Exam : PW0-200

Title : Wireless Security Professional

Ver : 05-07-08

QUESTION 1:

You are hired by Certkiller .com as a consultant. Certkiller .com is deciding on a security solution for their new WLAN, and a PPTP VPN is their primary consideration since it is included with both server and desktop operating systems. While the 128-bit encryption of Microsoft's MPPE is considered strong enough to adhere to corporate security policy, Certkiller .com is concerned about security holes in MS-CHAPv2 authentication. Which three of the following would you advise Certkiller .com about applying MS-CHAPv2 authentication in a PPTP VPN? (Choose three)

A. MS-CHAPv2 is subject to offline dictionary attacks.
B. MS-CHAPv2 is only secure when combined with MAC filters.
C. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
D. MS-CHAPv2 can be replaced with EAP-TLS as the authentication mechanism for PPTP.
E. MS-CHAPv2 uses anonymous Diffie-Hellman authentication, and is therefore secure.
F. MS-CHAPv2 is appropriate for WLAN security when used inside a TLS-encrypted tunnel.

Answer: A,D,F

QUESTION 2:

Certkiller .com is installing an 802.11i-compliant wireless security solution using 802.1X/EAP authentication. According to Certkiller .com's policy, an eavesdropper must be prevented from decrypting data frames traversing a wireless connection by the security solution. Which of the following is the security solution feature that satisfies Certkiller .com's policy requirement?

A. Message Integrity Check (MIC)
B. Mutual Authentication
C. Encrypted Passphrase
D. 4-Way Handshake
E. Integrity Check Value (ICV)

Answer: D

QUESTION 3:

you drives a forklift for Certkiller .com. The forklift can reach speeds of 20 mph (32 km/h), and has an 802.11g enabled industrial computer mounted to the frame to receive warehouse orders. Your industrial laptop's communication with the access point is secured with 802.11i compliant 802.1X/EAP-TTLS. Certkiller .com's warehouse application requires reassociation speeds of less than 50ms, and 802.1X/EAP-TTLS authentication takes roughly 800ms. which of the following is required for Certkiller .com's warehouse application to work properly? (Choose all that apply)

A. APs must have a hardware accelerator chip that performs "fast key generation" after receiving a reauthentication message.
B. A WLAN controller that can maintain all PMKSAs internally must be installed.
C. No changes are needed, because 802.11i compliant devices can cache the initial PMK and send it to other APs over the wired network as needed.
D. An x.509 certificate must be installed on the client to reduce the EAP-TTLS authentication time to <50ms.
E. The authentication server must be configured to generate, buffer, and distribute the next four temporal keys as needed.

Answer: B

QUESTION 4:

Certkiller .com's wireless network has been exposed to several Layer 1 and Layer 2 Denial of Service (DoS) attacks of late. Of the following options, which one is a security solution that can detect and report when and where a DoS attack is taking place?

A. Distributed spectrum analyzers
B. WPA2-Enterprise
C. WLAN positioning system
D. Wireless IPS
E. Wireless LAN discovery tools with GPS

Answer: D

QUESTION 5:

Which of the following is an advantage of employing EAP-TTLS, as opposed to EAP-TLS as an authentication mechanism in a WLAN environment?

A. EAP-TTLS supports mutual authentication between supplicants and authentication servers.
B. EAP-TTLS sends client credentials through an encrypted TLS tunnel to the server.
C. EAP-TTLS is integrated into Microsoft Active Directory and Novell eDirectory.
D. EAP-TTLS uses proven standards-based technology, but EAP-TLS is still in draft format.
E. EAP-TTLS allows clients to authenticate to the server using passwords.
F. EAP-TTLS supports smart card clients.

Answer: E

QUESTION 6:

Which of the following is a WLAN client device feature that works to the advantage of the attacker in a WLAN hijacking attack?

A. The IEEE 802.11 standard specifies that clients using Open System authentication must allow direct client-to-client connections, even in Infrastructure mode.
B. Clients auto-detect Ad Hoc and Infrastructure service sets and will associate to the appropriate network type.
C. When the RF signal between a client and an access point is lost for more than a few seconds, the client device will attempt reassociation only with the same access point until the Layer 3 session times out.
D. When the RF signal between a client and an access point is significantly disrupted, the client will seek to reassociate with another access point with the same SSID and a stronger, higher-quality signal.

Answer: D

QUESTION 7:

Due to constant standards development and changes within the industry, Certkiller .com has not applied a WLAN. As the chief network administrator, you notify the IT staff that since the 802.11i amendment was approved, most vendors have submitted their equipment for WPA2 interoperability testing. Although the majority of the staff seems encouraged, one of the administrators is worried whether the WPA2 certification adds value to the equipment. Which of the following is a statement that addresses this concern?

A. WPA2-certified equipment supports both layer 2 and layer 3 security mechanisms, unlike WPA.
B. WPA2-certified equipment can use Transient Key IP for backwards compatibility with WPA-certified equipment.
C. WPA2-certified equipment supports all security features found in the 802.11i amendment.
D. WPA2-certified equipment can support RSNAs and Shared Key WEP sessions simultaneously.

Answer: B

QUESTION 8:

Of the following, which is the security weakness present in pre-802.11i systems using 802.1X with dynamic WEP?

A. APs automatically downgrade the security level to standard WEP if the wireless client device does not support dynamic WEP.
B. The session key is crackable if enough traffic is transmitted using the key.
C. All versions of EAP used with dynamic WEP pass the username across the wireless medium in clear text.
D. There is no ability to authenticate individual users.

Answer: B

QUESTION 9:

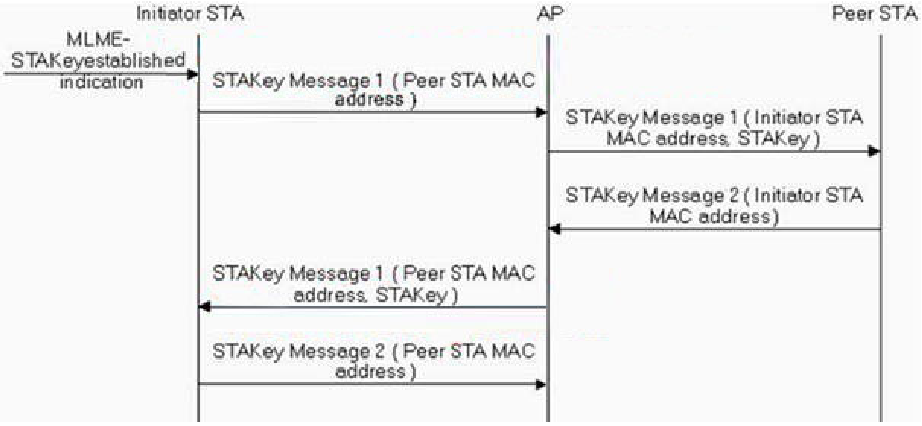
Which two of the following are the performance-limiting factors when using a VPN-enabled router as a WLAN segmentation device? (Choose two)

A. Each VPN tunnel must have one x.509 certificate
B. The maximum number of tunnel terminations supported by the VPN router
C. 802.11e QoS frame tagging support
D. No support for private (non-routable) IP addresses inside VPN tunnels
E. Encrypted throughput of the VPN router

Answer: B,E

QUESTION 10:

Exhibit:


Initiator STA
AP
Peer STA
MLME-STAKeyestablished indication
STAKey Message 1 (Peer STA MAC address)
STAKey Message 1 (Initiator STA MAC address, STAKey)
STAKey Message 2 (Initiator STA MAC address)
STAKey Message 1 (Peer STA MAC address, STAKey)
STAKey Message 2 (Peer STA MAC address)

Which of the following best explains when the illustrated 802.11i amendment's STAKey handshake will be used? (Choose all that apply)

A. When a supplicant wishes to receive WMM information from an authenticator

B. When two wireless client stations wish to establish a WDS
C. When two client stations want to communicate directly while associated to an AP
D. When a wireless client station wants to roam to a peer station
E. When a wireless client station wants to establish a VPN tunnel to a peer station

Answer: C

QUESTION 11:

When Transient Key IP uses an 8 octet message integrity check (MIC), which of the following is the type of attack prevented?

A. RF jamming attack
B. Replay attack
C. Forgery attack
D. Collision attack
E. Weak-key attack

Answer: C

QUESTION 12:

Which of the following is a TRUE statement regarding Certkiller .com's WLAN security, if Certkiller .com has a single access point, 15 client devices, and utilizes WPA2-Personal for WLAN security?

A. Because WPA2-Personal uses Shared Key authentication followed by a 4-Way Handshake, EAP-Start flood attacks are easily performed.
B. Traffic injection attacks are possible because the transmitter lacks frame numbering.
C. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt data traffic.
D. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt broadcast traffic.
E. An authorized WLAN user with a protocol analyzer can decode frames captured from the 4-Way Handshake of another authorized user.

Answer: E

QUESTION 13:

Attacks against the identified weaknesses of WEP are prevented by which two of the following Transient Key IP features? (Choose two)

A. RC5 stream cipher
B. 32-bit ICV (CRC-32)
C. Arthur
D. Decreased IV length
E. Michael
F. Mandatory per-packet keys

Answer: E,F

QUESTION 14:

the most effective defense against an RF jamming attack is best described by which of the following? (Choose all that apply)

A. Higher gain on access point antennas and higher output power on access points
B. Multi-factor authentication on the wireless network
C. Installing all access points in lockable enclosures
D. Surrounding access points with RF barriers
E. Physical security of the premises
F. Virtual Private Network technology

Answer: E

QUESTION 15:

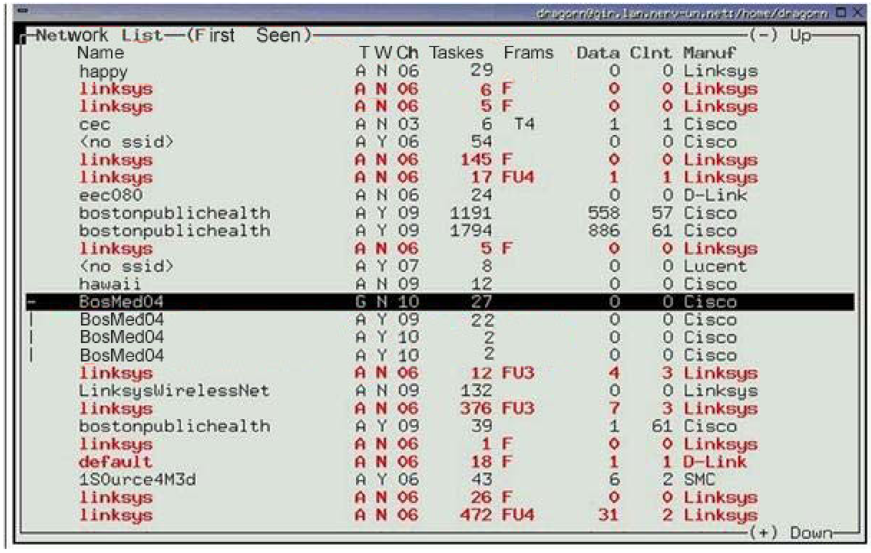
The functionality of the IEEE 802.1X-2004 standard is perfectly described by which of the following statements? (Choose all that apply)

A. Port access control with EAPoL support for 802.3 and 802.11 LANs
B. Port access control with support for EAP-MD5 authentication and RC4 encryption only
C. Port access control with support for authenticated-user VLANs only
D. Port access control with encryption key management and distribution

Answer: A

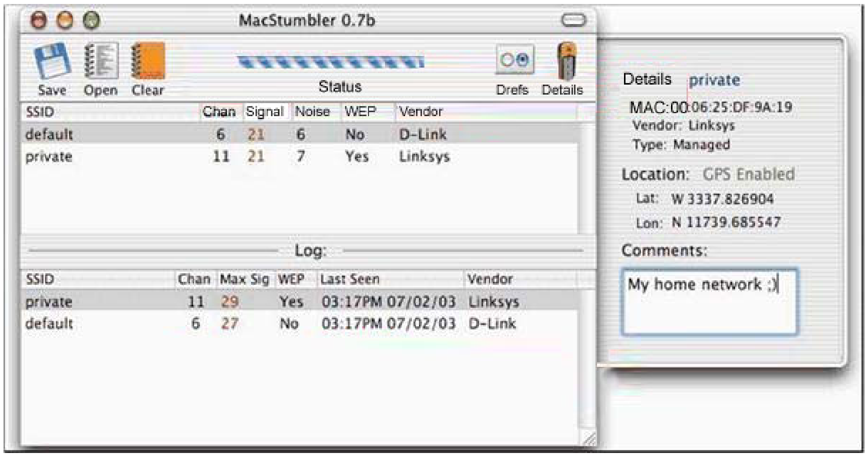
QUESTION 16:

Exhibit #1:



```
                                          dragorn@gir.lan.nerv-un.net:/home/dragorn
 Network List—(First  Seen)——————————————————————————————————————————(-) Up——
      Name                           T W Ch  Taskes  Frams   Data Clnt Manuf
      happy                          A N 06     29              0    0 Linksys
      linksys                        A N 06      6 F            0    0 Linksys
      linksys                        A N 06      5 F            0    0 Linksys
      cec                            A N 03      6  T4          1    1 Cisco
      <no ssid>                      A Y 06     54              0    0 Cisco
      linksys                        A N 06    145 F            0    0 Linksys
      linksys                        A N 06     17 FU4          1    1 Linksys
      eec080                         A N 06     24              0    0 D-Link
      bostonpublichealth             A Y 09   1191            558   57 Cisco
      bostonpublichealth             A Y 09   1794            886   61 Cisco
      linksys                        A N 06      5 F            0    0 Linksys
      <no ssid>                      A Y 07      8              0    0 Lucent
      hawaii                         A N 09     12              0    0 Cisco
 -    BosMed04                       G N 10     27              0    0 Cisco
 |    BosMed04                       A Y 09     22              0    0 Cisco
 |    BosMed04                       A Y 10      2              0    0 Cisco
 |    BosMed04                       A Y 10      2              0    0 Cisco
      linksys                        A N 06     12 FU3          4    3 Linksys
      LinksysWirelessNet             A N 09    132              0    0 Linksys
      linksys                        A N 06    376 FU3          7    3 Linksys
      bostonpublichealth             A Y 09     39              1   61 Cisco
      linksys                        A N 06      1 F            0    0 Linksys
      default                        A N 06     18 F            1    1 D-Link
      1SOurce4M3d                    A Y 06     43              6    2 SMC
      linksys                        A N 06     26 F            0    0 Linksys
      linksys                        A N 06    472 FU4         31    2 Linksys
 ————————————————————————————————————————————————————————————————————(+) Down—
```

Exhibit #2:



SSID	Chan	Signal	Noise	WEP	Vendor
default	6	21	6	No	D-Link
private	11	21	7	Yes	Linksys

Log:

SSID	Chan	Max Sig	WEP	Last Seen	Vendor
private	11	29	Yes	03:17PM 07/02/03	Linksys
default	6	27	No	03:17PM 07/02/03	D-Link

Details private

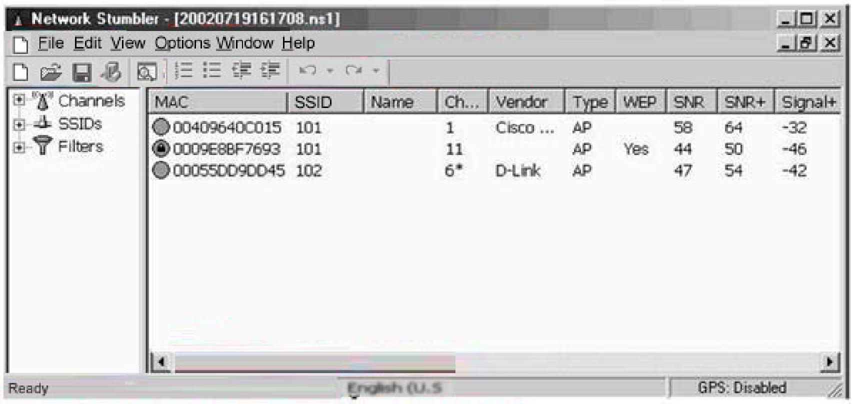
MAC: 00:06:25:DF:9A:19
Vendor: Linksys
Type: Managed

Location: GPS Enabled
Lat: W 3337.826904
Lon: N 11739.685547

Comments:

My home network ;)

Exhibit #3:



Network Stumbler - [20020719161708.ns1]
File Edit View Options Window Help
Channels
SSIDs
Filters
Ready
English (U.S
GPS: Disabled

MAC	SSID	Name	Ch...	Vendor	Type	WEP	SNR	SNR+	Signal+
00409640C015	101		1	Cisco ...	AP		58	64	-32
0009E8BF7693	101		11		AP	Yes	44	50	-46
00055DD9DD45	102		6*	D-Link	AP		47	54	-42

The WLAN software utilities illustrated in the exhibits above (Exhibit #1, Exhibit #2, and Exhibit #3) serves which purpose?

A. Injecting 802.11 frames into a WLAN
B. Cracking Transient Key IP encryption in real-time
C. Performing offline dictionary attacks

D. WLAN location and identification
E. Capturing and decoding 802.11 frames

Answer: D

QUESTION 17:

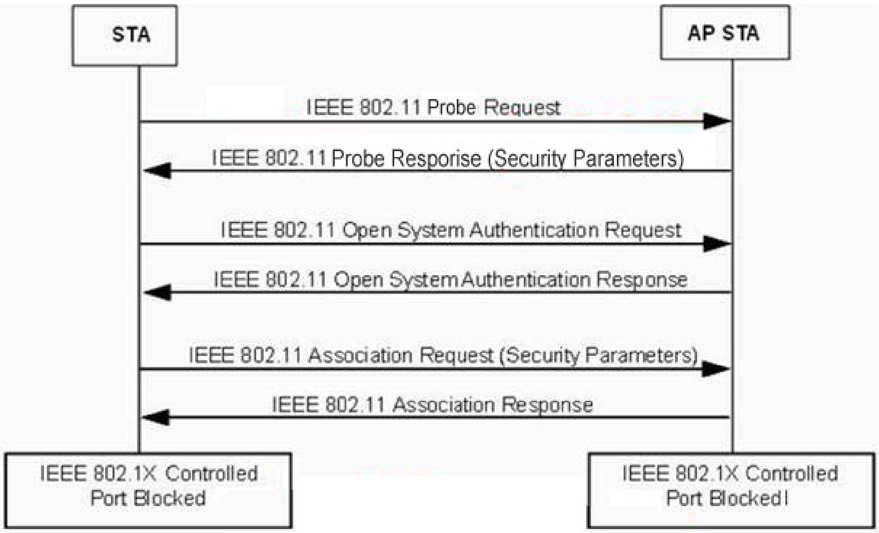
To protect their 802.11a connections, Certkiller .com has employed both WPA2-Enterprise and IPSec/ESP security mechanisms. Which of the following is an option that specifies the paired layers involved in this security implementation?

A. Layer 2, Layer 3
B. Layer 3, Layer 7
C. Layer 1, Layer 2
D. Layer 2, Layer 7
E. Layer 2, Layer 4

Answer: A

QUESTION 18:

Exhibit:


STA
AP STA
IEEE 802.11 Probe Request
IEEE 802.11 Probe Response (Security Parameters)
IEEE 802.11 Open System Authentication Request
IEEE 802.11 Open System Authentication Response
IEEE 802.11 Association Request (Security Parameters)
IEEE 802.11 Association Response
IEEE 802.1X Controlled Port Blocked
IEEE 802.1X Controlled Port Blocked I

What process immediately follows the 802.11 association procedure from the 802.11i amendment, which is illustrated above, in a WPA2-Enterprise network?

A. 802.11 authentication process
B. STAKey Handshake
C. Pass-phrase-to-PSK mapping process
D. 802.1X/EAP framework process
E. Group Handshake

F. 4-Way Handshake

Answer: D

QUESTION 19:

Which of the following is the element that the 802.11i Pairwise Transient Key is derived from?

A. Pass-phrase-to-PSK mapping algorithm
B. Group Master Key (GMK)
C. Group Temporal Key
D. Extended Master Session Key (EMSK)
E. AAA Key
F. Pairwise Master Key (PMK)

Answer: F

QUESTION 20:

Certkiller .com owns a coffee shop and has just installed a free 802.11g wireless hotspot for the benefit of Certkiller .com's customers. For legal reasons, Certkiller .com wants to inhibit spammers from sending bulk email via Certkiller .com's Internet connection. The best way to accomplish this objective is specified by which of the following options? (Choose all that apply)

A. Install an 802.11g camera to monitor patron's activities
B. Block TCP port 25 outbound on the Internet router
C. Allow only trusted patrons to use the WLAN
D. Disable the WLAN during non-business hours
E. Use a WLAN protocol analyzer to locate and block malicious WLAN frames
F. Install WPA2-Personal security on your access point

Answer: B

QUESTION 21:

A network security auditor is evaluating a wireless network's exposure to security holes. Which of the following tasks would save the most time if executed prior to the audit? (Choose all that apply)

A. Identify the manufacturer of the wireless infrastructure hardware.
B. Identify the IP subnet information for each network segment.

C. Identify the skill level of the wireless network security administrator(s).
D. Identify the wireless security solutions currently in use.
E. Identify security holes in the wireless security policy.

Answer: D

QUESTION 22:

To secure their wireless connections, Certkiller .com decides to employ IPSec VPN technology. Strong encryption is an important factor in the security solution for preventing eavesdropping attacks. When the data payload must be encrypted, which of the following is the IPSec protocol required?

A. PPP
B. ESP
C. L2F
D. IKE
E. AH

Answer: B

QUESTION 23:

Which two of the following amounts to four tools that are required to hijack a wireless client from the authorized wireless network onto the unauthorized wireless network? (Choose two)

A. MAC spoofing software and data flooding software
B. A wireless PC card and DHCP server software
C. A wireless bridge and a spectrum analyzer
D. Access point software and a narrowband RF jamming device
E. A high-gain Yagi antenna and terminal emulation software

Answer: B,D

QUESTION 24:

You are a network administrator at Certkiller .com. You frequently work from home and wireless hotspots, rather than commuting to the office. Your laptop hooks up to the office network via WLANs. Which of the following are two wireless security policy items that you should implement to safeguard your data? (Choose two)

A. Use a protocol analyzer on his laptop to sniff WLAN traffic for risks

B. Use 802.1X/PEAPv0 to connect to the office network
C. Use a personal firewall on his laptop
D. Use an IPSec VPN for remote connectivity
E. Use an HTTPS captive portal

Answer: C,D

QUESTION 25:

Certkiller .com is in the process of installing a WLAN switch/controller and one thousand 802.11a/g lightweight access points. which of the following best describes how the WLAN switch/controller should connect to the Ethernet network in this environment? (Choose all that apply)

A. The WLAN switch/controller should connect to the core Layer 3 switch via a gigabit (or faster) Ethernet segment.
B. The WLAN switch/controller should connect to a Layer 3 distribution switch in a wireless VLAN using a gigabit (or faster) connection.
C. The WLAN switch/controller should be connected between the Layer 3 core Ethernet switch/controller and the corporate Internet firewall using a 100 Mbps connection.
D. The WLAN switch/controller should connect between every Layer 3 distribution Ethernet switch and every Layer 2 access Ethernet switch by having one port in each VLAN.

Answer: A

QUESTION 26:

Certkiller .com has recently finished installing a WLAN switch/controller with 10 lightweight (thin) access points. 802.11i compliant PEAPv0/EAP-MSCHAPv2 has been specified by the Chief Security Officer as the only authorized WLAN authentication and encryption scheme. The x.509 server certificate must reside in which two of the following locations, in Certkiller .com's network? (Choose two)

A. Supplicant devices
B. LDAP server
C. WLAN switch/controller
D. Lightweight access points
E. RADIUS server

Answer: A,E

QUESTION 27:

In which of the following ways should the problem of rogue access points be addressed by a wireless security professional, as a part of a large organization security policy? (Choose all that apply)

A. Install and monitor a WIPS by a trained employee.
B. Use a WPA2-Enterprise compliant security solution with strong authentication and encryption.
C. Reduce the power of all access points on the network so that rogues stand out.
D. Hide the SSID of all access points on the network so that intruders don't know how to configure rogue APs.

Answer: A

QUESTION 28:

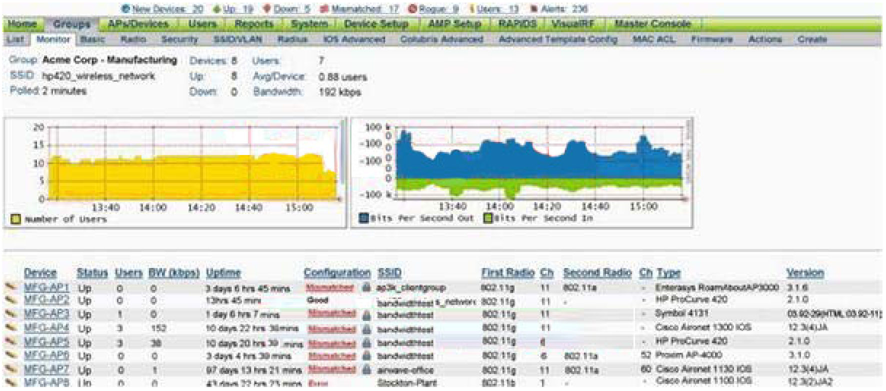
You are a administrator at Certkiller .com. Certkiller .com's 802.11g WLAN has been working perfectly for the last 6 months. One morning, not one of Certkiller .com's 10 users are able to hook up to the company's only access point. When you log into the access point, there are hundreds of users associated using Open System authentication. Which of the following is the cause of this problem?

A. The AP has been the victim of an RF DoS attack.
B. The AP firmware has been corrupted and is erroneously reporting the number of users.
C. The AP has experienced an association flood attack.
D. The AP has experienced an AP spoofing attack from a rogue AP.

Answer: C

QUESTION 29:

Exhibit:



Group: Acme Corp - Manufacturing
SSID: hp420_wireless_network
Polled: 2 minutes

Devices: 8
Up: 8
Down: 0

Users: 7
Avg/Device: 0.88 users
Bandwidth: 192 kbps

Device	Status	Users	BW (kbps)	Uptime	Configuration	SSID	First Radio	Ch	Second Radio	Ch	Type	Version
MFG-AP1	Up	0	0	3 days 6 hrs 45 mins	Mismatched	ap3k_clientgroup	802.11g	11	802.11a	-	Enterasys RoamAboutAP3000	3.1.6
MFG-AP2	Up	0	0	13hrs 45 mins	Good	bandwidthtest t_network	802.11g	11	-	-	HP ProCurve 420	2.1.0
MFG-AP3	Up	1	0	1 day 6 hrs 7 mins	Mismatched	bandwidthtest	802.11g	11		-	Symbol 4131	03.92-29(HTML 03.92-11)
MFG-AP4	Up	3	152	10 days 22 hrs 38mins	Mismatched	bandwidthtest	802.11g	11		-	Cisco Aironet 1300 IOS	12.3(4)JA
MFG-AP5	Up	3	38	10 days 20 hrs 39 mins	Mismatched	bandwidthtest	802.11g	6		-	HP ProCurve 420	2.1.0
MFG-AP6	Up	0	0	3 days 4 hrs 39 mins	Mismatched	bandwidthtest	802.11g	6	802.11a	52	Proxim AP-4000	3.1.0
MFG-AP7	Up	0	1	97 days 13 hrs 21 mins	Mismatched	airwave-office	802.11g	11	802.11a	60	Cisco Aironet 1130 IOS	12.3(4)JA
MFG-AP8	Up	0	0	43 days 22 hrs 23 mins	Error	Stockton-Plant	802.11b	1	-	-	Cisco Aironet 1100 IOS	12.3(2)JA2

Which of the following describes the type of WLAN system illustrated in the above exhibit?

A. EAP-enabled RADIUS Server
B. Enterprise Encryption Gateway
C. Wireless Intrusion Prevention System
D. Wireless Switch Configuration GUI
E. Wireless Network Management System

Answer: E

QUESTION 30:

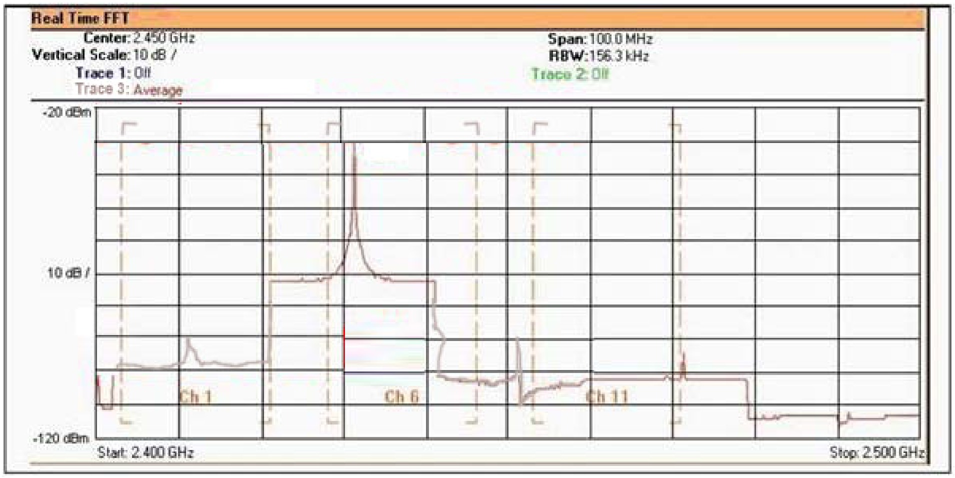
Numerous companies have guest VLANs on their WLAN, which permit visitors to have wireless Internet access only. Which of the following describe two risks related to employing guest VLANs without any security or control features? (Choose two)

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 guest users cannot be prevented.
D. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate network.
E. Guest users can reconfigure APs in the guest VLAN unless 802.1X/EAP is configured on the APs.

Answer: A,B

QUESTION 31:

Exhibit:



Center: 2.450 GHz
Vertical Scale: 10 dB /
Trace 1: Off
Trace 3: Average
Span: 100.0 MHz
RBW: 156.3 kHz
Trace 2: Off
Start: 2.400 GHz
Stop: 2.500 GHz

Which of the following is displayed on the screenshot of a RF spectrum analyzer? (Choose all that apply)

A. A DSSS-based phased array WLAN antenna transmission

B. A deauthentication frame from a WIPS blocking an AP on channel 5
C. A frequency hopping station transmitting on channel 5
D. A high-power, narrowband signal at approximately 2.430 GHz
E. An OFDM access point operating on channel 6

Answer: D

QUESTION 32:

Which of the following is an attack that a Wireless Intrusion Prevention System (WIPS) CANNOT detect?

A. MAC Spoofing
B. Netstumbler
C. Deauthentication flood
D. 802.11 eavesdropping
E. Fake AP

Answer: D

QUESTION 33:

A WLAN administrator is allowed to carry out which of the following network functions by the Role-Based Access Control (RBAC)? (Choose all that apply)

A. Provide wireless network access to users through specific access points, based on their 802.11e priority level.
B. Allow specific user groups more bandwidth than others.
C. Allow simultaneous support of multiple EAP types on a single access point.
D. Allow access to specific files and applications based on the user's IP subnet.

Answer: B

QUESTION 34:

Which of the following states how the 802.11i Group Handshake differs from the 4-Way Handshake? (Choose all that apply)

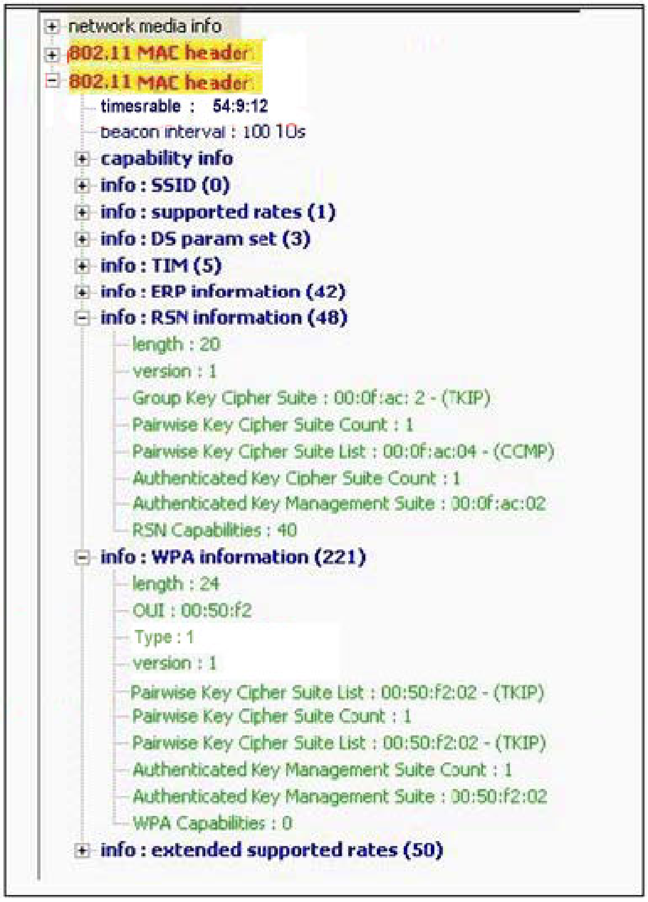
A. The Group Handshake is a 4-Way Handshake, but does not contain EAPoL Key frames.
B. The Group Handshake requires 6 exchanges, including the TCP 3-Way handshake traffic.
C. The Group Handshake has only two messages instead of four.

D. The Group Temporal Key is always part of the Group Handshake, but never part of the 4-Way Handshake.
E. The Group Handshake has four messages like the 4-Way Handshake, except when it is performed after a reauthentication when it exhibits only three messages.

Answer: C

QUESTION 35:

Exhibit:



```
+ network media info
+ 802.11 MAC header
- 802.11 MAC header
    timesrable :   54:9:12
    beacon interval : 100 10s
  + capability info
  + info : SSID (0)
  + info : supported rates (1)
  + info : DS param set (3)
  + info : TIM (5)
  + info : ERP information (42)
  - info : RSN information (48)
      length : 20
      version : 1
      Group Key Cipher Suite : 00:0f:ac: 2 - (TKIP)
      Pairwise Key Cipher Suite Count : 1
      Pairwise Key Cipher Suite List : 00:0f:ac:04 - (CCMP)
      Authenticated Key Cipher Suite Count : 1
      Authenticated Key Management Suite : 00:0f:ac:02
      RSN Capabilities : 40
  - info : WPA information (221)
      length : 24
      OUI : 00:50:f2
      Type : 1
      version : 1
      Pairwise Key Cipher Suite List : 00:50:f2:02 - (TKIP)
      Pairwise Key Cipher Suite Count : 1
      Pairwise Key Cipher Suite List : 00:50:f2:02 - (TKIP)
      Authenticated Key Management Suite Count : 1
      Authenticated Key Management Suite : 00:50:f2:02
      WPA Capabilities : 0
  + info : extended supported rates (50)
```

A WLAN protocol analyzer decoding an 802.11 Beacon Management Frame is displayed by the above exhibit. Which of the following is a TRUE statement with reference to the access point's BSS that can be verified with this illustration?

A. There is currently one wireless client associated with the AP using CCMP within the BSS.
B. Data frames within the BSS must have Transient Key IP key rotation set to rotate every 40 minutes.
C. The only cipher suite supported in the BSS is WPA-Personal.
D. The BSS supports both CCMP and Transient Key IP cipher suites simultaneously.
E. The BSS Group Key Cipher will be rotated by the access point after two more beacon

frames.

Answer: D

QUESTION 36:

With which criteria must the EAP-response/identity frame comply, as specified by RFC 3748?

A. The EAP-response/identity frame must contain the user identity.
B. When TLS-tunneling mode is active, the EAP-response frame must have a blank user identity.
C. The user identity value must be hashed prior to insertion into the EAP-response identity frame.
D. The EAP-response/identity frame must not contain a null identity value.

Answer: D

QUESTION 37:

Integrated protocol analysis engines are provided by Wireless Intrusion Prevention Systems (WIPS) to troubleshoot which of the following problems? (Choose all that apply)

A. Cipher suites supported by individual access points
B. PMKSA caching in WLAN controllers
C. 802.3af Power-over-Ethernet connectivity
D. VoWLAN phones roaming between access points
E. Access Point CPU overloading

Answer: A

QUESTION 38:

As part of Certkiller .com's new WLAN, they will be employing a WPA2-Enterprise security solution that makes use of an existing RADIUS server. Certkiller .com will require which of the following RADIUS server features to accomplish this? (Choose all that apply)

A. CCMP support
B. LDAP support
C. EAP support
D. Windows compatibility

E. 802.11d support

Answer: C

QUESTION 39:

Certkiller .com has an Information Technology (IT) building where the Active Directory server is located. Certkiller .com are installing a small WLAN switch and a small RADIUS server in each of the 20 campus buildings. WLAN encryption keys are generated by the RADIUS servers and each RADIUS server will proxy user authentication to the Active Directory server in the IT building. Which of the following is the AAA model described by this setup?

A. Distributed sites, centralized authentication and security
B. Distributed autonomous sites
C. Single site deployment
D. Distributed sites and security, centralized authentication

Answer: D

QUESTION 40:

To compel an authenticated WLAN client's data traffic into a particular VLAN on the AP, you should use which two of the following processes? (Choose two)

A. Create a "data type" filter on the AP to direct distinct traffic types into specific Ethernet VLANs.
B. Set the 802.11q tag on the AP to correspond with the appropriate VLAN on the Ethernet switch.
C. The AP is configured with manual SSID-to-VLAN mappings, and the user will be assigned to a VLAN according to the SSID being used.
D. Create a username-to-VLAN mapping on the AP to direct data traffic from a specific user to a designated VLAN.
E. RADIUS sends a return list attribute to the AP assigning the user to a specific VLAN.

Answer: C,E

QUESTION 41:

The first step in securing an 802.11 WLAN is a strong security policy. which two of the following are the proper sections for a WLAN security policy? (Choose two)

A. Application performance standards

B. Acceptable use and abuse of the network
C. Attack classification
D. Periodic security audits
E. Off-site data backups

Answer: B,D

QUESTION 42:

Which of the following is a baselining task that should be carried out subsequent to finishing the new WIPS overlay installation?

A. Identify the authorized, external, and rogue WLAN devices.
B. Authorized 802.3af traffic must be identified.
C. Approved 802.1X/EAP methods need to be selected and configured.
D. Wireless Anomaly Detection (WAD) filters should be created on the WIPS management server.

Answer: A

QUESTION 43:

Which of the following describes when the 802.1X Controlled Port is placed into the unblocked state, in an 802.11i-compliant WLAN? (Choose all that apply)

A. After any Group Handshake
B. After generation of a PMK
C. After RADIUS Authentication
D. After a 4-Way Handshake
E. After Open System Authentication

Answer: D

QUESTION 44:

Certkiller .com's administrator makes use of a coffee shop's Internet hotspot to transfer funds between his checking and savings accounts at his bank's website. The bank website employs the HTTPS protocol to protect sensitive account information. A hacker was able to obtain the administrator's bank account user ID and password, and transferred all of his money to another account. How was the administrator's bank account user ID and password obtained by the hacker?

A. The administrator's bank is using an expired x.509 certificate on their web server. The

certificate is on the administrator's Certificate Revocation List (CRL), causing the user ID and password to be sent unencrypted.
B. The administrator uses the same username and password for banking that he does for his IPSec VPN software. The administrator accessed his corporate network with his IPSec VPN software at the wireless hotspot. An IPSec VPN only encrypts data. The user ID and password are sent in clear text.
C. The administrator uses the same username and password for banking that he does for email. The administrator used a POP3 email client at the wireless hotspot to check his email, and the user ID and password were not encrypted.
D. The bank web server is using an x.509 certificate that is not signed by a root CA and is also using an expired public key, causing the user ID and password to be sent unencrypted.

Answer: C

QUESTION 45:

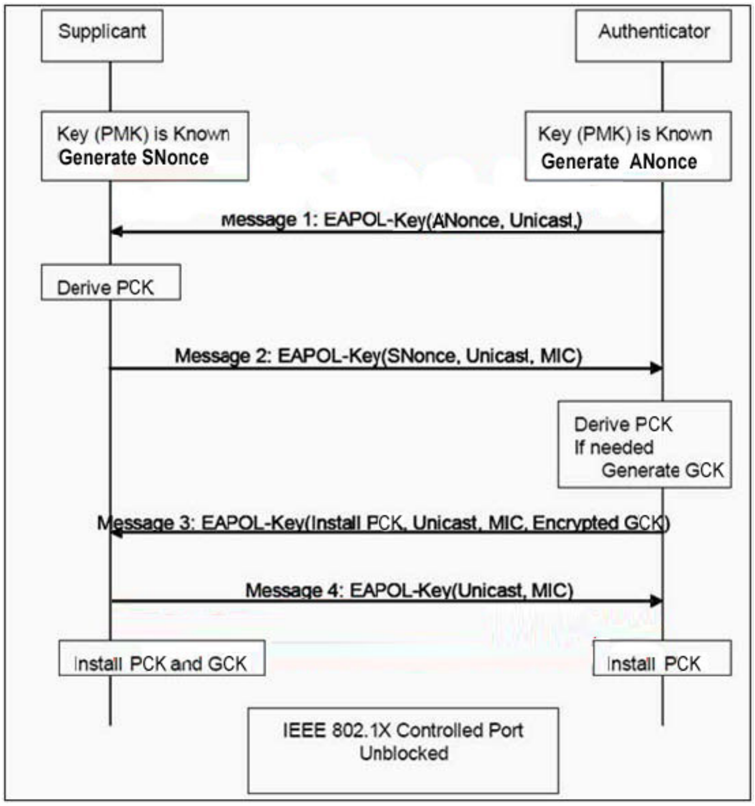
You have recently completed the installation of a WLAN switch/controller with 10 lightweight (thin) access points for Certkiller .com. All VLANs use one RADIUS server. The VLANs are configured as follows:
VLAN red (5 access points) - SSID red - Lightweight EAP (LEAP) authentication - CCMP cipher suite
VLAN blue (5 access points) - SSID blue - EAP-TTLS authentication - CCMP cipher suite
Your computer can successfully authenticate and browse the Internet when using the red VLAN, but cannot authenticate when using the blue VLAN. Which of the following is the most probably the cause of this problem?

A. The Lightweight Access Point Protocol (LWAPP) does not support EAP-TTLS authentication over lightweight access points.
B. Jack does not have a valid Kerberos ID on the blue VLAN.
C. The CCMP cipher suite is not a valid option for EAP-TTLS authentication.
D. The WIPS has been configured to perform a DoS attack on blue VLAN RADIUS packets.
E. The clock on Jack's computer pre-dates the RADIUS server's certificate creation date/time.
F. The blue VLAN does not support certificate-based authentication traffic.

Answer: E

QUESTION 46:

Exhibit:


Supplicant
Authenticator
Key (PMK) is Known
Generate SNonce
Key (PMK) is Known
Generate ANonce
Message 1: EAPOL-Key(ANonce, Unicast,)
Derive PCK
Message 2: EAPOL-Key(SNonce, Unicast, MIC)
Derive PCK
If needed
Generate GCK
Message 3: EAPOL-Key(Install PCK, Unicast, MIC, Encrypted GCK)
Message 4: EAPOL-Key(Unicast, MIC)
Install PCK and GCK
Install PCK
IEEE 802.1X Controlled Port
Unblocked

Which of the following is a TRUE statement pertaining to the Nonces used in the illustrated 802.11i amendment's 4-Way Handshake?

A. The SNonce and ANonce are combined at the Supplicant and Authenticator to create unique Pairwise transient keys for each device.
B. Nonces are the secret keys that are combined to unblock the 802.1X controlled port.
C. Both Nonces are used by the Supplicant and Authenticator in the derivation of a single Pairwise transient key.
D. The Supplicant uses the ANonce to derive its unique Pairwise transient key, and the Authenticator uses the SNonce to derive its unique Pairwise transient key.
E. The Nonces are created by mixing the MAC addresses of the Supplicant and the Authenticator.

Answer: C

QUESTION 47:

Which of the following is protected against clear text transmission across the wireless medium when employing a tunneled EAP type?

A. Pairwise Master Keys
B. EAPoL Keys
C. Server Credentials
D. x.509 certificates

E. User Credentials

Answer: E

QUESTION 48:

Why does the 802.11i-2004 amendment implement a pass-phrase-to-PSK mapping algorithm, which is recommended for use with Robust Security Network Associations (RSNAs)?

A. To enhance the security level of the 4-Way Handshake when WPA2-Personal is used
B. To encourage users unfamiliar with cryptographic concepts to enable the security features of their WLAN
C. To eliminate proprietary roaming mechanisms when Preshared Key security is used
D. To avoid using 802.1X/EAP authentication in independent basic service sets

Answer: B

QUESTION 49:

802.1X/EAP mutual authentication resolves which of the following 802.11 WLAN security problems? (Choose all that apply)

A. Weak Initialization Vectors
B. Hijacking by rogue access points
C. Weak password policies
D. Offline dictionary attacks
E. Disassociation attacks
F. MAC spoofing

Answer: B

QUESTION 50:

20 data entry clerks that use an unencrypted wireless LAN to access the main network are employed by Certkiller .com. In an attempt to hijack the wireless users, an intruder is utilizing a laptop running a software access point. Of the following, which option explains how the intruder can cause all of these clients to establish Layer 2 connectivity with the software access point?

A. When the signal between the clients and the authorized access point is temporarily disrupted and the intruder software access point is using the same SSID on a different channel than the authorized access point, the clients will reassociate to the software

access point.
B. A higher SSID value programmed into the intruder software access point will take priority over the SSID in the authorized access point, causing the clients to reassociate.
C. WLAN clients can be forced to reassociate if the intruder laptop uses a WLAN card capable of emitting at least 5 times more power than the authorized access point.
D. When the signal between the clients and the authorized access point is permanently disrupted and the intruder software access point is using the same SSID and the same channel as the authorized access point, the clients will reassociate to the software access point.

Answer: A

QUESTION 51:

A WLAN security policy should address which two of the following elements? (Choose two)

A. Security policy details should only be known by IT staff to prevent abuse
B. Enabling encryption to prevent SSIDs from being sent in clear text
C. Social engineering mitigation techniques
D. Verification that all wireless infrastructure devices are attached to the network core
E. Use of rotating encryption key mechanisms as defined in the 802.11 standard
F. End user training on security solutions

Answer: C,F

QUESTION 52:

Certkiller .com has recently installed an 802.11g WLAN. Certkiller .com requires the ability to control access to network services, such as file shares, intranet web servers, and Internet access based on an employee's job functions. Of the following WLAN security solution options, which one satisfies Certkiller .com's requirement?

A. An Enterprise Encryption Gateway with LDAP support
B. A WLAN controller with RBAC features
C. A WLAN router with wireless VLAN support
D. A VPN server with multiple DHCP scopes, one for a each type of user
E. An autonomous access point with MAC filters

Answer: B

QUESTION 53:

Which of the following are two password-related items that you, as an administrator, should include in a security policy when implementing a WLAN? (Choose two)

A. Passwords should be at least as long as usernames when user authentication is used instead of hardware authentication.
B. Passwords should contain numbers, special characters, and upper and lower case letters.
C. The password policy should be extended to provide guidance on selecting passphrases for security solutions such as WPA2-Personal.
D. Service Set Identifiers (SSIDs) should be configured to the same length and strength requirements as any other administrative-level password in the enterprise.
E. Certificates should always be used instead of passwords when securing a WLAN.

Answer: B,C

QUESTION 54:

You manage a Certkiller .com wireless network that services 100 wireless users. Certkiller .com's facility needs 7 access points, and you have installed an 802.11i-compliant implementation of 802.1X/LEAP (Transient Key IP) as an authentication and encryption solution. Which of the following is the type of attack that the wireless network is susceptible to in this configuration?

A. Man-in-the-middle
B. Session hijacking
C. Layer 3 peer-to-peer
D. Password dictionary
E. Eavesdropping
F. WEP cracking

Answer: D

QUESTION 55:

To locate their WLAN switch/controller, Lightweight (thin) access points use which of the following valid method?

A. Lightweight access points identify their controller by the LOCN field in the controller's beacon frames.
B. The access points can use the Dynamic Thin Access Point Protocol (DTAPP) to identify and communicate with a controller.
C. Lightweight access points are programmed with the DNS name of the controller. They receive an IP address and the address of a DNS server from a DHCP server.
D. Lightweight access points use SNMP to determine the host name and IP address of the

controller.
E. Controllers use the Address Resolution Protocol (ARP) to map Layer 3 IP addresses to the MAC addresses of the access points.
F. Controllers contain unique Radio Frequency Identifier (RFID) tags that can be located and tracked by lightweight access points.

Answer: C

QUESTION 56:

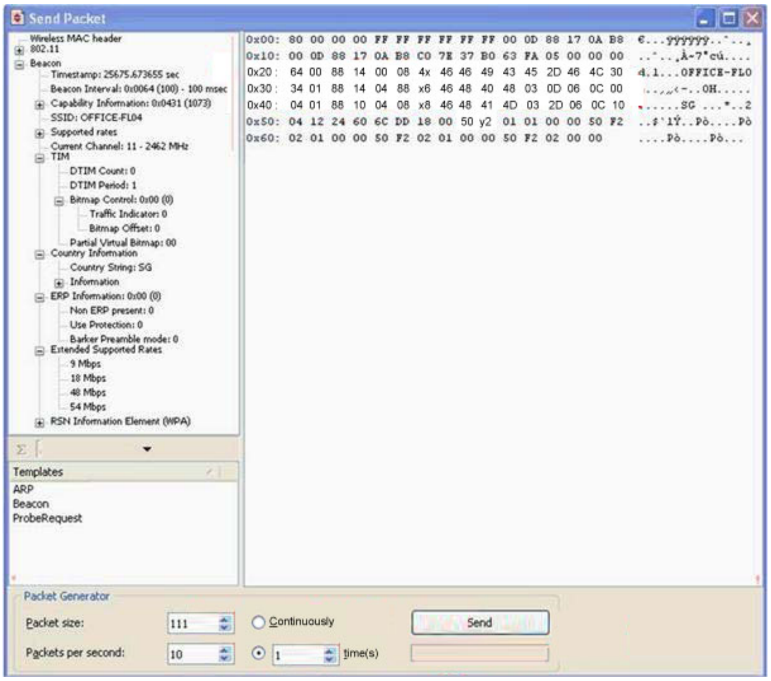
A WIPS detected a new access point connected to an authorized network segment. Which of the following is applied to the new access point by the WIPS? (Choose all that apply)

A. Default security policy
B. FIPS values
C. SNMP MIB
D. Updated firmware
E. Site survey template
F. User property profile

Answer: A

QUESTION 57:

Exhibit:



```
Wireless MAC header
⊞ 802.11
⊟ Beacon
    Timestamp: 25675.673655 sec
    Beacon Interval: 0x0064 (100) - 100 msec
  ⊞ Capability Information: 0x0431 (1073)
    SSID: OFFICE-FL04
  ⊞ Supported rates
    Current Channel: 11 - 2462 MHz
  ⊟ TIM
      DTIM Count: 0
      DTIM Period: 1
    ⊟ Bitmap Control: 0x00 (0)
        Traffic Indicator: 0
        Bitmap Offset: 0
      Partial Virtual Bitmap: 00
  ⊟ Country Information
      Country String: SG
    ⊞ Information
  ⊟ ERP Information: 0x00 (0)
      Non ERP present: 0
      Use Protection: 0
      Barker Preamble mode: 0
  ⊟ Extended Supported Rates
      9 Mbps
      18 Mbps
      48 Mbps
      54 Mbps
  ⊞ RSN Information Element (WPA)
```

```
0x00: 80 00 00 00 FF FF FF FF FF FF 00 0D 88 17 0A B8  €...ÿÿÿÿÿÿ..ˆ...¸
0x10: 00 0D 88 17 0A B8 C0 7E 37 B0 63 FA 05 00 00 00  ..ˆ..¸À~7°cú....
0x20: 64 00 88 14 00 08 4x 46 46 49 43 45 2D 46 4C 30  d.ˆ...OFFICE-FL0
0x30: 34 01 88 14 04 88 x6 46 48 40 48 03 0D 06 0C 00  4.ˆ..ˆ‹-..0H.....
0x40: 04 01 88 10 04 08 x8 46 48 41 4D 03 2D 06 0C 10  ......SG ...*..2
0x50: 04 12 24 60 6C DD 18 00 50 y2 01 01 00 00 50 F2  ..$`lÝ..Pò....Pò
0x60: 02 01 00 00 50 F2 02 01 00 00 50 F2 02 00 00     ....Pò....Pò...
```

ARP
Beacon
ProbeRequest

Packet size: 111
○ Continuously
Packets per second: 10
● 1 time(s)

The above exhibit displays a WLAN software tool that can transmit customized 802.11

frames. Which of the following are two uses for such a tool? (Choose two)

A. Auditing the security features of a WIPS
B. Changing the supported data rates on an AP
C. Monitoring for unencrypted passwords as they traverse the WLAN
D. Deauthentication attacks
E. Modifying a network's logical topology
F. Altering physical layer frame headers for frame injection attacks

Answer: A,D

QUESTION 58:

Of the following, which are two wireless security protocols that offer mutual authentication without using x.509 certificates? (Choose two)

A. PEAPv0/EAP-MSCHAPv2
B. PEAPv1/EAP-GTC
C. EAP-TLS
D. EAP-TTLS
E. EAP-FAST
F. LEAP

Answer: E,F

QUESTION 59:

Which of the following denotes what the immediate response of the network administrative staff should be if a rogue access point is detected on a network?

A. Shut down the entire network until an investigation can be completed and the logs reviewed.
B. Immediately dispose of the rogue access point and notify management.
C. Detach the access point from the wired network and follow the organization response policy.
D. Call the police and lock everyone inside the facility.
E. Make a list of everyone who was near the access point at the time of its discovery.
F. Inform the security guard staff to begin parking lot patrols immediately.

Answer: C

QUESTION 60:

which of the following are the two options required to maintain a secure WLAN as soon as strong authentication and encryption mechanisms are implemented and tested in a WLAN? (Choose two)

A. Internet firewall
B. Personal firewalls
C. LDAP
D. VPN
E. WIPS

Answer: B,E

QUESTION 61:

Which of the following is an advantage that 802.1X/EAP-TLS has over an IPSec/ESP VPN as a WLAN security solution, if both are designed to utilize client-side and server-side x.509 certificates?

A. EAP-TLS is based on HTTPS, allowing Layer 2 encryption keys to be exchanged inside a secure tunnel.
B. EAP-TLS has less protocol overhead and therefore higher throughput at the same data rate.
C. A data frame protected with EAP-TLS encryption has two privacy fields in the header, providing two layers of security.
D. EAP-TLS protects the client's username and password inside an encrypted tunnel, but IPSec does not.

Answer: B

QUESTION 62:

Certkiller .com utilizes their 802.11a/g WLAN extensively to transfer general data traffic, VoWLAN traffic, and guest access Internet-only data. Which of the following is the best method to attain the highest level of security and QoS for each data type, while reducing troubleshooting complexity across the entire WLAN?

A. Implement DiffServ bit detection and transference for QoS and security.
B. 802.11h should be implemented for QoS and 802.11i should be implemented for security. This is true for 802.11a and 802.11g.
C. Each data type should be on a separate VLAN.
D. Each QoS and security level should have its own SSID
E. Guest access should use 802.11g and all other traffic should use 802.11a.

Answer: C

QUESTION 63:

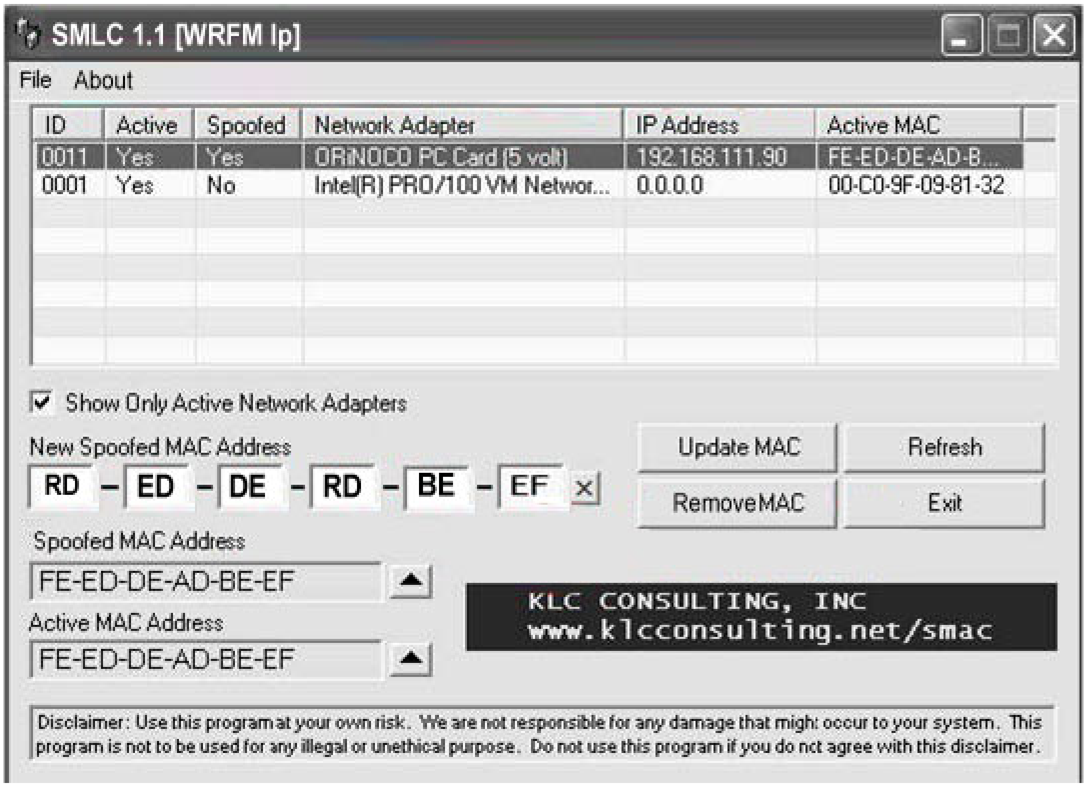
Which three of the following policies would prevent peer-to-peer attacks against wireless-enabled corporate laptop computers, if these laptops are utilized on public access networks such as wireless hotspots as well? (Choose three)

A. Require secure applications such as POP3/S, HTTPS, and SSH2.
B. Require WPA2-Enterprise as the minimal WLAN security solution.
C. Require Port Address Translation (PAT) on each laptop.
D. Require personal firewall software on each laptop.
E. Require VPN software for connectivity to the corporate network.

Answer: A,D,E

QUESTION 64:

Exhibit:



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	ORiNOCO PC Card (5 volt)	192.168.111.90	FE-ED-DE-AD-B...
0001	Yes	No	Intel(R) PRO/100 VM Networ...	0.0.0.0	00-C0-9F-09-81-32

☑ Show Only Active Network Adapters

New Spoofed MAC Address: RD - ED - DE - RD - BE - EF

Spoofed MAC Address: FE-ED-DE-AD-BE-EF

Active MAC Address: FE-ED-DE-AD-BE-EF

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Which of the following is a WLAN attack that can be carried out using the illustrated software utility?

A. Bit flipping

B. 802.1X EAP Start flood
C. Fake AP
D. MAC address spoofing
E. 802.11 deauthentication

Answer: D

QUESTION 65:

You are a network administrator at Certkiller .com. You are instructed to securely transfer a Certkiller .com's new operating system image to a WLAN switch/controller. Which of the following are two protocols that will allow you to carry this out? (Choose two)

A. SNMPv2c
B. SCP
C. HTTPS
D. FTP
E. TFTP

Answer: B,C

QUESTION 66:

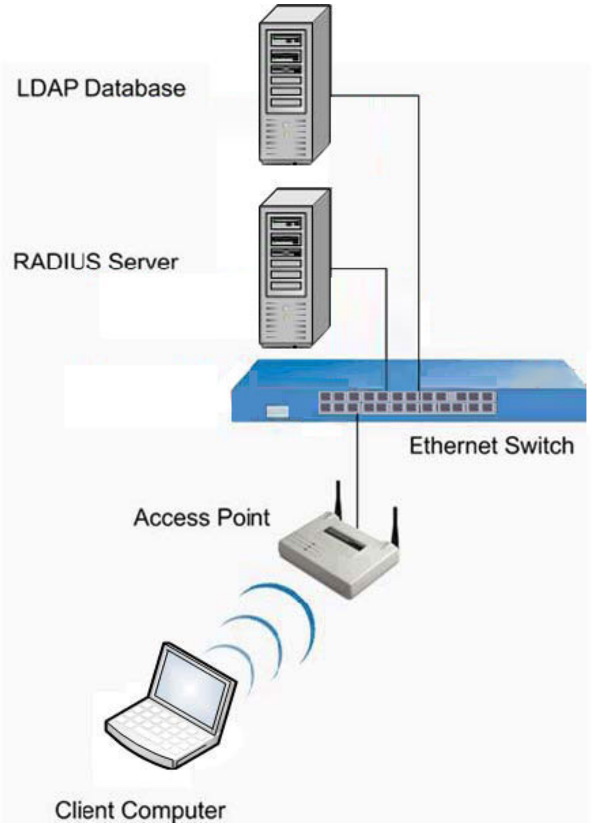
Most of the current lightweight (thin) access points today support 802.3af and can be positioned anywhere in the network infrastructure, rather than directly connected to a WLAN switch/controller port. Which of the following is logical connection that a lightweight access point can make to its controller?

A. RSVP protocol connection
B. LLC port connection
C. GRE tunnel
D. Mobile IP connection
E. HTTPS tunnel

Answer: C

QUESTION 67:

Exhibit:



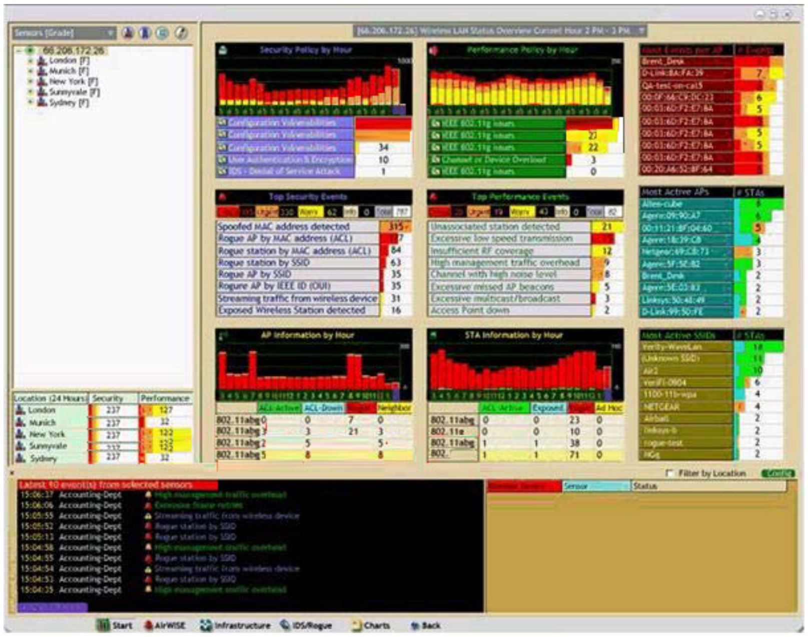
The exhibit displays a Certkiller .com network diagram that implements an 802.1X/EAP-based wireless security solution. which of the following is the device that operates as the EAP Supplicant?

A. Wireless Client Computer
B. Access Point
C. LDAP Database
D. RADIUS Server
E. Ethernet Switch

Answer: A

QUESTION 68:

Exhibit #1:



[66.206.172.26] Wireless LAN Status Overview Current Hour 2 PM - 3 PM

Sensors [Grade]

- 66.206.172.26
  - London [F]
  - Munich [F]
  - New York [F]
  - Sunnyvale [F]
  - Sydney [F]

Security Policy by Hour

Configuration Vulnerabilities	
Configuration Vulnerabilities	
Configuration Vulnerabilities	34
User Authentication & Encryption	10
IDS - Denial of Service Attack	1

Performance Policy by Hour

IEEE 802.11g issues	
IEEE 802.11g issues	27
IEEE 802.11g issues	22
Channel or Device Overload	3
IEEE 802.11g issues	0

Most Events per AP	# Events
Brent_Desk	
D-Link:BA:FA:39	7
QA-test-on-cal5	
00:0F:66:C8:DC:22	6
00:01:6D:F2:E7:8A	5
00:01:6D:F2:E7:8A	
00:01:6D:F2:E7:8A	5
00:01:6D:F2:E7:8A	5
00:01:6D:F2:E7:8A	
00:20:A6:52:BF:64	

Top Security Events

Urgent 330 Warn 62 Info 0 Total 787

Spoofed MAC address detected	315
Rogue AP by MAC address (ACL)	7
Rogue station by MAC address (ACL)	84
Rogue station by SSID	63
Rogue AP by SSID	35
Rogue AP by IEEE ID (OUI)	35
Streaming traffic from wireless device	31
Exposed Wireless Station detected	16

Top Performance Events

Urgent 19 Warn 43 Info 0 Total 82

Unassociated station detected	21
Excessive low speed transmission	
Insufficient RF coverage	12
High management traffic overhead	9
Channel with high noise level	8
Excessive missed AP beacons	5
Excessive multicast/broadcast	3
Access Point down	2

Most Active APs	# STAs
Allen-cube	
Agere:09:90:A7	
00:11:21:8F:04:60	5
Agere:18:39:C8	
Netgear:49:C8:73	3
Agere:5F:5E:82	3
Brent_Desk	2
Agere:5E:03:83	2
Linksys:50:48:49	2
D-Link:99:50:FE	2

AP Information by Hour

	ACL-Active	ACL-Down		Neighbor
802.11abg	0	7	0	
802.11abg	3	21	3	
802.11abg	5		5	
802.11abg	8		8	

STA Information by Hour

	ACL-Active	Exposed		Ad Hoc
802.11abg	0	0	23	0
802.11a	0	0	10	0
802.11abg	1	1	38	0
802.	1	1	71	0

Most Active SSIDs	# STAs
Verity-WaveLan	18
(Unknown SSID)	11
Air2	10
VeriFi-0904	6
1100-11b-wpa	4
NETGEAR	4
Airball	2
linksys-b	2
rogue-test	2
NGq	2

Location (24 Hours)	Security	Performance
London	237	127
Munich	237	32
New York	237	122
Sunnyvale	237	122
Sydney	237	32

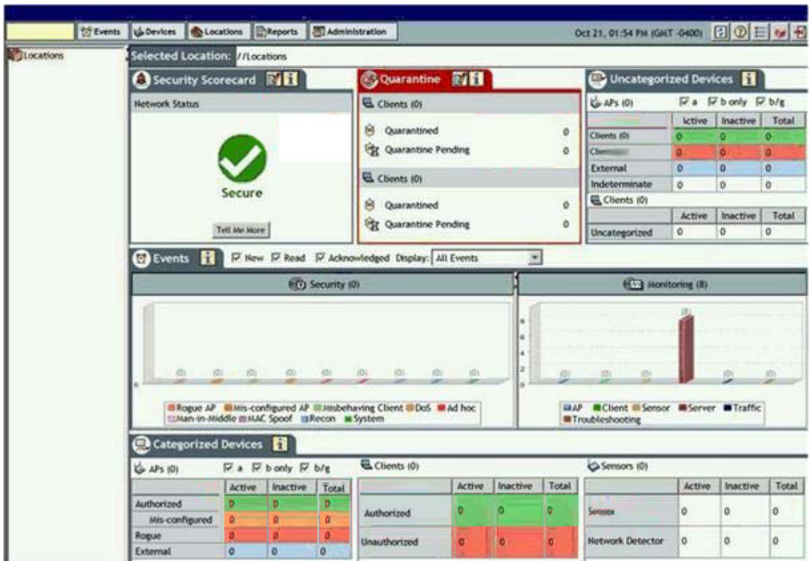
☐ Filter by Location

Latest 10 event(s) from selected sensors

```
15:06:37 Accounting-Dept   High management traffic overhead
15:06:06 Accounting-Dept   Excessive frame retries
15:05:55 Accounting-Dept   Streaming traffic from wireless device
15:05:52 Accounting-Dept   Rogue station by SSID
15:05:13 Accounting-Dept   Rogue station by SSID
15:04:58 Accounting-Dept   High management traffic overhead
15:04:55 Accounting-Dept   Rogue station by SSID
15:04:54 Accounting-Dept   Streaming traffic from wireless device
15:04:53 Accounting-Dept   Rogue station by SSID
15:04:35 Accounting-Dept   High management traffic overhead
```

Sensor | Status

Exhibit #2:



Oct 21, 01:54 PM (GMT -0400)

Selected Location: //Locations

Security Scorecard

Network Status

Secure

Quarantine

Clients (0)

Quarantined	0
Quarantine Pending	0

Clients (0)

Quarantined	0
Quarantine Pending	0

Uncategorized Devices

APs (0) ☑ a ☑ b only ☑ b/g

	ctive	Inactive	Total
Clients (0)	0	0	0
Clien	0	0	0
External	0	0	0
Indeterminate	0	0	0

Clients (0)

	Active	Inactive	Total
Uncategorized	0	0	0

Events ☑ New ☑ Read ☑ Acknowledged Display: All Events

Security (0)

Monitoring (8)

Categorized Devices

APs (0) ☑ a ☑ b only ☑ b/g

	Active	Inactive	Total
Authorized	0	0	0
Mis-configured	0	0	0
Rogue	0	0	0
External	0	0	0

Clients (0)

	Active	Inactive	Total
Authorized	0	0	0
Unauthorized	0	0	0

Sensors (0)

	Active	Inactive	Total
Sensor	0	0	0
Network Detector	0	0	0

Which of the following best describes the system types illustrated by "Exhibit #1" and "Exhibit #2"? (Choose all that apply)

A. WNMS access point monitors
B. RF spectrum scanners
C. WIPS dashboards
D. Wireless VPN management systems
E. WLAN switch device monitors

Answer: C

QUESTION 69:

Certkiller .com's marketing department WLAN users need to contact their own server and the Internet, but must NOT have access to any other network resources. To comply with these requirements, which of the following WLAN security features should you employ? (Choose all that apply)

A. Wireless routing
B. Captive portal
C. Mutual authentication
D. Role-based access control

Answer: D

QUESTION 70:

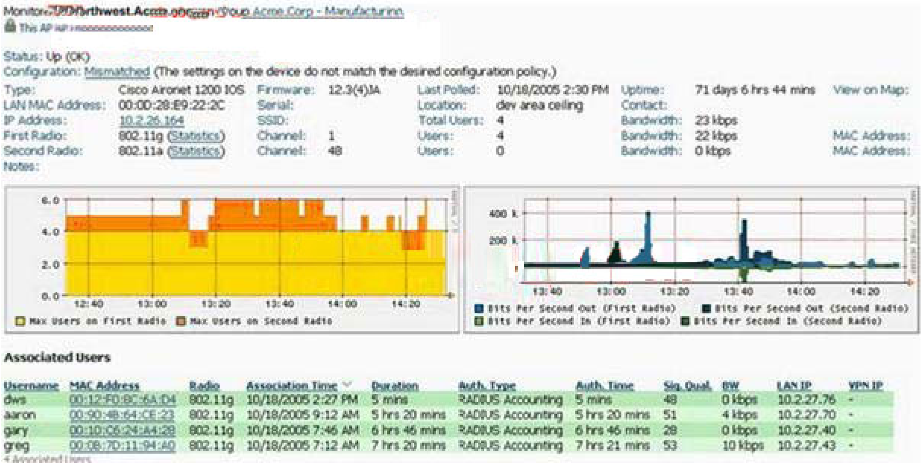
Certkiller .com's IT staff has agreed that an Enterprise Encryption Gateway (EEG) using a strong, proprietary, Layer 2 encryption technique satisfies their corporate wireless security policy requirements. The access points are positioned on the encrypted segment of the network. Of the following options, which one specifies what is needed to administer the access points from a management workstation found on the network backbone?

A. This management technique is not possible. Access points on the encrypted side of an EEG can only be managed from the encrypted segment.
B. The access points must support AES encryption.
C. A proxy client must be located on the encrypted segment and configured to relay management traffic from the management station to each access point.
D. The EEG must be configured to allow destination-specific unencrypted traffic to traverse the encrypted segment.

Answer: D

QUESTION 71:

Exhibit:



Monitor > Northwest.Acme... Group Acme Corp - Manufacturing

This AP [illegible]

Status: Up (OK)

Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)

Type:	Cisco Aironet 1200 IOS	Firmware:	12.3(4)JA	Last Polled:	10/18/2005 2:30 PM	Uptime:	71 days 6 hrs 44 mins	View on Map:
LAN MAC Address:	00:0D:28:E9:22:2C	Serial:		Location:	dev area ceiling	Contact:		
IP Address:	10.2.26.164	SSID:		Total Users:	4	Bandwidth:	23 kbps	
First Radio:	802.11g (Statistics)	Channel:	1	Users:	4	Bandwidth:	22 kbps	MAC Address:
Second Radio:	802.11a (Statistics)	Channel:	48	Users:	0	Bandwidth:	0 kbps	MAC Address:
Notes:								

6.0
4.0
2.0
0.0
12:40
13:00
13:20
13:40
14:00
14:20
Max Users on First Radio
Max Users on Second Radio
400 k
200 k
12:40
13:00
13:20
13:40
14:00
14:20
Bits Per Second Out (First Radio)
Bits Per Second Out (Second Radio)
Bits Per Second In (First Radio)
Bits Per Second In (Second Radio)

Associated Users

Username	MAC Address	Radio	Association Time	Duration	Auth. Type	Auth. Time	Sig. Qual.	BW	LAN IP	VPN IP
dws	00:12:F0:8C:6A:D4	802.11g	10/18/2005 2:27 PM	5 mins	RADIUS Accounting	5 mins	48	0 kbps	10.2.27.76	-
aaron	00:90:4B:64:CE:23	802.11g	10/18/2005 9:12 AM	5 hrs 20 mins	RADIUS Accounting	5 hrs 20 mins	51	4 kbps	10.2.27.70	-
gary	00:10:C6:24:A4:28	802.11g	10/18/2005 7:46 AM	6 hrs 46 mins	RADIUS Accounting	6 hrs 46 mins	28	0 kbps	10.2.27.40	-
greg	00:0B:7D:11:94:A0	802.11g	10/18/2005 7:12 AM	7 hrs 20 mins	RADIUS Accounting	7 hrs 21 mins	53	10 kbps	10.2.27.43	-

4 Associated Users

Which two of the following secure protocols are utilized by a wireless network management system when monitoring access points as illustrated above? (Choose two)

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

Answer: A,D

QUESTION 72:

Which requirement has to be part of the WIPS installation, so that WIPS can describe the location of a rogue WLAN device?

A. A GPS system must be installed including the coordinates of the building's corners.
B. A graphical floor plan diagram must be imported into the WIPS.
C. All authorized AP radios must be placed in RF monitor mode so that the WIPS knows where the authorized APs are in relation to the WIPS sensors.
D. The predictive site survey results must be imported into the WIPS.

Answer: B

QUESTION 73:

Which of the following best describes the function of the 802.11i STAKey Handshake in a WLAN BSS? (Choose all that apply)

A. Initiating an 802.11r handoff, allowing access points to use the IAPP protocol
B. Producing keys for securing data frames directly between stations while associated with an access point

C. Producing Group Transient Keys for encrypting multicast and broadcast frames in a BSS
D. Allows client stations to securely authenticate to a repeater access point
E. Allows supplicants to roam across access points they have not previously associated to without using the 802.1X/EAP authentication process
F. Initiates 802.11e client prioritization, ensuring two stations can control the medium until a data exchange is complete

Answer: B

QUESTION 74:

Which of the following best describes how rogue access points are discovered when using a Wireless Network Management System (WNMS)?

A. Authorized access points detect unauthorized RF fluctuations on channels where rogue access points are deployed. These fluctuations are reported via SNMP to the WNMS.
B. Proprietary detection protocols run on the 802.11a/g access points and report all discovered access points to the WNMS analytics engine.
C. An open source finder tool is deployed by all WNMS vendors. This tool probes the RF channels for rogue access points and reports to the WNMS.
D. Access points report all BSSID values they can hear to the WNMS via SNMP. The BSSID values are compared against an authorized access point list.
E. Dedicated sensor access points are deployed throughout the coverage area.

Answer: D

QUESTION 75:

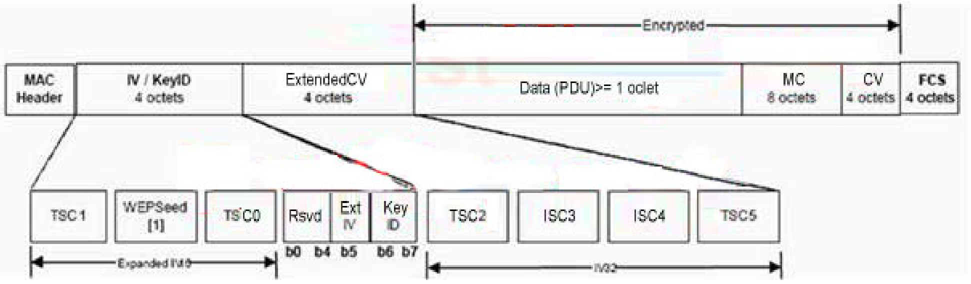
Certkiller .com has just deployed a WLAN switch and RADIUS server, and have to transfer authenticated wireless users from different departments onto their chosen network segments. This should be accomplished in which of the following ways? (Choose all that apply)

A. The WLAN user must contact the network administrator at step 4 of the 802.1X/EAP authentication process to receive a network number.
B. RADIUS will send a return list attribute with the GRE tunnel number to the WLAN switch.
C. Manually map each wireless user's MAC address to a VLAN number in the Ethernet switch.
D. The RADIUS server coordinates with an authenticated DHCP server.
E. Implement multiple 802.1Q VLANs in both the WLAN and Ethernet switches.

Answer: E

QUESTION 76:

Exhibit:



An expanded Transient Key IP MPDU is displayed in the exhibit above. Which two of the following features were included in Transient Key IP to improve the security of WEP? (Choose two)

A. ICV
B. MIC
C. Encrypted PDU
D. FCS
E. Extended IV

Answer: B,E

QUESTION 77:

Certkiller .com has decided that installing, securing, and maintaining a wireless infrastructure is beyond their IT budget for this calendar year. Certkiller .com do, however, believe that there are advantages to employing wireless Ad Hoc networks in their environment, particularly for meetings. Certkiller .com eventually decides to utilize wireless Ad Hoc networks, but are worried about security. which three of the following statements concerning wireless Ad Hoc network security are TRUE? (Choose three)

A. WPA2-Enterprise allows Ad Hoc networks to scale to a larger number of users than WPA2-Personal.
B. The IEEE 802.11i standard supports an authenticator and authentication server on each client device that is part of the wireless Ad Hoc network.
C. WPA2 passphrases are the most effective, low-cost mechanism for protecting wireless Ad Hoc networks from eavesdropping.
D. IPSec client software and personal firewall software on each client provide strong WLAN security for Ad Hoc networks.

Answer: B,C,D

QUESTION 78:

Certkiller .com is an Internet Service Provider with thousands of customers, who employs a LDAP server as the central user credential database. In which way can Certkiller .com utilize their existing user database for wireless user authentication, as they deploy a large-scale WPA2-Enterprise WLAN security solution?

A. Import all users from the LDAP server into the RADIUS server with an LDAP-to-RADIUS conversion tool.
B. Install a TACACS+ server, configure an ODBC connection between the TACACS+ and LDAP servers, and have the TACACS+ server query the LDAP server.
C. Implement a RADIUS server and proxy user authentication requests to the LDAP server.
D. Implement an x.509 compliant Certificate Authority and enable SSL queries on the LDAP server.

Answer: C

QUESTION 79:

Certkiller .com is implementing a single WLAN switch/controller with 6 lightweight (thin) access points that can authenticate users directly against a Kerberos-based authentication database. Certkiller .com does not have a RADIUS server. Which of the following is the device that generates new encryption keys as wireless client devices roam between access points?

A. WLAN switch/controller
B. Ethernet switch
C. Kerberos server
D. Lightweight access points
E. Client device

Answer: A

QUESTION 80:

Which of the following is preventative measure executed by a WIPS against intrusions?

A. NAV attack against an unclassified AP
B. Evil twin attack against a rogue AP
C. Deauthentication attack against an authorized client associating to a rogue AP
D. Disassociation attack against an external AP that is not connected to your network
E. EAPoL Start frame flood against a rogue AP

Answer: C

QUESTION 81:

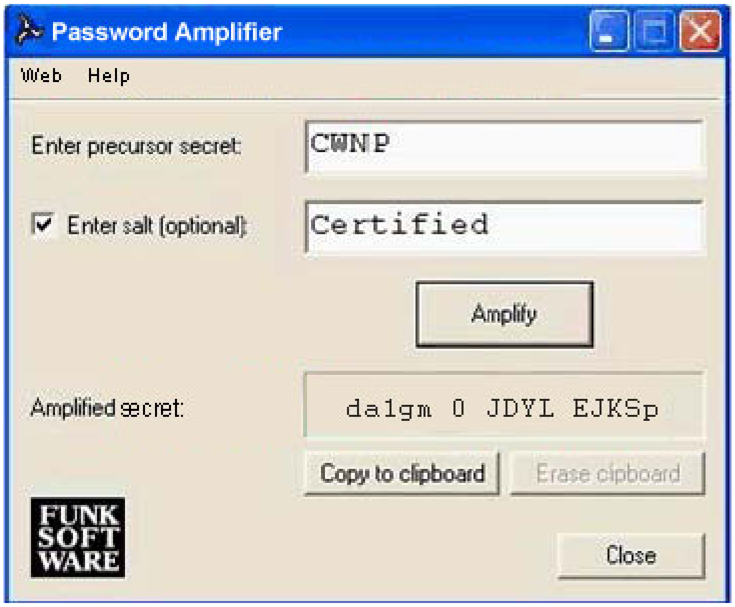
In 802.11i Authentication and Key Management, which of the following is the function of the Pairwise Transient Key ?

A. The Pairwise Transient Key is combined with a nonce during the 802.11i 4-Way Handshake to create the GMK.
B. The Pairwise Transient Key is used to encrypt the Pairwise Master Key (PMK) for distribution to the 802.1X Authenticator during the 802.11i 4-Way Handshake.
C. The Pairwise Transient Key is used to encrypt unicast data frames that traverse the wireless medium.
D. The Pairwise Transient Key is XOR'd with the PSK on the Authentication server to create the AAA key.
E. The GMK, used for encrypting multicast data frames, is derived from the Pairwise Transient Key.

Answer: C

QUESTION 82:

Exhibit:



Enter precursor secret: CWNP

☑ Enter salt (optional): Certified

Amplified secret: da1gm 0 JDYL EJKSp

Which of the following are two WLAN security functions that can be executed by the software utility illustrated in the above exhibit? (Choose two)

A. Generating random EAP-TTLS session keys
B. Generating strong passwords for protecting a RADIUS server from application layer WLAN attacks
C. Generating strong passwords for 802.11i-compliant 802.1X/EAP-TLS systems

D. Generating strong passwords for WLAN infrastructure equipment logins
E. Generating strong passwords for WLAN systems secured with WPA2-Personal

Answer: D,E

QUESTION 83:

Certkiller .com recently installs a WLAN switch/controller solution that uses WPA2-Enterprise security. Certkiller .com configures a security profile on the WLAN switch for each group within the company (Marketing, Sales, and Engineering). Which of the following describes how authenticated users are assigned to groups to obtain the appropriate security profile?

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

Answer: B

QUESTION 84:

Certkiller .com has just employed IPSec VPN technology, using the Authentication Header (AH) protocol, to secure their wireless connections. Certkiller .com hires you as a security auditor, for the purpose of testing the security strength of the wireless network. Which of the following is a TRUE statement with regard to this WLAN security implementation?

A. AH uses 3DES encryption, causing high latency on half-duplex networks.
B. AH uses public key cryptography, which is incompatible with the 802.11 protocol.
C. The AH protocol does not encrypt the data payload, so the ESP protocol should be used.
D. Wireless clients should be configured for NAT transparency, so encrypted frames can traverse gateways.
E. When using AH as a VPN solution, the implementation must incorporate SSH2 tunneling.

Answer: C

QUESTION 85:

What security protocols can use MS-CHAPv2 or EAP-TLS for wireless client authentication?

A. LEAP
B. PPTP
C. L2TP
D. IPSec
E. PEAP

Answer: B,E

QUESTION 86:

Which of the following best explains the role of LDAP, when it is employed as part of a WLAN authentication solution? (Choose all that apply)

A. An X.500 standard compliant database that can be queried by 802.1X compliant devices
B. An EAP compliant port access control mechanism for blocking connections until users are authenticated
C. A SQL compliant authentication service capable of encryption key generation and distribution
D. A data retrieval protocol used by an authentication service such as RADIUS

Answer: D

QUESTION 87:

Certkiller .com currently employs a Public Key Infrastructure (PKI) to permit employees to securely access network resources using smart cards. The wireless segment of Certkiller .com's network utilizes WPA-Enterprise as its primary security solution. You have been hired by Certkiller .com to suggest a Wi-Fi Alliance-approved EAP method. Which two of the following solutions will involve the smallest amount of change in the way users are currently authenticated and still integrate with their existing PKI? (Choose two)

A. EAP-FAST
B. PEAPv0/EAP-MSCHAPv2
C. LEAP
D. PEAPv1/EAP-GTC
E. EAP-TLS

Answer: D,E

QUESTION 88:

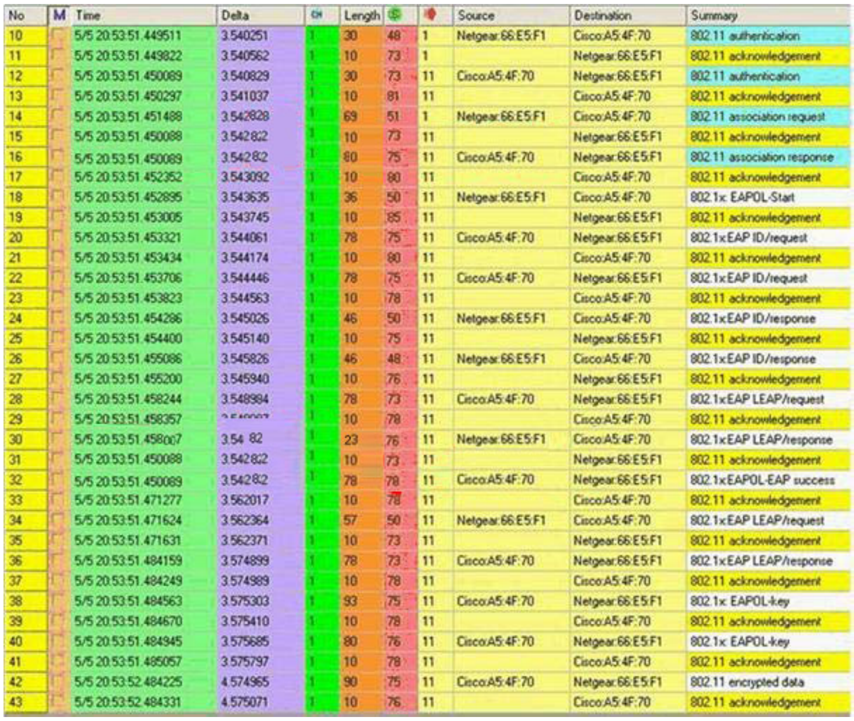
Certkiller .com transmits highly sensitive data files and email over the wireless network every day. Certkiller .com has decided that unbreakable standards-based authentication and data encryption are required on their new wireless LAN to prevent eavesdropping attacks. Certkiller .com has documented this requirement in their corporate security policy. You are contracted to implement a wireless security solution that satisfies Certkiller .com's policy requirements. Certkiller .com has 3 access points and 15 users. Which of the following are two appropriate wireless LAN security solutions? (Choose two)

A. WPA2-Personal with a strong passphrase
B. 802.1X/Kerberos
C. WPA2-Enterprise with EAP-FAST
D. IPSec/AH VPN with RBAC
E. PPTP/MPPE-128 VPN

Answer: A,C

QUESTION 89:

Exhibit:



No	M	Time	Delta	CH	Length			Source	Destination	Summary
10	☐	5/5 20:53:51.449511	3.540251	1	30	48	1	Netgear:66:E5:F1	Cisco:A5:4F:70	802.11 authentication
11	☐	5/5 20:53:51.449822	3.540562	1	10	73	1		Netgear:66:E5:F1	802.11 acknowledgement
12	☐	5/5 20:53:51.450089	3.540829	1	30	73	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.11 authentication
13	☐	5/5 20:53:51.450297	3.541037	1	10	81	11		Cisco:A5:4F:70	802.11 acknowledgement
14	☐	5/5 20:53:51.451488	3.542828	1	69	51	1	Netgear:66:E5:F1	Cisco:A5:4F:70	802.11 association request
15	☐	5/5 20:53:51.450088	3.542822	1	10	73	11		Netgear:66:E5:F1	802.11 acknowledgement
16	☐	5/5 20:53:51.450089	3.54282	1	80	75	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.11 association response
17	☐	5/5 20:53:51.452352	3.543092	1	10	80	11		Cisco:A5:4F:70	802.11 acknowledgement
18	☐	5/5 20:53:51.452895	3.543635	1	36	50	11	Netgear:66:E5:F1	Cisco:A5:4F:70	802.1x: EAPOL-Start
19	☐	5/5 20:53:51.453005	3.543745	1	10	85	11		Netgear:66:E5:F1	802.11 acknowledgement
20	☐	5/5 20:53:51.453321	3.544061	1	78	75	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x:EAP ID/request
21	☐	5/5 20:53:51.453434	3.544174	1	10	80	11		Cisco:A5:4F:70	802.11 acknowledgement
22	☐	5/5 20:53:51.453706	3.544446	1	78	75	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x:EAP ID/request
23	☐	5/5 20:53:51.453823	3.544563	1	10	78	11		Cisco:A5:4F:70	802.11 acknowledgement
24	☐	5/5 20:53:51.454286	3.545026	1	46	50	11	Netgear:66:E5:F1	Cisco:A5:4F:70	802.1x:EAP ID/response
25	☐	5/5 20:53:51.454400	3.545140	1	10	75	11		Netgear:66:E5:F1	802.11 acknowledgement
26	☐	5/5 20:53:51.455086	3.545826	1	46	48	11	Netgear:66:E5:F1	Cisco:A5:4F:70	802.1x:EAP ID/response
27	☐	5/5 20:53:51.455200	3.545940	1	10	76	11		Netgear:66:E5:F1	802.11 acknowledgement
28	☐	5/5 20:53:51.458244	3.548984	1	78	73	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x:EAP LEAP/request
29	☐	5/5 20:53:51.458357	[illegible]	1	10	78	11		Cisco:A5:4F:70	802.11 acknowledgement
30	☐	5/5 20:53:51.458007	3.54 82	1	23	76	11	Netgear:66:E5:F1	Cisco:A5:4F:70	802.1x:EAP LEAP/response
31	☐	5/5 20:53:51.450088	3.542822	1	10	73	11		Netgear:66:E5:F1	802.11 acknowledgement
32	☐	5/5 20:53:51.450089	3.54282	1	78	78	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x:EAPOL-EAP success
33	☐	5/5 20:53:51.471277	3.562017	1	10	78	11		Cisco:A5:4F:70	802.11 acknowledgement
34	☐	5/5 20:53:51.471624	3.562364	1	57	50	11	Netgear:66:E5:F1	Cisco:A5:4F:70	802.1x:EAP LEAP/request
35	☐	5/5 20:53:51.471631	3.562371	1	10	73	11		Netgear:66:E5:F1	802.11 acknowledgement
36	☐	5/5 20:53:51.484159	3.574899	1	78	73	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x:EAP LEAP/response
37	☐	5/5 20:53:51.484249	3.574989	1	10	78	11		Cisco:A5:4F:70	802.11 acknowledgement
38	☐	5/5 20:53:51.484563	3.575303	1	93	75	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x: EAPOL-key
39	☐	5/5 20:53:51.484670	3.575410	1	10	78	11		Cisco:A5:4F:70	802.11 acknowledgement
40	☐	5/5 20:53:51.484945	3.575685	1	80	76	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.1x: EAPOL-key
41	☐	5/5 20:53:51.485057	3.575797	1	10	78	11		Cisco:A5:4F:70	802.11 acknowledgement
42	☐	5/5 20:53:52.484225	4.574965	1	90	75	11	Cisco:A5:4F:70	Netgear:66:E5:F1	802.11 encrypted data
43	☐	5/5 20:53:52.484331	4.575071	1	10	76	11		Cisco:A5:4F:70	802.11 acknowledgement

The displayed frame trace of an 802.11b client station authenticating to an access point using the 802.1X/LEAP protocol was captured by a WLAN protocol analyzer. The 802.11b access point supports which of the following levels of security? (Choose all that apply)

A. Shared Key WEP-128
B. 802.1X with Dynamic WEP
C. WPA-Enterprise
D. WPA2-Enterprise
E. WPA-Personal

Answer: B

QUESTION 90:

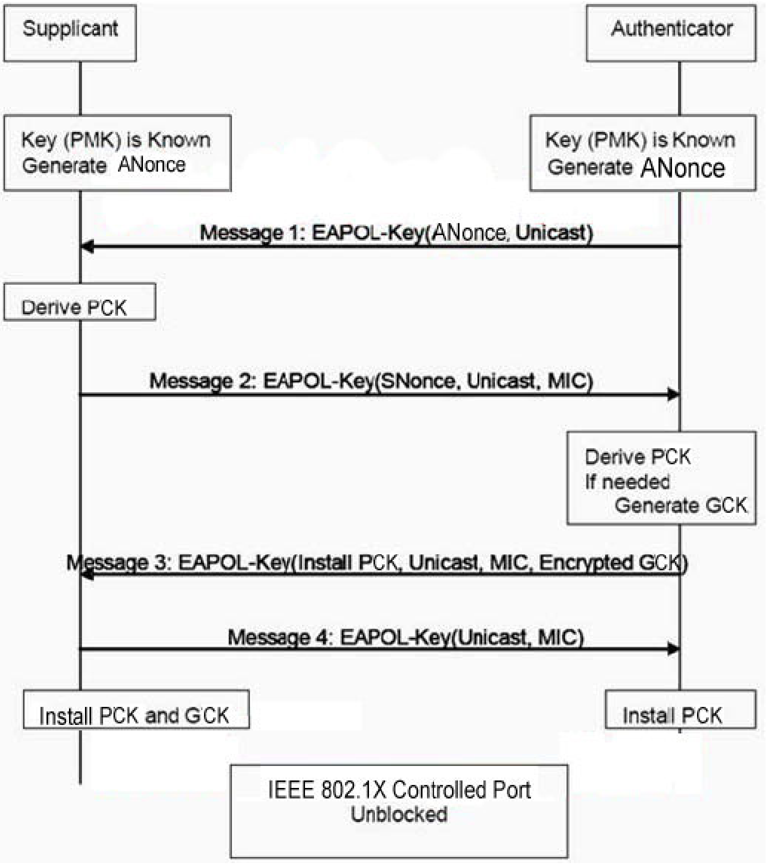
You have a laptop computer and a Wi-Fi compliant PC card. The limited effectiveness of locating rogue access points using WLAN discovery software such as Netstumbler or Kismet, is best described by which four of the following statements? (Choose four)

A. Discovery tools like Netstumbler and Kismet cannot determine the authorization status of an access point.
B. Discovery tools like Netstumbler and Kismet cannot determine if an access point is attached to a wired network.
C. A laptop computer can only be in one location at a time, even in large enterprise environments.
D. Rogue access points using non-Wi-Fi frequency bands or unpopular modulations are not detected.
E. When WEP, WPA, or WPA2 are in use, access points cannot be detected using discovery tools like Netstumbler and Kismet.

Answer: A,B,C,D

QUESTION 91:

Exhibit:


Supplicant
Authenticator
Key (PMK) is Known
Generate ANonce
Key (PMK) is Known
Generate ANonce
Message 1: EAPOL-Key(ANonce, Unicast)
Derive PCK
Message 2: EAPOL-Key(SNonce, Unicast, MIC)
Derive PCK
If needed
Generate GCK
Message 3: EAPOL-Key(Install PCK, Unicast, MIC, Encrypted GCK)
Message 4: EAPOL-Key(Unicast, MIC)
Install PCK and GCK
Install PCK
IEEE 802.1X Controlled Port
Unblocked

Which of the following best describes the function of the ANonce and SNonce, illustrated in this diagram from the 802.11i amendment? (Choose all that apply)

A. They are used to pad Message 1 and Message 2 so there is no empty space in the frame.
B. They are random values used in the derivation of the Pairwise Transient Key.
C. The IEEE 802.11-1999 (R2003) standard requires that all unicast frames contain a nonce for security purposes.
D. They are added together and used as the GMK, from which the Group Transient Key is derived.

Answer: B

QUESTION 92:

Which of the following is a security hole caused by a lack of staging and installation procedures for WLAN infrastructure equipment?

A. Incorrect RADIUS IP address configuration on WLAN switches
B. MAC address filters with mismatched OUIs on access points
C. Default usernames and passwords on access points
D. Default QoS priority settings

Answer: C

QUESTION 93:

The WIPS parameter configured to generate notifications is __________.

A. Probe sensitivity levels
B. Social engineering status
C. Policy threshold values
D. 802.11h TPC capacity
E. EAPoL-start frames: on/off

Answer: C

QUESTION 94:

WLAN usernames are discovered in which of the following ways by a wireless network management system (WNMS)? (Choose all that apply)

A. The RADIUS server sends the username to the WNMS after the wireless device successfully authenticates.
B. The client device sends the username to the WNMS on port 113 (ident service) after successful authentication.
C. The WNMS polls access points using SNMP.
D. The WNMS captures the username by sniffing the wireless network during the authentication process.
E. The WNMS finds the MAC address of the wireless client device in the authentication database and parses the username from the entry.

Answer: C

QUESTION 95:

Which of the following are two wireless authentication technologies that build a TLS-encrypted tunnel between the supplicant and the authentication server, prior to passing client authentication credentials to the authentication server? (Choose two)

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

F. EAP-MD5

Answer: D,E

QUESTION 96:

Certkiller .com is designing a secure, scalable, and manageable 802.11g WLAN, which will support hundreds of users. when selecting the type of WLAN switch/controller to procure, which of the following is the feature that is least important?

A. WPA2-Enterprise authentication/encryption
B. SNMPv3 support
C. 802.1Q VLANs
D. Internal RADIUS server
E. Integrated WIPS

Answer: D

QUESTION 97:

You are a network administrator at Certkiller .com. Certkiller .com wants you to apply a secure VoWLAN system that is compliant with the 802.11i standard, and has the fastest roaming capability available. Which type of WLAN system would suit Certkiller .com best?

A. WLAN switches with lightweight access points
B. WLAN mesh routers
C. Wireless VoIP routers
D. Autonomous (thick) access points

Answer: A

QUESTION 98:

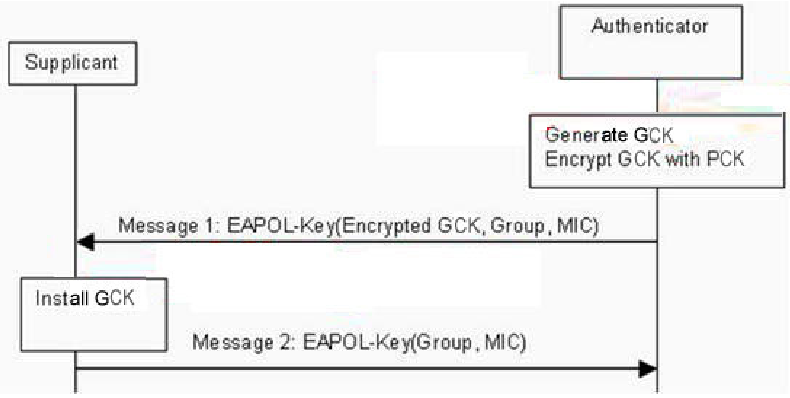
As a Certkiller .com consultant, you are requested to troubleshoot Certkiller .com's new WLAN. Numerous end users have complained about the following four problems: While browsing the Internet, the connection suddenly stops.Instant messenger sessions get randomly disconnected from the server.Despite the interruption in signal, the users WLAN utility indicates the wireless connection is good.Users' IP addresses change to a different subnet unexpectedly.
These problems are produce by which of the following wireless network attacks? (Choose all that apply)

A. Hijacking
B. Wideband RF jamming
C. Bit-flipping
D. Eavesdropping
E. PING sweep

Answer: A

QUESTION 99:

Exhibit:


Supplicant
Authenticator
Generate GCK
Encrypt GCK with PCK
Message 1: EAPOL-Key(Encrypted GCK, Group, MIC)
Install GCK
Message 2: EAPOL-Key(Group, MIC)

In which of the following instances is the illustrated 802.11i Group Key Handshake used in a WPA2-Enterprise network? (Choose all that apply)

A. When the PSK is regenerated
B. When any supplicant disassociates in a BSS
C. When a WLAN controller fails over to a backup authentication server
D. At the end of the default reassociation key timeout period
E. When a new Group Transient Key is required and a security association already exists between peers

Answer: E

QUESTION 100:

A Certkiller .com campus has 4 buildings in a hub and spoke topology (point-to-multipoint). Certkiller .com wants to link each spoke building with the hub building via wireless bridges, but they are concerned about security. Certkiller .com would like to make use of their existing VPN hardware to cut costs, and the VPN hardware only supports PPTP VPN technology. You have been hired by Certkiller .com to evaluate this recommended solution for them. which of the following paired statements best describe the use of PPTP in Certkiller .com's environment? (Choose all that apply)

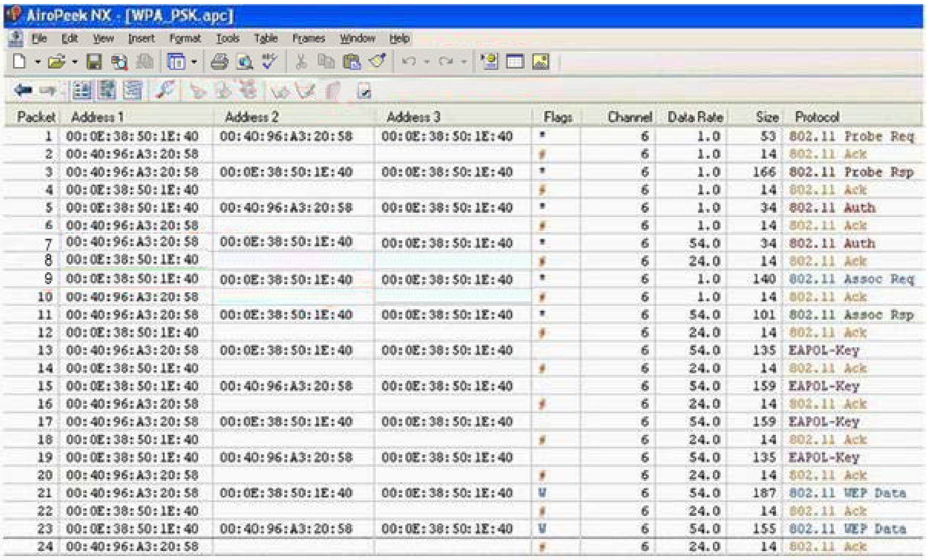
A. Advantage: PPTP provides AES encryption.
Disadvantage: PPTP is open to network layer peer attacks.

B. Advantage: PPTP provides data encryption support.
Disadvantage: PPTP does not support RADIUS authentication.
C. Advantage: PPTP is simple to implement.
Disadvantage: PPTP introduces numerous new subnet boundaries.
D. Advantage: PPTP is widely supported.
Disadvantage: PPTP does not support multiple protocols.

Answer: C

QUESTION 101:

Exhibit:


AiroPeek NX - [WPA_PSK.apc]
File Edit View Insert Format Tools Table Frames Window Help

Packet	Address 1	Address 2	Address 3	Flags	Channel	Data Rate	Size	Protocol
1	00:0E:38:50:1E:40	00:40:96:A3:20:58	00:0E:38:50:1E:40	*	6	1.0	53	802.11 Probe Req
2	00:40:96:A3:20:58			#	6	1.0	14	802.11 Ack
3	00:40:96:A3:20:58	00:0E:38:50:1E:40	00:0E:38:50:1E:40	*	6	1.0	166	802.11 Probe Rsp
4	00:0E:38:50:1E:40			#	6	1.0	14	802.11 Ack
5	00:0E:38:50:1E:40	00:40:96:A3:20:58	00:0E:38:50:1E:40	*	6	1.0	34	802.11 Auth
6	00:40:96:A3:20:58			#	6	1.0	14	802.11 Ack
7	00:40:96:A3:20:58	00:0E:38:50:1E:40	00:0E:38:50:1E:40	*	6	54.0	34	802.11 Auth
8	00:0E:38:50:1E:40			#	6	24.0	14	802.11 Ack
9	00:0E:38:50:1E:40	00:0E:38:50:1E:40	00:0E:38:50:1E:40	*	6	1.0	140	802.11 Assoc Req
10	00:40:96:A3:20:58			#	6	1.0	14	802.11 Ack
11	00:40:96:A3:20:58	00:0E:38:50:1E:40	00:0E:38:50:1E:40	*	6	54.0	101	802.11 Assoc Rsp
12	00:0E:38:50:1E:40			#	6	24.0	14	802.11 Ack
13	00:40:96:A3:20:58	00:0E:38:50:1E:40	00:0E:38:50:1E:40		6	54.0	135	EAPOL-Key
14	00:0E:38:50:1E:40			#	6	24.0	14	802.11 Ack
15	00:0E:38:50:1E:40	00:40:96:A3:20:58	00:0E:38:50:1E:40		6	54.0	159	EAPOL-Key
16	00:40:96:A3:20:58			#	6	24.0	14	802.11 Ack
17	00:40:96:A3:20:58	00:0E:38:50:1E:40	00:0E:38:50:1E:40		6	54.0	159	EAPOL-Key
18	00:0E:38:50:1E:40			#	6	24.0	14	802.11 Ack
19	00:0E:38:50:1E:40	00:40:96:A3:20:58	00:0E:38:50:1E:40		6	54.0	135	EAPOL-Key
20	00:40:96:A3:20:58			#	6	24.0	14	802.11 Ack
21	00:40:96:A3:20:58	00:0E:38:50:1E:40	00:0E:38:50:1E:40	W	6	54.0	187	802.11 WEP Data
22	00:0E:38:50:1E:40			#	6	24.0	14	802.11 Ack
23	00:0E:38:50:1E:40	00:40:96:A3:20:58	00:0E:38:50:1E:40	W	6	54.0	155	802.11 WEP Data
24	00:40:96:A3:20:58			#	6	24.0	14	802.11 Ack

The illustrated WLAN protocol analyzer shows the trace of a client station's original authentication onto the wireless network. Which of the following is the security device being employed on the WLAN?

A. IPSec/ESP
B. WPA2-Enterprise
C. WEP-128
D. 802.1X/LEAP
E. WPA-Personal

Answer: E

QUESTION 102:

Which of the following transpires in a bit flipping attack against a wireless LAN device? (Choose all that apply)

A. An attacker sends a custom frame containing all zeros in the POWER-DOWN header field, notifying the access point that it should no longer accept wireless traffic in preparation for powering down.
B. An attacker uses a non-linear Message Integrity Check (MIC) on his or her computer to form a wireless crossover connection with the target computer.
C. In Ad Hoc mode, an attacker sends each frame with the last bit set to zero, causing the target computer to disable encryption to increase throughput.
D. An attacker captures an encrypted frame, modifies the ciphertext, modifies the ICV to hide the change to the ciphertext, and then transmits the frame to appear as if it is from the original source.

Answer: D

QUESTION 103:

You are a wireless security professional at Certkiller .com. You are troubleshooting an 802.11g network performance problem using WLAN protocol analyzer software on your 802.11a/g enabled laptop computer. The network is protected with 802.1X/PEAP, and the client devices are authenticating properly. When you configure your laptop for PEAP and try to connect to the wireless network, you are unsuccessful. Which of the following is a statement that best explains why you cannot access the network from your laptop computer?

A. You needs a special security chip in your laptop to decode PEAP frames.
B. You must enter the proper PSK to decode PEAP frames.
C. Your wireless radio card does not support PEAP frame formatting.
D. The authentication server is currently offline.
E. The protocol analyzer's PC card drivers do not support the version of PEAP being used.

Answer: E

QUESTION 104:

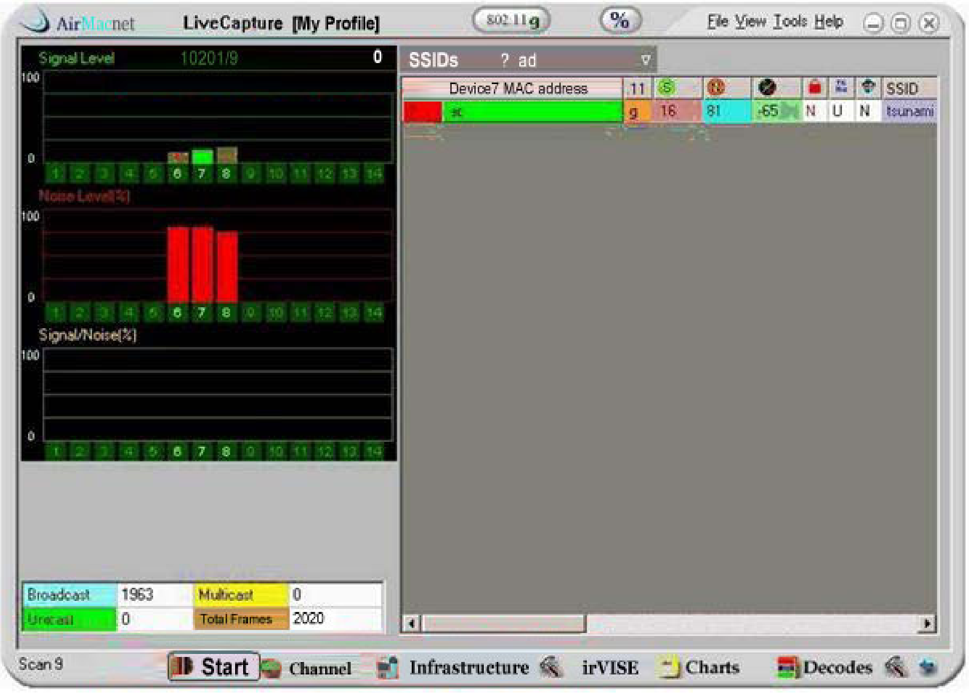
The 802.1X Uncontrolled Port serves which of the following purposes, according to the 802.11i amendment? (Choose all that apply)

A. To pass general data traffic after the completion of 802.11i AKM
B. To block authentication traffic until the 4-Way Handshake completes
C. To allow authentication PDUs to flow between the Supplicant and Authentication Server
D. To block unencrypted PDUs after a 4-Way Handshake completes

Answer: C

QUESTION 105:

Exhibit:



Device7 MAC address	11	Ⓢ	Ⓝ	●	🔒			SSID
🟥 :c	g	16	81	-65	N	U	N	tsunami

Broadcast	1963	Multicast	0
Unicast	0	Total Frames	2020

Of the following options, which one is a type of WLAN attack illustrated on the 802.11 protocol analyzer screenshot?

A. Hijacking
B. Man-in-the-middle
C. Frame injection
D. Authentication flood
E. RF jamming

Answer: E

QUESTION 106:

You are an administrator at Certkiller .com. Certkiller .com wants you to install an 802.11g WLAN that supports fast roaming for 802.11b IP phones. The ability to troubleshoot reassociations that are delayed or dropped during roaming is a requirement. Of the following, which is the most cost-effective system that you can apply to meet Certkiller .com's troubleshooting requirement?

A. Autonomous (thick) access points with a WIDS overlay system
B. Hybrid WLAN switch with integrated RF planning tool

C. WLAN switch with integrated WIPS
D. WLAN protocol analyzer software on laptop computers
E. WLAN switch with dual lightweight 802.11a/b/g radios

Answer: C

QUESTION 107:

Which two of the following protocols permit a network administrator to download log files from an access point securely? (Choose two)

A. SNMPv3
B. Telnet
C. SSH2
D. TFTP over SSH2
E. FTP over SSL

Answer: C,E

QUESTION 108:

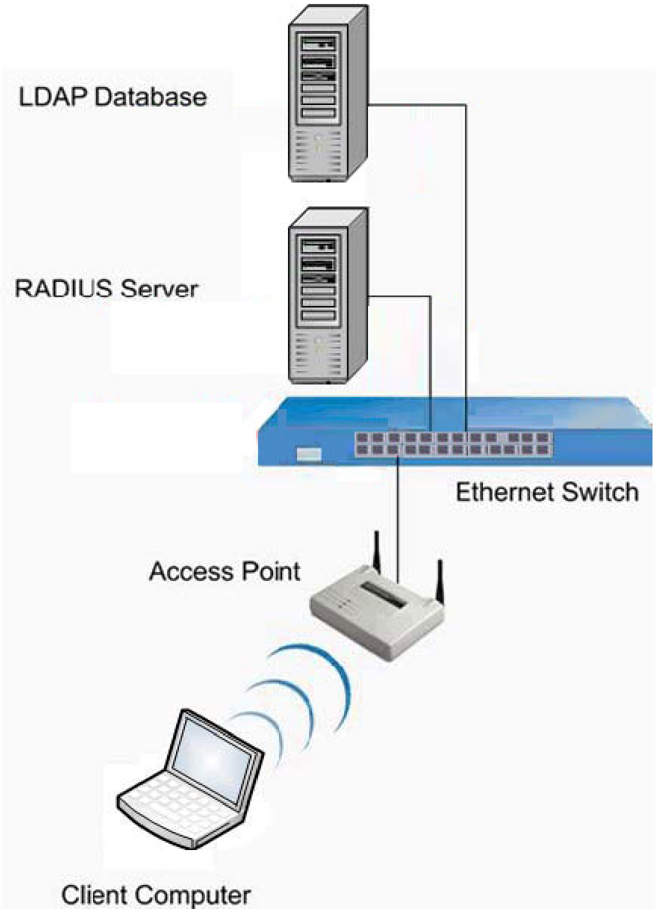
For which three purposes are 802.11a/g Wireless Intrusion Prevention Systems (WIPS) employed? (Choose three)

A. Security monitoring and notification
B. Enforcing wireless network policy
C. Detecting and defending against eavesdropping attacks
D. Preventing virtual carrier sense attacks by 802.11 transmitters
E. Performance monitoring and troubleshooting
F. Informing nearby access points of a failed access point

Answer: A,B,E

QUESTION 109:

Exhibit:



The exhibit depicts a network diagram that employs an 802.1X/EAP-based wireless security solution. Which device fulfills the EAP Authenticator functions?

A. Client computer
B. Ethernet switch
C. RADIUS server
D. Access point
E. LDAP database

Answer: D

QUESTION 110:

Certkiller .com is planning a security solution for their new wireless network. Some of Certkiller .com's client device applications employ Layer 3 protocols rather than IP. A consultant has suggested VPN technology as part of the wireless solution, but Certkiller .com does not know which VPN protocol should be used. Which of the following is the appropriate VPN protocol for Certkiller .com?

A. EAP-TTLS
B. IPSec

C. WPA
D. Kerberos
E. SSH2
F. PPTP

Answer: F

QUESTION 111:

For the prevention of which kind of WLAN attack does Transient Key IP employ a per-MPDU Transient Key IP
sequence counter (TSC)?

A. Forgery
B. Weak-IV
C. Session hijacking
D. Replay
E. Bit-flipping

Answer: D

QUESTION 112:

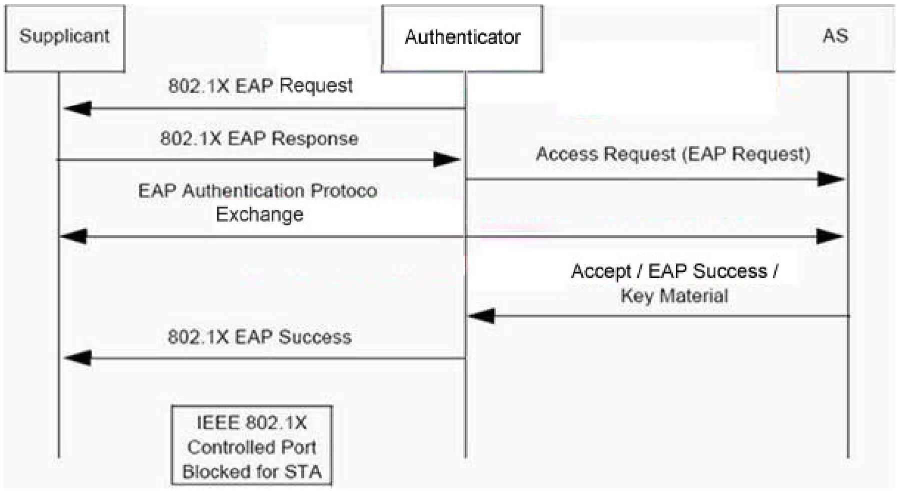
Utilizing clear text across the wireless medium during LEAP authentication, which of the following is the authentication credential passed?

A. PAC
B. Shared secret
C. Password
D. Username
E. x.509 certificate

Answer: D

QUESTION 113:

Exhibit:



The above exhibit illustrates The 802.1X/EAP framework that is described by the 802.11i amendment. Which of the following is the reason why the 802.1X Controlled Port is still blocked after the 802.1X/EAP framework has completed successfully?

A. The 802.1X Controlled Port remains blocked until a Layer 3 address is obtained by the Supplicant.
B. The 802.1X Controlled Port is always blocked, but theUncontrolled Port opens after the EAP authentication process completes.
C. The 802.1X Controlled Port is blocked until Vender Specific Attributes (VSAs) are exchanged inside a radius packet between the Authenticator and Authentication Server.
D. The 4-Way Handshake must be completed successfully before the 802.1X Controlled Port changes to the unblocked state.

Answer: D

QUESTION 114:

You are a network administrator at Certkiller .com. You often telecommute from a coffee shop, which has an 802.11g access point with a captive portal for authentication, near your home. To which three of the following types of WLAN attacks are you susceptible at this hotspot? (Choose three)

A. Wi-Fi publishing
B. UDP port redirection
C. 802.11 reverse ARP
D. Peer-to-peer
E. Happy AP
F. Eavesdropping/packet reassembly

Answer: A,D,F

QUESTION 115:

To physically locate rogue access points, which of the following parameters is required? (Choose all that apply)

A. IP Address
B. Beacons per second
C. Signal strength
D. BSSID
E. DSSS parameter set

Answer: C

QUESTION 116:

You are a network administrator at Certkiller .com. The size of Certkiller .com's WLAN is growing rapidly. Which two of the following tasks must be carried out to maintain consistent network security? (Choose two)

A. Configure APs to load their firmware from a TFTP server during initialization
B. Update the WLAN architecture to support autonomous APs managed by WNMS
C. Create and maintain a security checklist for equipment staging
D. Include the WLAN in a change management program
E. Use Role Based Access Control (RBAC) to assign security policies to users

Answer: C,D

QUESTION 117:

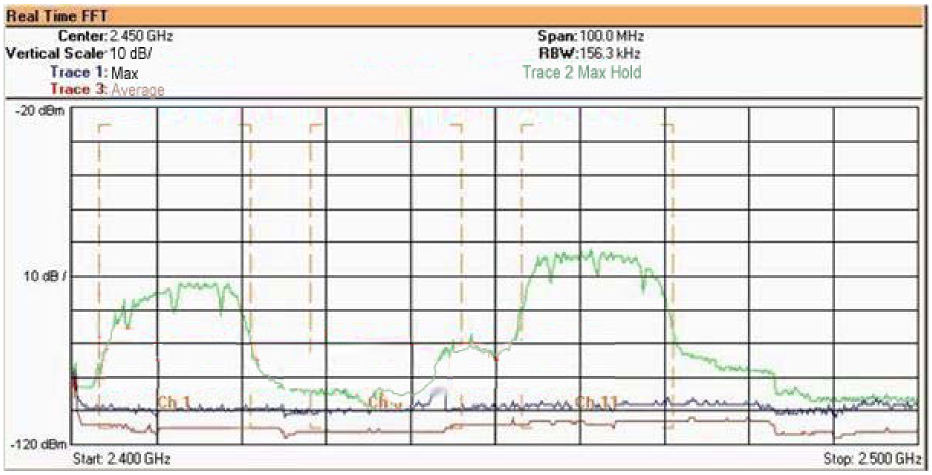
For the added security and scalability benefits, Certkiller .com is migrating from WPA-Personal to WPA2-Enterprise. The migration is gradual, so the least number of users are disrupted simultaneously. Of the following, which are two ACCURATE statements with regard to this migration? (Choose two)

A. Radio cards that do not support CCMP must be replaced.
B. The existing WPA-Personal compliant RADIUS server must be upgraded to support WPA2-Enterprise.
C. Because multiple cipher suites are in use, the WLAN will only be as secure as the weakest cipher suite.
D. Personal firewall software must be installed on each client device to protect against transitional man-in-the-middle attacks.
E. A new, longer passphrase must be given to each user migrating to WPA2-Enterprise.

Answer: A,C

QUESTION 118:

Exhibit:



Real Time FFT

Center: 2.450 GHz

Vertical Scale: 10 dB/

Trace 1: Max

Trace 3: Average

Span: 100.0 MHz

RBW: 156.3 kHz

Trace 2 Max Hold

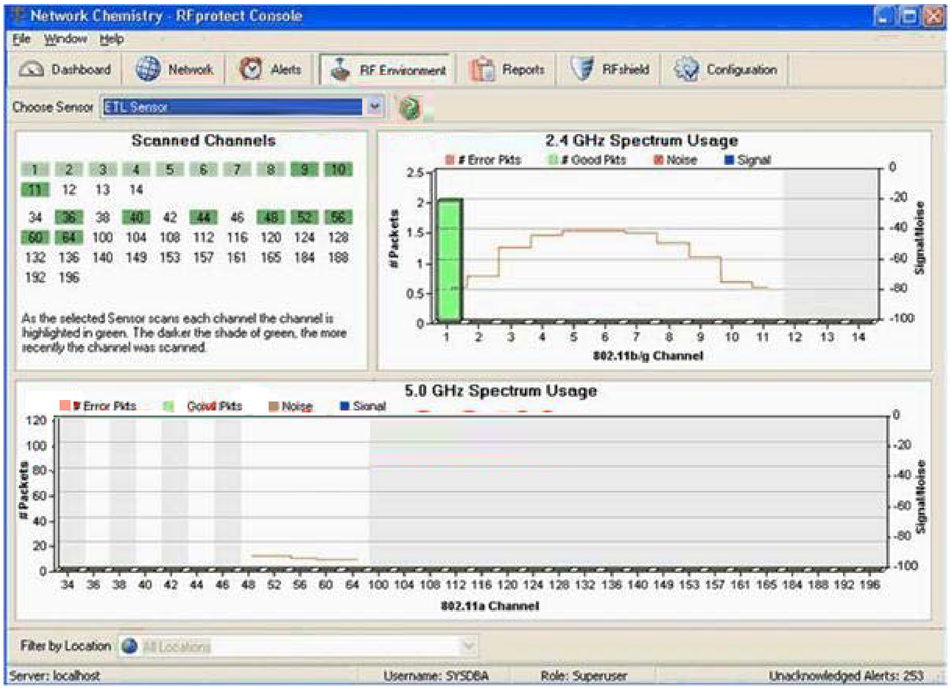
Which of the following does the RF spectrum analyzer illustrate? (Choose all that apply)

A. A narrowband RF attack is in progress on channel 11, and there is an 802.11b access point on channel 1.
B. Two FHSS systems have hopped onto channels 1 and 11 simultaneously.
C. There are 802.11g access points on channels 1 and 11 and both are operating normally.
D. There is an 802.11b radio performing a wideband DoS attack on channels 1 through 11.

Answer: C

QUESTION 119:

Exhibit:



Choose Sensor: ETL Sensor

As the selected Sensor scans each channel the channel is highlighted in green. The darker the shade of green, the more recently the channel was scanned.

Filter by Location: All Locations

Server: localhost Username: SYSDBA Role: Superuser Unacknowledged Alerts: 253

which of the following does the illustrated Wireless Intrusion Prevention System (WIPS) display? (Choose all that apply)

A. Wideband RF jamming attack
B. Only channels 9, 10, and 11 are enabled on the access point
C. Use of channels 12-14 is not allowed
D. An access point on channel 6
E. 802.11a access points on channels 34, 38, 42, and 46

Answer: A

QUESTION 120:

The similarity of an RF jamming attack and a wireless hijacking attack is specified by which of the following options (Choose all that apply)?

A. Both can be detected by wireless intrusion prevention systems.
B. Both can be deterred by appropriate client security solutions.
C. Both can be averted through the use of FHSS technology.
D. Both can be prevented through the use of 802.1X/EAP solutions.
E. Both can be blocked through the use of lockable enclosures for all access points.

Answer: A

QUESTION 121:

A hacker tries a brute force attack in an effort to compromise the passwords of a network. What does this attack entail?

A. A powerful RF signal is generated, forcing access.
B. A search is conducted using all known words.
C. A packet generator is used to overwhelm the access points.
D. A search is conducted using all possible combinations of numbers and letters.

Answer: D

QUESTION 122:

Which of the following is the principal target for a malicious hacker bent on financial gain?

A. Personal information
B. Identity theft
C. Credit card numbers
D. Corporate secrets

Answer: C

QUESTION 123:

Which of the following is the portion of an IDS, which acts almost like a traditional management system, analyzes gathered information, and monitors business rules for the wireless LAN?

A. Anomaly detection
B. Misuse detection
C. Vulnerability detection
D. Performance monitoring

Answer: B

Explanation:
The Misuse detection portion of an IDS acts almost like a traditional management system. In some cases, the IDS is even tied directly into a wireless management software package.

QUESTION 124:

Which of the following is a disadvantage of employing RBAC for Certkiller .com's wireless VPN?

A. Reduces unintentional denial of service occurrences.
B. Enables individualized account features.
C. Increases access of users to all network functions.
D. Reduces administrative overhead.

Answer: C

QUESTION 125:

Which of the following is a type of wireless LAN authentication protocol that has user-based authentication and accounting service, and uses either an internal or external database of users?

A. Kerberos
B. LDAP
C. Multi-factor Authentication
D. RADIUS

Answer: D

Explanation:
Remote Access Dial In User Service is an authentication and accounting service used by many enterprises and ISPs. RADIUS uses a NAS to pass usernames and passwords to the RADIUS server, and is configured with either an internal or external database of users.

QUESTION 126:

What is the focal point of a hijack that creates a denial of service in a wireless LAN?

A. Layer 3
B. Authorized Access Point
C. Layer 2
D. DHCP File Server

Answer: C

QUESTION 127:

Of the following options, which is NOT a VPN protocol type?

A. PPTP

B. L2TP
C. SSH2
D. PEAP

Answer: D

QUESTION 128:

Which VPN protocol is best described by the following statement?
A collection of IETF standards that include specifics on key management protocols as well as the encrypted packet formats/protocols?

A. IPSec
B. L2TP
C. PPTP
D. SSH2

Answer: A

Explanation:
IPSec/IKE actually refers to a collection of standards (RFC5 2401 to 241X) IPSec/IKE supports a wide variety of encryption algorithms as well as data integrity mechanisms.

QUESTION 129:

Which IEEE standard is an interim security solution that implements and standardizes Transient Key IP and 802.1x/EAP and is designed to run on existing hardware as a firmware patch?

A. 802.11f
B. 802.11i
C. 802.lx
D. WPA

Answer: D

Explanation:
There are several versions of WP
A. Having multiple and growing versions of WPA will undoubtedly cause some confusion among end-users and hardship on network administrators.

QUESTION 130:

Which of the following can be used to defend against an attack by Lucent Registry Crack (LRC) on the encrypted WEP key in the Windows registry?

A. Limit peer-to-peer file sharing.
B. Implement peer attack safeguards such as personal firewalls or IPSec policies.
C. Add Windows 2000 SysKey feature.
D. Upgrade Windows operating system service pack to NTLMv2.

Answer: B

Explanation:
Implement peer attack safeguards. In an attack using LRC, the hacker breaks into a remote registry connection using Window's Registry Editor on his own computer, finds the WEP key, and then copies it to LRC where it is decrypted. Service pack upgrades to NTLMv2 or the SysKey feature protect against password capture. File sharing has nothing to do with this type of attack.

QUESTION 131:

Which VPN protocol supports multiple encapsulated protocols, authentication and encryption, and employs a client/server architecture?

A. SSH2
B. IPSec
C. L2TP
D. PPTP

Answer: D

Explanation:
PPTP is based on the point-to-point protocol. PPTP enables users to access wireless networks securely and easily, and is natively supported by most Microsoft desktop and server operating systems.

QUESTION 132:

Unique and changing encryption keys are provided for by which of the following Layer 2 security solutions, so that an intruder will never be able to gather sufficient data to crack the keys?

A. 802.lx/EAP
B. Transient Key IP
C. Static WEP
D. Dynamic WEP

Answer: D

QUESTION 133:

Which of the following describes VPN's ability to assign guest user, authorized user, and other types of privileges based on a user's function.

A. Pre-shared keys
B. Initialization vectoring
C. Broadcast key rotation
D. Role based access control

Answer: D

QUESTION 134:

What does a hacker need to have if he wants to attack a network via network management tools like Hyena and LANBrowser?

A. Wireless Card.
B. Administrative Access.
C. Email Server
D. Application Layer Analyzer

Answer: B

QUESTION 135:

IPSec virtual private network technology operates at which layer of the OSI model?

A. Layer 3
B. Layer 7
C. Multilayer
D. Layer 2

Answer: A

Explanation:
IPSec operates at Layer 3. It has grown in popularity because of its strength in authentication and data privacy. It supports many encryption protocols such as DES, 3DES and AES.

QUESTION 136:

What would you NOT deem to be a security benefit of using a proprietary protocol?

A. Uses per packet authentication
B. Uses leading-edge encryption algorithms
C. Uses features not yet available on the market
D. Entire communication process strongly encrypted

Answer: C

QUESTION 137:

What three are properties of VPN connections? (Choose three)

A. User Authentication
B. Data Encryption
C. Layer 2 Switch Routers
D. Encapsulation

Answer: A, B, D

QUESTION 138:

Which term best describes the situation where a hacker intrudes on one network to send malicious data, such as SPAM or viruses, to another network?

A. Malicious data insertion
B. Hijacking
C. Illegal transmission
D. Third path attack

Answer: D

QUESTION 139:

Which of the following is raised proportionally, and in turn raises the time needed for a brute force attack to locate an encryption key exponentially?

A. variable rotation
B. key expansion
C. key length

D. number of rounds

Answer: D

QUESTION 140:

You are a network administrator at Certkiller .com. What is a major concern you should have about utilizing Transient Key IP during the interim stage of WPA, with some phases of IEEE 802.11i already in place?

A. Possibility of replay attacks
B. Possibility of weak-key attacks
C. Lost message integrity checks
D. Lack of interoperability between vendors

Answer: D

QUESTION 141:

You head a Certkiller .com network administration team that gets minimum, maximum, and average values from baseline data and utilizes it for setting alarms on Certkiller .com's IDS software. What kind of traffic baselining does this refer to?

A. Performance
B. Emergent
C. Security
D. Reference

Answer: C

Explanation:
After alarm values are developed with security baselining, when an intruder exceeds network normalcy levels, alarms are triggered and security administrators are notified.

QUESTION 142:

WLAN'S using 802.1x based security solutions has overwhelmingly adopted RADIUS as its preferred authentication process. Which of the following does not apply in this situation?

A. Hardware theft does not compromise security because user authorization is required
B. Authentication based on hardware
C. RADIUS already in heavy use in wired LAN's

D. Accounting and auditing are available, allowing usage auditing and intrusion alarms.

Answer: B

Explanation:
RADIUS authentication is NOT based on hardware, with reduces costs and administration overhead when upgrades occur or authentication data is changed.

QUESTION 143:

You are an administrator at Certkiller .com. Certkiller .com has not installed an intrusion detection system on their network. Of the following, which task will decrease the efficiency scanning of Certkiller .com's network for rogue devices manually?

A. Search in the 2.4-2.5 GHz band.
B. Search all physical locations of the company.
C. Use a wireless packet analyzer for the scan.
D. Use an up-to-date listing of the MAC addresses and SSIDs of all authorized devices.

Answer: A

QUESTION 144:

For which authentication type can any kind of supplicant credentials; mutual authentication and only server-side digital certificates be used?

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

Answer: A

QUESTION 145:

An access point is employing an EAP protocol. In response to an EAP request identity message, a client device sends an EAP response packet. What action does the AP take next?

A. AP sends an EAP-reject message to client
B. AP forwards EAP-response to authentication server
C. AP enables port to authorized state.
D. AP sends an EAP-success message to client

Answer: B

QUESTION 146:

Unique and changing encryption keys with a flexible authentication protocol included, as well as the addition of broadcast key rotation in some implementations is provided for by what Layer 2 security solution?

A. Dynamic WEP
B. Transient Key IP
C. Static WEP
D. 802.1x/EAP

Answer: D

QUESTION 147:

DHCP was prone to hijacking prior to the inclusion of authentication protocols. Normally an attack would commence by jamming a particular channel. The security hole was created by what system response?

A. Clients would be forced to roam, and then lease an IP address from a rogue DHCP server.
B. Clients would become saturated and would cease transmission of data.
C. Clients would be forced to roam, and would be unable to reconnect with the network.
D. Clients would be forced to roam, and then release their network IP addresses.

Answer: A

QUESTION 148:

Devices will be shipped with WPA security enabled by default, when WPA becomes a compulsory part of Wi-Fi certification testing. The user will have to carry out which task at that time?

A. Configure AP's for certification testing.
B. Configure AP's for AES-CCMP
C. Configure a master key or authentication server.
D. No action is required. Device is preconfigured.

Answer: C

QUESTION 149:

802.11 vendors use which method in an attempt to hide wireless LAN's from Netstumbler?

A. Use Broadcast SSID in the beacons.
B. Use MAC address in the beacons.
C. Use Reassociate Requests in the beacons.
D. Use Probe Response in the beacons.

Answer: A

QUESTION 150:

You are an engineer at Certkiller .com. While you are working on a Microsoft Excel spreadsheet at a thin client computer, somebody stumbles over the power cable and the machine shuts down. After the power has been restored and the thin client computer is restarted, how much data will have been lost?

A. None. The data is located on the thin client's host server.
B. All data. A thin client has no hard drive and can only make hard prints.
C. None. The thin client computer automatically saves data.
D. All data since the last save.

Answer: A

QUESTION 151:

Which of the following is SSH2 not capable of doing?

A. Provide secure command shell
B. Allow secure file transfer
C. Provide port forwarding
D. Allow encapsulating security payloads

Answer: D

Explanation:
ESP is a security protocol used to provide security in the IPSec protocol, which functions at Layer 3 of the OSI. SSH2 functions at Layer 4.

QUESTION 152:

Which statement pertaining to Authenticated Host Configuration Protocols is inaccurate?

A. Computers added to network without manually assigning an IP address
B. Software keeps track of IP addresses
C. Servers are able to authenticate clients.
D. Provide a framework for passing configuration information to hosts on a TCP/IP network.

Answer: C

Explanation:
Among the chief benefits of authenticated DHCP is that client and servers are able to authenticate each other. This limits rogues, unauthorized access and denial-of-service attacks.

QUESTION 153:

Capturing encrypted packets, changing some of the data within them, and then resending the packets is a partial description of which kind of attack against WEP?

A. Weak-key
B. Forgery
C. Collision
D. Replay

Answer: B

QUESTION 154:

Which of the following is a security risk you CANNOT detect with a wireless packet analyzer?

A. missing security patches.
B. exposed Network Layer information
C. oversized RF cells
D. unencrypted wireless traffic

Answer: A

QUESTION 155:

Which sub-routine is NOT executed during an RC5 encryption routine?

A. bitwise XOR
B. integer addition
C. key expansion
D. variable rotation

Answer: C

Explanation:
Encryption using the keystream is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.

QUESTION 156:

Which of the following is a type of segmentation device that supports RADIUS or ACS authentication, does NOT do routing, and is a Layer 2 encryption device that may also perform Layer 4 port filtering?

A. Router
B. VPN Concentrator
C. Firewall
D. Enterprise Encryption Gateway

Answer: D

Explanation:
EEG is a newcomer to WLAN security, and is unlike any other device on the market. EEGs serve as gateways because they segment wireless networks from a network's backbone.

QUESTION 157:

With reference to the use of Pre-Shared Keys in VPNs, which of the following is false?

A. Can configure multiple pre-shared keys for all L2TP/IPSec connections
B. if pre-shared key on VPN server is changed, a client using a pre-shared key will be unable to connect.
C. Do not require investment in a PKI
D. Can be either typed or pasted into the IPSec VPN configuration utility

Answer: A

QUESTION 158:

Which statement pertaining to the Transport and Tunnel modes of IPSec is accurate?

A. Both modes encrypt both the header and payload.
B. Tunnel mode encrypts only the payload (data).
C. Transport mode encrypts only the payload (data).
D. Transport mode encrypts both the header and payload.

Answer: C

QUESTION 159:

The provisions for access, use, disclosure, interception, and privacy protections of electronic communications are set out by which Act?

A. 1998 Identity Theft and Assumption Deterrence Act
B. 1986 Computer Fraud and Abuse Act
C. 1986 Electronic Communications Privacy Act.
D. 2003U.S.
A. Patriot Act

Answer: C

QUESTION 160:

Which of the following device types can be deployed on an enterprise class access point to alert system management in the event of a packet flooding type of denial of service attack?

A. SNMP trap
B. Signal generator
C. RF antenna
D. Auto dialer

Answer: A

QUESTION 161:

Which of the following is a method an intruder would use to compel local client devices to roam, or to introduce interference to examine stability?

A. RF Jamming
B. Port Scanning
C. Operating System Fingerprinting
D. War walking

Answer: A

QUESTION 162:

Which of the following authenticates each other in an EAP solution that employs mutual authentication?

A. Client and switch filter
B. Client and access point
C. Access point and authentication server
D. Client and authentication server

Answer: D

Explanation:
When mutual authentication is employed, the client device and the authentication server exchange identification information and authorization prior to commencing normal data transmission.

QUESTION 163:

Which task will NOT assist customer support centers to prevent social engineering?

A. End-user verifies support center identity before giving password information.
B. Positively identify person calling help desk.
C. Shred documents prior to throwing them away.
D. Use established, secure channels for passing security information.

Answer: A

QUESTION 164:

Which is an accurate statement when comparing the authentication processes of PPTP and L2TP?

A. PPTP requires two levels of authentication; L2TP requires only one
B. PPTP authentication process is encrypted, where L2TP is not.
C. L2TP requires two levels of authentication; PPTP requires only one

D. Their authentication processes are virtually the same.

Answer: C

QUESTION 165:

Which of the following best describes the term SPAM?

A. Uploading pornographic material to a company website
B. Sending worm viruses via email
C. Sending trojan horse email viruses
D. Sending unsolicited bulk email.

Answer: D

QUESTION 166:

What is not a benefit of 802.1x?

A. Device-based identification
B. Dynamic key management
C. Maturity and interoperability
D. Flexible authentication

Answer: A

Explanation:
With 802.1x/EAP-based wireless security solutions, identification is no longer based on a particular wireless device connecting to the network, but rather on the actual user.

QUESTION 167:

Which three of the following statements are true regarding the use of switches to connect to the wired segment of a network?

A. Create full duplex connectivity at the bridge
B. Broadcast each frame entering any port to every other port
C. Create full duplex connectivity at the access point
D. Allows support for security and network management tools like VLANs.

Answer: B

QUESTION 168:

Which of the following is an advantage that Windows 2000 service pack 3 (SysKey) provides for network security?

A. Prevents password capture by LOphtCrack.
B. Offers better virus protection.
C. Prevents peer file sharing.
D. Prevents decryption of the WEP key.

Answer: A

QUESTION 169:

You are a network administrator at Certkiller .com. You install a new segment of a wireless LAN, and then monitor its performance over the next several days by gathering data on all aspects of its operation. Which type of traffic baselining are you using?

A. Reference
B. Performance
C. Emergent
D. Security

Answer: A

Explanation:
When a new installation is complete, reference baselining provides a standard that represents network normalcy. This can be defined as traffic quantities and types that are found on the network over a period of time, and at particular times of the day or week.

QUESTION 170:

Which of the following is an encryption scheme that is a symmetric-key algorithm used to protect sensitive Federal information, and is also a CPU intensive algorithm that entails co-processing in wireless systems?

A. RC5
B. RC4
C. AES
D. DES/3DES

Answer: C

QUESTION 171:

Which EAP authentication type is characterized by the creation of an encrypted tunnel between the supplicant and the authentication server?

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

Answer: B

QUESTION 172:

Outdoor bridge link security will improve by executing which three of the following actions? (Choose three)

A. Enable client connectivity at the bridge
B. Utilize strong encryption and authentication
C. Use 802.1x/EAP authentication.
D. Change the bridge default settings

Answer: B,C,D

QUESTION 173:

Which of the following is a reason why an intruder would opt for a 900 MHz unit instead of 2.4 0Hz or 5.0Hz when placing a rogue device onto a wireless network?

A. Less expensive to deploy.
B. Causes maximum disruption to the system.
C. Prevents discovery of device.
D. Offers less interference for transmission of data.

Answer: C

QUESTION 174:

Which three of the following are forms of social engineering? (Choose three)

A. Calling the help desk and asking for secure information.
B. Using a directional antenna and NetStumbler to obtain LAN information.

C. Sending fake instant messages asking for information from authorized sources.
D. Searching through a company's trash to find a phone list and org chart.

Answer: A,C,D

QUESTION 175:

What type of VPN connection is being employed when you use a wireless VPN client device to 'dial' into a VPN server, which is wired into a network?

A. Remote access
B. Peer-to-peer
C. Enterprise wireless gateway
D. Network

Answer: A

Explanation:
Remote access is a point-to-point connection made between VPN clients and a VPN server (also called an enterprise wireless gateway) to gain access to a network. Some connections can have mutual authentication, though most feature only client authentication.

QUESTION 176:

The security of packets en route to their destination is guaranteed using which of the following?

A. Authentication Server
B. Authenticator
C. Message Integrity Check
D. Initialization Vector

Answer: C

QUESTION 177:

Which of the following is an issue that must NOT deal with Certkiller .com's wireless security plan?

A. Intrusion
B. Privacy
C. Resources

D. Capacity

Answer: D

QUESTION 178:

What has been estimated as the shortest time a hacker needs to crack WEP?

A. Several days.
B. Three to four hours
C. Within an hour
D. Almost immediately.

Answer: B

QUESTION 179:

Which of the following describes a virtual server that a hacker may set up in a reconfiguration attack of a wireless network?

A. A software application that enables Telnet.
B. Network management utilities like Solarwinds and SNMPc.
C. Redirected port mappings that allow internal hosting of services.
D. A type of rogue device.

Answer: C

Explanation:
Virtual servers are redirected port mappings that allow internal hosting of services behind a Port Address Translation router such as a SOHO gateway. The virtual server allows the hacker to come back into the network via an Internet connection, and may be used to enable services such as SNMP or Telnet. A virtual server is neither a device nor a software application.

QUESTION 180:

Which type of segmentation device is utilized to filter between networks and can be designed as all-purpose, or for specific filtering functions?

A. Enterprise Encryption Gateway
B. VPN Concentrator
C. Router
D. Firewall

Answer: D

QUESTION 181:

Network segments are monitored by which portion of an IDS, which also compares their current status to the normal baseline?

A. Performance monitoring
B. Misuse detection
C. Anomaly detection
D. Vulnerability detection

Answer: C

Explanation:
The anomaly detector portion of an IDS monitors network segments and compares their current status to the normal baseline and looks for anomalies. Baselines can, and should, be established for typical network load, protocols and packet size.

QUESTION 182:

Which is the preferred mode of encryption for use in IEEE 802.11i?

A. AES-CCMP
B. RC6
C. 3DES
D. PSK

Answer: A

QUESTION 183:

An intruder employs what kind of information gathering to calculate the usage levels of parts of a LAN, peak activity periods, and where on the network data is headed?

A. Trace Routing
B. Traffic Pattern Analysis
C. Target Profiling
D. LAN Mapping

Answer: B

QUESTION 184:

Which of the following best describes the reason for eliminating availability of certain services from a wireless segment of a network?

A. Creates more bandwidth for file sharing
B. Reduces security risk to the entire network
C. Speeds email communications
D. Forces end-users to comply with security program

Answer: B

QUESTION 185:

Enforcing end-user compliance with corporate wireless security policy, is least successful using which one of the following the methods?

A. Financial incentives
B. Small group accountability
C. Periodic spot checks
D. Restricting network use

Answer: D

QUESTION 186:

Which three statements about WPA Pre-shared Keys are true? (Choose three)

A. Passwords referred to as Master Keys.
B. Following password entry, Transient Key IP is manually initiated.
C. Allows use of manually entered keys or passwords.
D. Designed to be easy for home-user to configure

Answer: A,C,D

QUESTION 187:

Which of the following does NOT form part of the Kerberos system?

A. Client and server software applications
B. Security Policies
C. Internal database of users

D. Key Distribution Center

Answer: C

QUESTION 188:

Which of the following is a type of segmentation device that is described as intelligent, but slow, and uses security that is comparable to a strong set of access control lists?

A. Layer 3 switch
B. VPN Concentrator
C. Router
D. Firewall

Answer: C

QUESTION 189:

One of the most secure schemes employed to authenticate secure shell, is Public Key Authentication. What range of bit lengths does each key have?

A. 64 to 128 bits
B. 128 to 256 bits
C. 512 to 1024 bits
D. 1024 to 2048 bits

Answer: D

QUESTION 190:

When applying a wireless security policy, which of the following is the most significant success factor?

A. Accurate assessments.
B. Executive sponsorship.
C. End-user buy in.
D. Technical thoroughness.

Answer: B

QUESTION 191:

Which type of segmentation device offers strong authentication via RADIUS or TACACS+, builds encrypted port between client and network, and has a high overhead?

A. Layer 3 Switch
B. VPN Concentrator
C. Enterprise Encryption Gateway
D. Firewall

Answer: B

Explanation:
VPN Concentrators support RADIUS or TACAS+ authentication, multiple types of VPN technologies and protocols, and can scale form supporting only a few users to many thousands. The strong authentication and encryption they provide comes with a high cost, high overhead, and reduced throughput.

QUESTION 192:

Which term best describes the method a hacker could use to locate open wireless LANs?

A. War Driving
B. Search Engines
C. War Chalking
D. Trace Routing

Answer: A

QUESTION 193:

What encryption scheme, which is extensively employed by the financial services industry, is both a block cipher and a product cipher?

A. RC4
B. AES
C. DES/3DES
D. RC2

Answer: C

Explanation:
Developed by IBM for the NIST, DES was intended to be used as a strong cryptographic algorithm to protect non-classified information, but a series of demonstrated cracks of the encryption scheme pushed the development of 3DES.

QUESTION 194:

Consider the following statement:
An open standard that is guided by the IETF, it provides a cryptographically secure TCP/IP tunnel between two computers with authentication, encryption occurs at the transport layer?
Which VPN protocol does this describe best?

A. PPTP
B. L2TP
C. SSH2
D. IPSec

Answer: C

Explanation:
SSH2 is a protocol implemented in an application that provides a secure tunnel between two authenticated computers. Encryption occurs at a special SSH transport layer, and authentication is implemented within the application, it is based on a client/server model.

QUESTION 195:

How is Encapsulating Security Payload, which is a security protocol used IPSec, accomplished?

A. A keyed one-way hash function is applied to the datagram to create a message digest.
B. Performing encryption at the IP layer.
C. A shared code is mutually transmitted between stations.
D. An encrypted authentication code is transmitted as a message digest.

Answer: B

Explanation:
ESP provides confidentiality by performing encryption at the IP layer. It supports a variety of symmetric encryption algorithms, the default being 56-bit DES. This cipher must be implemented to guarantee interoperability among IPSec products.

QUESTION 196:

Enterprise Wireless Gateways has what major security weakness?

A. Do not support RADIUS authentication.
B. Lack of encryption on some Layers

C. Do not support IPSec protocol.
D. Lack of protection for access points

Answer: D

QUESTION 197:

You are a network administrator at Certkiller .com. Certkiller .com's network is configured with an EWG performing NAPT with a RADIUS server carrying out port-based access control. In order to effectively manage this arrangement, which additional configuration step do you not need to take?

A. Configure access points with gateway addresses
B. Configure EWG to do 1:1 static NAT mappings
C. During RADIUS server configuration, give each NAS entry an IP address
D. Enable port mapping to manage access points.

Answer:

Explanation:
Pending. Send your suggestion to feedback@ Certkiller .com
If port mapping is used without additional configurations, only one access point can be managed, which is not feasible. Setting up EWG to do 1:1 static NAT mappings, in which the EWG assigns backbone IP addresses on behalf of the access points allows the network administrator to see the ports.

QUESTION 198:

Which EAP authentication type is based on Secure Socket Layer protocol, and applies both server and client-side certificates?

A. LEAP
B. EAP-TTLS
C. EAP-MD5
D. EAP-TLS

Answer: D

QUESTION 199:

What term best describes the communications standards utilized to build and manage VPN connections, and to encapsulate private data?

A. Tunneling Protocols
B. Certificates
C. Passwords
D. Pre-shared Keys

Answer: A

QUESTION 200:

Which type of segmentation device is extremely fast and rather expensive, uses ACLS for security using fast, has distributed CPUs, and does not supply any mode of authentication?

A. Enterprise Encryption Gateway
B. Layer 3 Switch
C. Firewall
D. VPN Concentrator

Answer: B

Explanation:
Layer 3 switches have many names: route switches, switch routers, Layer 3 switches, network layer switches, and many others. They are simply routers that have an additional switching functionality.

QUESTION 201:

Which of the following is a false statement with regards to a typical Kerberos implementation?

A. Clear text password entry and transmission
B. Dynamic encryption key distribution
C. New keys generated at start of every session
D. Mutual authentication

Answer: A

QUESTION 202:

You are a network administrator at Certkiller .com. A network-based IDS that you have configured in the passive mode, detects a rogue device located downstream of an AP. How does the IDS respond in this event?

A. Initiates an alarm and prompts a 'deny' probe response from the AP.
B. Initiates an alarm and disconnects the AP from the network.
C. Initiates an alarm and sends transmission to RADIUS server to deny access.
D. Initiates a network intrusion alarm and prints an alarm log.

Answer: D

QUESTION 203:

Which option best describes a self-replicating, self-proliferating virus that is often delivered via email?

A. Worm
B. Spyware
C. Trojan Horse
D. Rogue

Answer: A

QUESTION 204:

What is a system that checks inbound and outbound traffic and attempts to identify suspicious activity known as?

A. Authentication Server
B. Intrusion Detection System
C. Firewall
D. VPN Concentrator

Answer: B

QUESTION 205:

What advantage does allowing an outside consultant to perform a security audit of a network have?

A. Creates easy target to assign blame to
B. Saves money
C. Provides fresh perspective on potential risks
D. Reduces impact on staff

Answer: C

QUESTION 206:

What is the sequence of bits utilized as a key in a stream cipher known as?

A. self-synchronous
B. keystream
C. symmetric algorithm
D. bitwise XOR

Answer: B

Explanation:
Encryption using the keystream is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.

QUESTION 207:

Directly after intruding into a system, what term is given to the actions a hacker takes to open up more security holes in the system?

A. Spy lining
B. Unauthorized access
C. Hijacking
D. Opening the front door.

Answer: D

QUESTION 208:

Which type of encryption is described as a variable length stream cipher that is used by WEP, Transient Key IP, MPPE, SSL as well as TLS security protocols, and is thought to be moderately secure?

A. RC4
B. DES/3DES
C. AES
D. RC5

Answer: A

Explanation:
RC4 is the most commonly used stream cipher today. It is a typed of symmetric encryption algorithm and is much faster than any block cipher.

QUESTION 209:

By which of the following tasks will password "strength" NOT be improved?

A. Change passwords monthly
B. Make passwords at least 8 characters in length
C. Reuse passwords.
D. Use mixed case, punctuation and numerals in passwords

Answer: C

QUESTION 210:

In which way does installing software that creates fake access points help to reduce the efficiency of discovery tools like Netstumbler and Kismet?

A. Fools the programs into believing there are hundreds of access points on the network.
B. Overloads the discovery program with data.
C. Forces the programs to channel hop.
D. Jams data transmission with multiple probe response frames.

Answer: A

QUESTION 211:

Which Layer 2 security solution offers unique and changing encryption keys to prevent a hacker from ever being able to amass adequate data to crack the keys?

A. Static WEP
B. 802.1x/EAP
C. Dynamic WEP
D. Transient Key IP

Answer: C

QUESTION 212:

Which of the following is the recommended data integrity mechanism for IPSec?

A. DES
B. SHA-1

C. RC4
D. MD5

Answer: B

QUESTION 213:

A wireless LAN security policy should be employed by which kind of organization?

A. All organizations with any type of computer network
B. Organizations with only a wireless LAN
C. Organizations with critical data on their wireless LAN.
D. Organizations considering deploying a wireless LAN.

Answer: A

QUESTION 214:

For the purpose of improving the security of Certkiller .com's wireless network, Certkiller .com procures enterprise class access points that support leading edge technologies. How will the cost of Certkiller .com's access points generally be affected?

A. Slightly lowered cost
B. Essentially the same.
C. Raises cost by about 500%
D. Raises cost by about 200%

Answer: D

QUESTION 215:

Which of the following is a VPN protocol that combines Cisco's Layer 2 Forwarding Protocol and Microsoft's point-to-point tunneling protocol, but does NOT define any encryption standard?

A. PPTP
B. L2TP
C. SSH2
D. IPSec

Answer: B

QUESTION 216:

What term, pertaining to RADIUS, refers to the design capability that allows multiple servers to run as a single computer, where each shares in the workload of the application?

A. Distributed
B. Scalability
C. Failover
D. Clustering

Answer: D

QUESTION 217:

An authentication framework for 802-based LANs is provided by which IEEE standard.

A. 802.lx
B. 802.11i
C. 802.11f
D. 802.11b

Answer: A

QUESTION 218:

You create three wired and wireless VLANs in an enterprise environment, and then separate them into full-time employee, part-time employee, and guest access sectors. What type of deployment strategy would this be an example of?

A. Enterprise wireless gateway
B. Segmentation by user group
C. Enterprise encryption gateway
D. Segmentation by device type

Answer: B

Explanation:
Segmentation by user group allows the network administrator to establish separate policies and protocols for each group, which can enhance overall network security.

QUESTION 219:

With SSIDs, which of the following is NOT a good baseline security action to take?

A. Keep SSID code settings confidential.
B. Change the default SSID setting to something cryptic
C. Change the SSID setting to closed system
D. Change the SSID setting to the department name

Answer: D

QUESTION 220:

What actions is taken by an access point that utilizes an EAP protocol after an authentication server sends the it an 'accept' message?

A. Waits for further requests from client.
B. Sends client EAP-success message and waits for instructions from the authentication server.
C. Sends client EAP-success message and transitions the port to authorize.
D. Sends client EAP-success message and waits for further requests from client.

Answer: C

Explanation:
As soon as the AP receives the accept message from the authentication server, it sends an EAP-accept message and transitions the port to an authorized state, allowing the client to begin forwarding traffic to the network.

QUESTION 221:

Which of the following is an IEEE standard that attends to wireless LAN security, and specifies the use of Transient Key IP and 802.1x/EAP with mutual authentication as likely security solutions?

A. 802.1x
B. WPA
C. 802.11i
D. 802.11f

Answer: C

Explanation:
Multiple methods of using AES are also specified as part of 802.11i. Any wireless LAN equipment complying with this standard will likely require a hardware upgrade due to the cryptographic overhead inherent with AES.

QUESTION 222:

What encryption scheme, which is extremely efficient on processors such as Intel's Pentium series, is the most recognized block cipher?

A. DES/3DES
B. RC5
C. AES
D. RC4

Answer: B

QUESTION 223:

To recognize faults in wireless networks prior to the networks becoming exposed to a malevolent threat, which class of general policy is designed?

A. Impact analysis
B. Threat prevention
C. Security auditing
D. Risk assessment

Answer: C

QUESTION 224:

What is the first action the access point takes using an EAP protocol when a client device sends it an EAP-start message?

A. AP sends identity request to client.
B. AP detects client.
C. AP enables port to unauthorized state.
D. AP enables port to authorized state.

Answer: B

QUESTION 225:

Which of the following is the general term that means "any transfers of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or part by wire, radio, EM, photo electronic or photo optical system...", in U.S. code?

A. electronic communications
B. wireless transmission
C. world wide web
D. internet

Answer: A

QUESTION 226:

On the subject of redundancy, which of the following is a network design fault?

A. AP's installed with hot/cold failover switches
B. AP co-location used
C. All AP's on same VLAN behind a router
D. Multiple frequency bands are used

Answer: C

QUESTION 227:

One-way authentication, password-based protocol, and does NOT use WEP keys are characteristics of which type of EAP authentication?

A. EAP-TLS
B. EAP-TTLS
C. EAP-MD5
D. LEAP

Answer: C