B. RADIUS
C. Shared Key authentication
D. EAP

Correct Answer: AC
Explanation

Explanation/Reference:
Explanation:
Open System authentication is the default authentication method used by 802.11 devices. But, in fact, it provides no authentication at all. It exchanges messages between the two wireless devices without using any password or keys. A device configured to use the Open System authentication cannot refuse to authenticate another device. Shared key authentication is an authentication method specified in the 802.11 standard. In this authentication, a static WEP key should be configured on the client. The shared key authentication has the following processes:
1. The client makes a request to the access point for shared key authentication by sending an authentication request.
2. The access point sends authentication response to the client. Authentication response contains challenge text in a clear text format.
3. The client uses its locally configured WEP key to encrypt the challenge text and replies with a subsequent authentication request.
4. If the access point can decrypt the authentication request and retrieve the original challenge text, then it responds with an authentication response that allows the client to access the network.
Answer option B is incorrect. The radius-server key command is used to set the authentication and encryption key for all RADIUS communications between the switch and the RADIUS server. This command runs in the global configuration mode of the switch. In order to disable the key, the no form of this command is used.
Syntax:
Switch(config)#radius-server key {string}
Where the word string is a key used to set authentication and encryption for all RADIUS communications between the switch and the RADIUS server. Answer option D is incorrect. Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one-time passwords, public keys, etc. It is an extension to Point-to-Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection.

QUESTION 4
Which of the following methods are capable of operating in wireless networks? Each correct answer represents a complete solution. Choose all that apply.

A. EAP-TLS
B. LEAP
C. PEAP
D. EAP-TTLS

Correct Answer: BAD
Explanation

Explanation/Reference:
Explanation:
The methods that are capable of operating in wireless networks are as follows:
LEAP: The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary EAP method developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard. There is no native support

for LEAP in any Windows operating system, but it is widely supported by third-party client software most commonly included with WLAN (wireless LAN) devices. Due to the wide adoption of LEAP in the networking industry, many other WLAN vendors claim support for LEAP. EAP-TLS: EAP-Transport Layer Security (EAP-TLS) is an IETF open standard and is well-supported among wireless vendors. The security of the TLS protocol is strong, provided the user understands potential warnings about false credentials. It uses PKI to secure communication to a RADIUS authentication server or another type of authentication server. EAP-TTLS:
EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. It is widely supported across platforms; although there is no native OS support for this EAP protocol in Microsoft Windows, it requires the installation of small extra programs such as SecureW2. EAP-TTLS offers very good security. The client can but does not have to be authenticated via a CA-signed PKI certificate to the server. This greatly simplifies the setup procedure, as a certificate does not need to be installed on every client. After the server is securely authenticated to the client via its CA certificate and optionally the client to the server, the server can then use the established secure connection ("tunnel") to authenticate the client. Answer option C is incorrect. PEAP is not a method operated in wireless networks.

QUESTION 5
John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled.
Which of the following attacks is John performing?

A. Rainbow attack
B. DoS attack
C. Replay attack
D. ARP spoofing

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as a network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to the network. The effects of a DoS attack are as follows: Saturates network resources Disrupts connections between two computers, thereby preventing communications between services Disrupts services to a specific computer Causes failure to access a Web site Results in an increase in the amount of spam A Denial-of-Service attack is very common on the Internet because it is much easier to accomplish. Most of the DoS attacks rely on the weaknesses in the TCP/IP protocol. Answer option C is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Answer option D is incorrect. Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it. ARP spoofing attacks can be run from a compromised host, or from an attacker's machine that is connected directly to the target Ethernet segment. Answer option A is incorrect. The rainbow attack is the fastest method of password cracking. This method of password cracking is implemented by calculating all the possible hashes for a set of characters and then storing them in a table known as the Rainbow table. These password hashes are then employed to the tool that uses the Rainbow algorithm and searches the Rainbow table until the password is not fetched.

QUESTION 6
Which of the following protocols uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers?

A. TFTP
B. HTTPS
C. SCP
D. SSL

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:.Answer option C is incorrect. The SCP protocol sends data in encrypted format. It is used to prevent potential packet sniffers from extracting usable information from data packets. The protocol itself does not provide authentication and security; it relies on the underlying protocol, SSH, to provide these features. SCP can interactively request any passwords or passphrases required to make a connection to a remote host, unlike rcp that fails in this situation. The SCP protocol implements file transfers only. It does so by connecting to the host using SSH and there executes an SCP server (scp). The SCP server program is typically the same program as the SCP client. Answer option A is incorrect. Trivial File Transfer Protocol (TFTP) is a file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). TFTP can be implemented in a very small amount of memory. It is useful for booting computers such as routers which did not have any data storage devices. It is used to transfer small amounts of data between hosts on a network, such as IP phone firmware or operating system images when a remote X Window System terminal or any other thin client boots from a network host or server. The initial stages of some network based installation systems (such as Solaris Jumpstart, Red Hat Kickstart and Windows NT's Remote Installation Services) use TFTP to load a basic kernel that performs the actual installation. TFTP uses UDP port 69 for communication. Answer option B is incorrect. Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure (website security testing) identification of the server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems. Difference from HTTP As opposed to HTTP URLs which begin with "http://" and use port 80 by default, HTTPS URLs begin with "https://" and use port 443 by default. HTTP is insecure and is subject to man-in-the-middle and eavesdropping attacks which can let attackers gain access to website accounts and sensitive information. HTTPS is designed to withstand such attacks and is considered secure.

QUESTION 7
You have been hired to perform a penetration test on a client's network. You want to see if remote connections are susceptible to eavesdropping or perhaps session hijacking. Which network tool would be most helpful to you?

A. Vulnerability analyzer
B. Port scanner
C. Performance analyzer.
D. Protocol analyzer

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

A protocol analyzer allows you to view a network conversation and to see the text in English. If the conversation is not encrypted a protocol analyzer will quickly discover this vulnerability. Answer option B is incorrect. A port scanner can be used to find vulnerable ports and services, but not weaknesses in remote connections.

QUESTION 8

Which of the following wireless network security solutions refers to an authentication process in which a user can connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?

A. Remote Authentication Dial-In User Service (RADIUS)
B. IEEE 802.1x
C. Wired Equivalent Privacy (WEP)
D. Wi-Fi Protected Access 2 (WPA2)

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-topoint connection or preventing it if authentication fails. IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 which is known as "EAP over LANs" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004. The EAPOL protocol was also modified for use with IEEE 802.1AE (MACSec) and IEEE 802.1AR (Secure Device Identity / DevID) in 802.1X-2010. Answer option C is incorrect. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream. Answer option A is incorrect. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, Web servers, etc. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port- based authentication, and the Network Access Server, are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine. RADIUS serves three functions: To authenticate users or devices before granting them access to a network. To authorize those users or devices for certain network services. To account for usage of those services. Answer option D is incorrect. WPA2 is an updated version of WPA. This standard is also known as IEEE 802.11i. WPA2 offers enhanced protection to wireless networks than WPA and WEP standards. It is also available as WPA2-PSK and WPA2- EAP for home and enterprise environment respectively. You work as a Network Administrator for uCertify Inc. You need to secure web services of your company in order to have secure transactions.

QUESTION 9
Which of the following will you recommend for providing security?

A. HTTP
B. VPN
C. SSL
D. S/MIME

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and

Netscape browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:. Answer options D is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email encapsulated in MIME. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy, and data security (using encryption). Answer options A is incorrect. Hypertext Transfer Protocol (HTTP) is a client/server TCP/IP protocol used on the World Wide Web (WWW) to display Hypertext Markup Language (HTML) pages. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when a client application or browser sends a request to the server using HTTP commands, the server responds with a message containing the protocol version, success or failure code, server information, and body content, depending on the request. HTTP uses TCP port 80 as the default port. Answer option B is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet. John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows: It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

QUESTION 10
Which of the following tools is John using to crack the wireless encryption keys?

A. Kismet
B. AirSnort
C. Cain
D. PsPasswd

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option A is incorrect. Kismet is an IEEE 802.11 wireless network sniffer and intrusion detection system.John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

QUESTION 11
Which of the following tools is John using to crack the wireless encryption keys?

A. Kismet
B. AirSnort
C. Cain
D. PsPasswd

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option A is incorrect. Kismet is an IEEE 802.11 wireless network sniffer and intrusion detection system. Fact what is Kismet? Hide Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless car that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard

named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option C is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack Brute force attack Rainbow attack Hybrid attack Answer option D is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows:

QUESTION 12
Which of the following are the important components of the IEEE 802.1X architecture? Each correct answer represents a complete solution. Choose all that apply.

A. Authenticator server
B. Extensible Authentication Protocol (EAP)
C. Supplicant
D. Authenticator

Correct Answer: CAD
Explanation

Explanation/Reference:
Explanation:
The 802.1X standard is designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standards. IEEE 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. In the 802.1X architecture, there are three important components:
1.Supplicant: A user or client (known as the supplicant) who wants to be authenticated. 2.Authenticator server: The authentication server may use the Remote Authentication Dial-In User Service (RADIUS). Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. 3.Authenticator: The authenticator is the network device such as wireless access point. The authenticator acts like a security guard to a protected network. Answer option B is incorrect. Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and Point-to-Point connections. EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.

QUESTION 13
You work as a System Administrator for Tech Perfect Inc. The company has a wireless LAN network. You want to implement a tool in the company's network, which monitors the radio spectrum used by the wireless LAN network, and immediately alerts you whenever a rogue access point is detected in the network. Which of the following tools will you use?

A. Firewall
B. WIPS
C. MFP
D. NAT

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
Wireless intrusion prevention system (WIPS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices. Rogue devices can spoof MAC address of an authorized network device as their own. WIPS uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to

compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices. Answer option D is incorrect. Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a private network to share a global, ISP assigned address. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private. Answer option A is incorrect. A firewall is a combination of software and hardware that prevents data packets from coming in or going out of a specified network or computer. It is used to separate an internal network from the Internet. It analyzes all the traffic between a network and the Internet, and provides centralized access control on how users should use the network. A firewall can also perform the following functions: Block unwanted traffic. Direct the incoming traffic to more trustworthy internal computers. Hide vulnerable computers that are exposed to the Internet. Log traffic to and from the private network. Hide information, such as computer names, network topology, network device types, and internal user IDs from external users. Answer option C is incorrect. MFP (Management Frame Protection) is a method used to detect spoofed management frames. A user can avoid the vulnerabilities by enabling MFP in the Cisco wireless LAN. MFP works with the controller-based thin-AP architecture and the Cisco IOS software-based autonomous APs when they are used in combination with the Cisco Wireless LAN Solutions Engine. Cisco WLAN systems place a digital signature into the management frame. This signature is a field with an encrypted hash to check the message integrity. Only an authorized AP can create it and an authorized receiver can validate the signature. Packets that arrive without digital signatures are ignored.

QUESTION 14
Which of the following methods can be used to detect a rogue access point in order to enhance the security of the network? Each correct answer represents a complete solution.
Choose all that apply.

A. Install WIPS
B. Hide the SSID of all AP
C. Check in the managed AP list
D. Use of wireless sniffing tools

Correct Answer: ADC
Explanation

Explanation/Reference:
Explanation:
Following are the methods of detecting a rogue access point in order to enhance the security of the network: Installing a wireless intrusion prevention system (WIPS) will help in detecting the rogue access point. Wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention). The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. A wireless sniffing tool such as NetStumbler captures information regarding access points that are within its range and helps in securing the network. The rogue access point can be checked in the managed AP list by comparing the wireless MAC address (also called as BSSID) of the access point against the managed access point BSSID list. Answer option B is incorrect. Hiding the SSID of all AP will not help in detecting the rogue access point (AP).

QUESTION 15
Which of the following works as a protocol for providing secure communications between wireless clients and wireless access points?

A. Virtual Private Network
B. Firewall
C. Packet filtering
D. Robust Secure Network

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:
Robust Security Network (RSN) is a protocol for establishing secure communications between wireless clients and wireless access points (WAPs). It is a part of the 802.11i standard. The RSN protocol functions are as follows: The wireless client sends a probe request frame. As a response, the wireless access point (WAP) sends a probe response frame with an RSN information exchange (IE) frame. Now, the wireless client requests for authentication and sends an association request frame. As a response, the wireless access point (WAP) sends an association response frame. Answer option C is incorrect. Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet. Answer option B is incorrect. A firewall is a tool to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Answer option A is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet. The links between nodes of a Virtual Private Network are formed over logical connections or virtual circuits between hosts of the larger network. The Link Layer protocols of the virtual network are said to be tunneled through the underlying transport network.

QUESTION 16
Which of the following is a type of security management for computers and networks in order to identify security breaches?

A. EAP
B. IPS
C. IDS
D. ASA

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. Intrusion detection functions include the following: Monitoring and analyzing both user and system activities Analyzing system configurations and vulnerabilities Assessing system and file integrity Ability to recognize patterns typical of attacks Analysis of abnormal activity patterns Tracking user policy violations Answer option B is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, the IPS can drop the offending packets while still allowing all other traffic to pass. Answer option D is incorrect. Adaptive Security Appliance (ASA) is a new generation of network security hardware of Cisco. ASA hardware acts as a firewall, in other security roles, and in a combination of roles. The Cisco ASA includes the following components: Anti-x: Anti-x includes whole class of security tools such as Anti-virus, Anti-spyware, Anti-spam, etc. Intrusion Detection and Prevention: Intrusion Detection and Prevention includes tools such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for sophisticated kinds of attacks. Note: Earlier Cisco sold firewalls with the proprietary name PIX firewall. ASA is the new edition of security solutions by Cisco. Answer option A is incorrect. Extensible Authentication Protocol, or EAP, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections. It is defined in RFC 3748, which has been updated by RFC 5247. Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most often used in wireless LANs. The WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanism. EAP is an authentication framework, not a specific authentication mechanism. The EAP provides some common

functions and a negotiation of the desired authentication mechanism.

QUESTION 17
Which of the following types of attacks cannot be prevented by a firewall? Each correct answer represents a complete solution. Choose all that apply.

A. Shoulder surfing attack
B. Ping flood attack
C. URL obfuscation attack
D. Phishing attack

Correct Answer: CDA
Explanation

Explanation/Reference:
Explanation:
URL obfuscation attacks, phishing attacks, and shoulder surfing attacks are examples of social engineering attacks. Since these attacks occur as a result of man-made mistakes, they cannot be prevented with the help of any firewall.

QUESTION 18
Which of the following protocols uses public-key cryptography to authenticate the remote computer?

A. SSL
B. Telnet
C. SCP
D. SSH

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:
Secure Shell (SSH) is a protocol that provides strong authentication and secure communications over unsecured channels. It uses public key encryption as the main method for user authentication. SSH secures connections over the Internet by encrypting passwords and other datA. It also protects networks against IP spoofing, packet spoofing, password sniffing, and eavesdropping. SSH uses TCP port 22 as the default
port and operates at the application layer. SSH protocol has the following three components:
1. Transport layer protocol
2. User authentication protocol
3. Connection protocol
Answer option C is incorrect. The SCP protocol sends data in encrypted format. It is used to prevent potential packet sniffers from extracting usable information from data packets. The protocol itself does not provide authentication and security; it relies on the underlying protocol, SSH, to provide these features. SCP can interactively request any passwords or passphrases required to make a connection to a remote host, unlike rcp that fails in this situation. The SCP protocol implements file transfers only. It does so by connecting to the host using SSH and there executes an SCP server (scp). The SCP server program is typically the same program as the SCP client. Answer option A is incorrect. Secure Sockets Layer (SSL), also known as Transport Layer Security (TLS) are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. Answer option B is incorrect. The full form of Telnet is Teletype Network. It is used to connect a computer to a local network (LAN) or the Internet. It can also be used for accessing servers by using a valid user name and password. It is a common way to control Web servers remotely.

QUESTION 19
Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer?

Each correct answer represents a complete solution. Choose two.

A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.
B. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.
C. Attacker can use the Ping Flood DoS attack if WZC is used.
D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Correct Answer: AB
Explanation

Explanation/Reference:
Explanation:
Wireless Zero Configuration (WZC), also known as Wireless Auto Configuration, or WLAN AutoConfig is a wireless connection management utility included with Microsoft Windows XP and later operating systems as a service that dynamically selects a wireless network to connect to based on a user's preferences and various default settings. This can be used instead of, or in the absence of, a wireless network utility from the manufacturer of a computer's wireless networking device. The drivers for the wireless adapter query the NDIS Object IDs and pass the available network names to the service. WZC also introduce some security threats, which are as follows: WZC will probe for networks that are already connected. This information can be viewed by anyone using a wireless analyzer and can be used to set up fake access points to connect. WZC attempts to connect to the wireless network with the strongest signal. Attacker can create fake wireless networks with highpower antennas and cause computers to associate with his access point. Answer option D is incorrect. WZC does not interfere in the configuration of encryption and MAC filtering. Answer option C is incorrect. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs.

QUESTION 20
Which of the following is a part of computer network that is used to prevent unauthorized Internet users from accessing private networks connected to the Internet?

A. Protocol analyzer
B. Wired Equivalent Privacy
C. Intrusion detection system
D. Firewall

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteriA. The four important roles of a firewall are as follows:
1. Implement security policy: A firewall is a first step in implementing security policies of an organization. Different policies are directly implemented at the firewall. A firewall can also work with network routers to implement Types-Of-Service (ToS) policies.
2. Creating a choke point: A firewall can create a choke point between a private network of an organization and a public network. With the help of a choke point the firewall devices can monitor, filter, and verify all inbound and outbound traffic.
3. Logging Internet activity: A firewall also enforces logging of the errors and faults. It also provides alarming mechanism to the network.
4. Limiting network host exposure: A firewall can create a perimeter around the network to protect it from the Internet. It increases the security by hiding internal information. Answer option C is incorrect. Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security

breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. Intrusion detection functions include the following: Monitoring and analyzing both user and system activities Analyzing system configurations and vulnerabilities Assessing system and file integrity Ability to recognize patterns typical of attacks Analysis of abnormal activity patterns Tracking user policy violations Answer option B is incorrect. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream. Answer option A is incorrect. Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

QUESTION 21
Which of the following are the components of wireless intrusion prevention system (WIPS)?
Each correct answer represents a complete solution. Choose all that apply.

A. Sensors
B. Console
C. Supplicant
D. Server

Correct Answer: ADB
Explanation

Explanation/Reference:
Explanation:
WIPS is a network device that is used to prevent unauthorized network access to local area networks and other information assets by wireless devices. WIPS configurations consist of three components: Sensors: These devices contain antennas and radios that scan the wireless spectrum for packets and are installed throughout areas to be protected. Server: The WIPS server centrally analyzes packets captured by sensors. Console: The console provides the primary user interface into the system for administration and reporting. A simple intrusion detection system can be a single computer, connected to a wireless signal processing device, and antennas placed throughout the facility. For huge organizations, a Multi Network Controller provides central control of multiple WIPS servers, while for SOHO or SMB customers, all the functionality of WIPS are available in a single box. In a WIPS implementation, users first define the operating wireless policies in the WIPS. The WIPS sensors then analyze the traffic in the air and send this information to WIPS server. The WIPS server correlates the information, validates it against the defined policies, and classifies if it is a threat. The administrator of the WIPS is then notified of the threat, or, if a policy has been set accordingly, the WIPS takes automatic protection measures. WIPS is configured as either a network implementation or a hosted implementation.

QUESTION 22
Which of the following attacks are examples of Denial-of-service attacks (DoS)? Each correct answer represents a complete solution. Choose all that apply.

A. Birthday attack
B. Fraggle attack
C. Ping flood attack
D. Smurf attack

Correct Answer: DBC
Explanation

Explanation/Reference:
Explanation:
Examples of DoS attacks are as follows: Smurf attack: In a smurf DoS attack, an attacker sends a large amount of ICMP echo request traffic to the IP broadcast addresses. These ICMP requests have a spoofed

source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multiaccess broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Fraggle attack: In a fraggle DoS attack, an attacker sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi-access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Ping flood attack: In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication.

QUESTION 23
Which of the following stream ciphers is both a block cipher and a product cipher?

A. RC2
B. AES
C. DES
D. RC4

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
The Data Encryption Standard (DES) is the most widely used encryption standard. The algorithm itself is referred to as Data Encryption Algorithm (DEA). It uses a 56-bit key to encrypt or decrypt data in 64-bit blocks. DES is both a block cipher and a product cipher. Answer option D is incorrect. RC4 is a stream cipher designed by Ron Rivest. It is used in many applications, including Transport Layer Security (TLS), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), etc. RC4 is fast and simple. However, it has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, nonrandom or related keys are used, or a single keystream is used twice. Some ways of using RC4 can lead to very insecure cryptosystems such as WEP. It uses block cipher. Answer option A is incorrect. RC2 is a block cipher designed by Ron Rivest in 1987 and other ciphers designed by Rivest include RC4, RC5, and RC6. RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy Feistel network, with 16 rounds of one type punctuated by two rounds of another type. Answer option B is incorrect. The Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable. It became effective as a standard on May 26, 2002. As of 2009, AES is one of the most popular algorithms used in symmetric key cryptography. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information.

QUESTION 24
Which of the following security protocols is supported by Wi-Fi Protected Access (WPA)?

A. CCMP
B. LEAP
C. TKIP
D. PEAP

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
Wi-Fi Protected Access (WPA) is a certification program developed by Wi-Fi Alliance, supporting only the TKIP protocol. TKIP (Temporal Key Integrity Protocol) is an encryption protocol defined in the IEEE 802.11i standard for wireless LANs (WLANs). It is designed to provide more secure encryption than the disreputably weak Wired Equivalent Privacy (WEP). TKIP is the encryption method used in Wi-Fi Protected Access (WPA), which replaced WEP in WLAN products. TKIP is a suite of algorithms to replace WEP without requiring the replacement of legacy WLAN equipment. TKIP uses the original WEP programming but wraps additional code at the beginning and end to encapsulate and modify it. Like WEP, TKIP uses the RC4 stream encryption algorithm as its basis. Answer option A is incorrect. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE 802.11i encryption protocol created to replace both TKIP, the mandatory protocol in WPA, and WEP, the earlier, insecure protocol. CCMP is a mandatory part of the WPA2 standard, an optional part of the WPA standard, and a required option for Robust Security Network (RSN) Compliant networks. CCMP is also used in the ITU-T home and business networking standard. CCMP, part of the 802.11i standard, uses the Advanced Encryption Standard (AES) algorithm. Unlike in TKIP, key management and message integrity is handled by a single component built around AES using a 128-bit key, a 128-bit block, and 10 rounds of encoding per the FIPS 197 standard. Answer option B is incorrect. The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary EAP method developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard. There is no native support for LEAP in any Windows operating system, but it is widely supported by third-party client software most commonly included with WLAN (wireless LAN) devices. Due to the wide adoption of LEAP in the networking industry, many other WLAN vendors claim support for LEAP. Answer option D is incorrect. PEAP (Protected Extensible Authentication Protocol) is a method to securely transmit authentication information over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. PEAP is not an encryption protocol; as with other EAP protocols, it only authenticates a client into a network. PEAP uses server-side public key certificates to authenticate the server. It creates an encrypted SSL/TLS (Secure sockets layer/Transport layer security) 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 resultant exchange of authentication information inside the tunnel to authenticate the client is then encrypted and the user credentials are thus safe and secure.

QUESTION 25
You work as a Network Administrator for Tech Perfect Inc. The company has a wireless LAN network. The clients present on the network are excluded. You check the error and find the reason that there is no DHCP server. Which of the following devices will you configure as a DHCP server?

A. Access point
B. Controller
C. RADIUS Server
D. Wireless LAN switches

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
In this scenario, the clients are excluded because of the DHCP server. There is no DHCP server in the network, so the client may use the IP address that is already used by other clients. This issue is solved by configuring the controller as a DHCP server. After the configuration, controller provides IP addresses to the clients, direct connect access points, appliance-mode access point on the management interface, and DHCP requests that are transmitted from the access point. You must configure the management interface IP address of the controller as the DHCP server IP address. You can configure the controller by using the Web-browser interface. The step that you must follow is given below:
Controller > Internal DHCP Server > New Answer options A, C, and D are incorrect. The access point, Radius server, and wireless switches cannot act as a DHCP server in a wireless network.

QUESTION 26
A Cisco Unified Wireless Network has an AP that does not rely on the central control device of the network. Which type of AP has this characteristic?

A. Rogue AP
B. LWAPP
C. Lightweight AP
D. Autonomous AP

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:
Autonomous Access Point is an AP that does not rely on the central control device. It is also called Standalone Access Point. The home office, corporate office, or a Wi-Fi hot- spot will have autonomous access points. Autonomous AP is deployed as a standalone device in ISR routers at branch sites. Answer option C is incorrect. Lightweight Access Point is an 802.11 a/b/g dual-band, zero-touch configuration and management access point that provides secure, cost effective wireless access with advanced WLAN services for enterprise deployments. This lightweight access point provides industry-leading RF capabilities to increase wireless LAN performance, security, reliability, and scalability. Answer option B is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. The system also allows network administrators to closely analyze the network. Answer option A is incorrect. A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a cracker to conduct a man-in-the-middle attack. Rogue access points create a security threat to large organizations because anyone with access to the premises can maliciously install an inexpensive wireless router that can allow access to a secure network to unauthorized parties. Rogue access points do not employ mutual authentication.

QUESTION 27
Which of the following wireless security protocols is defined in IEEE 802.11 pre-RSNA security?

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

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
Wired Security Privacy (WEP) is the security protocol defined in IEEE 802.11 pre- SNA security. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream. Answer options D, C, and A are incorrect. CCMP, EAP, and TKIP are defined under the current 802.11-2007 standard for robust network security (RSN). Fact What is RSN? Hide Robust Security Network (RSN) is an element of 802.11i authentication and encryption algorithms to be used for communications between WAPs and wireless clients. It works as a protocol. It is used for establishing secure communications over an 802.11 wireless network. FactWhat is EAP? Hide Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one-time passwords, public keys, etc. It is an extension to Pointto- Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection. FactWhat is CCMP? Hide CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE 802.11i encryption protocol created to replace both TKIP, the mandatory protocol in WPA, and WEP, the earlier, insecure protocol. CCMP is a mandatory part of the WPA2 standard, an optional part of the WPA standard, and a required option for Robust Security Network (RSN) Compliant networks. CCMP is also used in the ITU-T home and business networking standard. CCMP, part of the 802.11i standard, uses the Advanced Encryption Standard (AES) algorithm. Unlike in TKIP, key management and message integrity is handled by a single

component built around AES using a 128-bit key, a 128-bit block, and 10 rounds of encoding per the FIPS 197 standard. FactWhat is TKIP? Hide TKIP (Temporal Key Integrity Protocol) is an encryption protocol defined in the IEEE 802.11i standard for wireless LANs (WLANs). It is designed to provide more secure encryption than the disreputably weak Wired Equivalent Privacy (WEP). TKIP is the encryption method used in Wi-Fi Protected Access (WPA), which replaced WEP in WLAN products. TKIP is a suite of algorithms to replace WEP without requiring the replacement of legacy WLAN equipment. TKIP uses the original WEP programming but wraps additional code at the beginning and end to encapsulate and modify it. Like WEP, TKIP uses the RC4 stream encryption algorithm as its basis.

QUESTION 28
Which of the following security levels are applied on the network to prevent unauthorized access? Each correct answer represents a complete solution. Choose all that apply.

A. Access control lists
B. Authentication
C. Authorization
D. MAC filtering

Correct Answer: CB
Explanation

Explanation/Reference:
Explanation:
Authorization and authentication are the security levels that are applied on the network to prevent unauthorized access. Authentication and authorization verifies username and password in order to determine whether the user is authorized or not.Answer options A and D are incorrect. Access control lists and MAC filtering are the security features that are used to prevent network attacks. Fact What is authorization? Hide Authorization is a process that verifies whether a user has permission to access a Web resource. A Web server can restrict access to some of its resources to only those clients that log in using a recognized username and password. To be authorized, a user must first be authenticated. FactWhat is authentication? Hide Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the subject are true ("authentification" is a variant of this word). This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what its packaging and labeling claims to be, or assuring that a computer program is a trusted one. Authentication is a process of verifying the user. The accuracy of the authentication can be determined by the number of factors used for the authentication, such as the following:
One-factor authentication Two-factor authentication Three-factor authentication Multi- factor authentication

QUESTION 29
Which of the following are legacy authentication protocols used within the stronger EAP authentication protocols? Each correct answer represents a complete solution. Choose all that apply.

A. MS-CHAP
B. PPTP
C. PAP
D. CHAP

Correct Answer: CDA
Explanation

Explanation/Reference:
Explanation:

A password authentication protocol (PAP) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Almost all network operating system remote servers support PAP. Working cycle: Client sends username and password. Server sends authentication- ack (if credentials are OK) or authentication-nak. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost all PPP servers. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the

new version of MSCHAP. MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the environment consisting of both Windows NT and Windows 2000/XP dialup clients. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving datA. Answer option B is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a remote access protocol. It is an extension of the Point-to-Point Protocol (PPP). PPTP is used to securely connect to a private network by a remote client using a public data network, such as the Internet. Virtual private networks (VPNs) use the tunneling protocol to enable remote users to access corporate networks securely across the Internet. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection.

QUESTION 30
You are setting up small offices for a major insurance carrier. The company policy states that all wireless configurations must fully implement the 802.11i standard. Based on this requirement, which encryption algorithm should you implement?

A. WEP
B. PKI
C. WPA2
D. WPA

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

WPA2 is, to date, the most 802.11 compliant encryption protocol available. Fact What is WPA2 (Wi-Fi Protected Access)? Hide WPA2 is an updated version of WPA. This standard is also known as IEEE 802.11i.WPA2 offers enhanced protection to wireless networks than WPA and WEP standards. It is also available as WPA2-PSK and WPA2- EAP for home and enterprise environment respectively. Answer option D is incorrect. WPA is an improvement over WEP, but unlike WPA2, it does not implement certain key elements of 802.11i such as Counter Mode with Cipher Block Chaining Message Authentication Code. Answer option A is incorrect. WEP does not implement many aspects of the 802.11i standards. Answer option B is incorrect. PKI is a method for exchanging encryption keys, not for encrypting datA.

QUESTION 31
Which of the following monitors program activities and modifies malicious activities on a system?

A. RADIUS
B. NIDS
C. HIDS
D. Back door

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
Host-based IDS (HIDS) is an Intrusion Detection System that runs on the system to be monitored. HIDS monitors only the data that is directed to or originating from that particular system on which HIDS is installed. Besides network traffic for detecting attacks, it can also monitor other parameters of the system such as running processes, file system access and integrity, and user logins for identifying malicious activities. BlackIce Defender and Tripwire are good examples of HIDS. Tripwire is an HIDS tool that automatically calculates the cryptographic hashes of all system files as well as any other files that a network administrator wants to monitor for modifications. It then periodically scans all monitored files and recalculates information to see whether or not the files have been modified. It raises an alarm if changes are detected. Answer option A is incorrect. RADIUS is an industry standard protocol to authenticate, authorize, and account for access server connections. Answer option D is incorrect. Back door is a program or account that allows access to a system by skipping the security checks. Many vendors and developers implement back doors to save time and effort by skipping the security checks while troubleshooting. Back door is considered to be a security threat and should be kept with the highest

security. If a back door becomes known to attackers and malicious users, they can use it to exploit the system Answer option B is incorrect. A Network-based Detection System (NIDS) analyzes data packets flowing through a network. It can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. It is responsible for detecting anomalous or inappropriate data that may be considered 'unauthorized' on a network. An NIDS captures and inspects all data traffic, regardless of whether or not it is permitted for checking.

QUESTION 32
Which of the following are the layers of physical security? Each correct answer represents a complete solution. Choose all that apply.

A. Procedural access control
B. Video monitor
C. Environmental design
D. Intrusion detection system

Correct Answer: CAD
Explanation

Explanation/Reference:
Explanation:

Environmental design is the initial layer of security for a campus, building, office, or physical space. It is used to determine threats. Some of the most common examples are also the most basic - barbed wire, warning signs and fencing, concrete bollards, metal barriers, vehicle height-restrictors, site lighting, and trenches. Procedural access control includes the use of policies, processes, and procedures to manage the ingress into the restricted areA. An example of this is the deployment of security personnel conducting checks for authorized entry at predetermined points of entry. It is the second layer of physical security. The third layer is the intrusion detection system. It is a device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. A video monitor, also called a broadcast monitor, broadcast reference monitor, or just reference monitor, is a device similar to a television, used to monitor the output of a video-generating device, such as a media playout server, IRD, video camera, VCR, or DVD player. Video monitors are used extensively in the security industry with closed- circuit television cameras and recording devices. It is the last layer of physical security.

QUESTION 33
Your Company is receiving false and abusive e-mails from the e-mail address of your partner company. When you complain, the partner company tells you that they have never sent any such e-mails. Which of the following types of cyber crimes involves this form of network attack?

A. Man-in-the-middle attack
B. Spoofing
C. Cyber squatting
D. Cyber Stalking

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:
This type of network attack is called spoofing. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer option C is incorrect. Cybersquatting (also known as domain squatting), according to the Anticybersquatting Consumer Protection Act, is registering, trafficking in, or using a domain name with bad intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

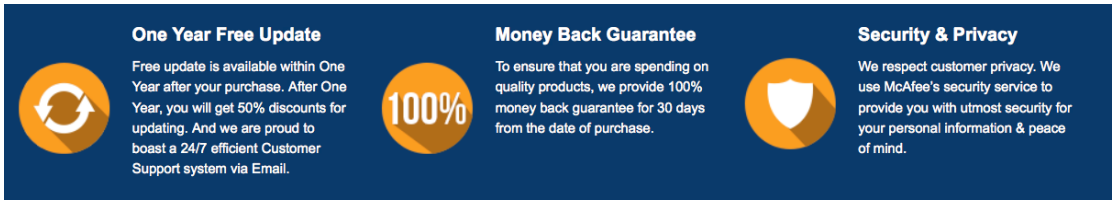
★ Average **99.9%** Success Rate

★ 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:



Guarantee & Policy | Privacy & Policy | Terms & Conditions