CWNA

Exam PW0-204

Certified Wireless Security Professional (CWSP)

Version: 7.1

[Total Questions: 181]

Topic 1, Main Exam

Question No : 1 - (Topic 1)

In an effort to optimize WLAN performance ABC Company has already upgraded their infrastructure from 802 11b/gto802 11n. ABC has always been highly security conscious but they are concerned with security threats introduced by incompatibilities between 802.11n and 802.11a/g in the past.ABC has performed manual and automated scans with products that were originally designed for use in 802 11a/g networks.Including laptop-based spectrum and protocol analyzers as well as an overlay 802 11a/g WIPS solution.ABC has sought your input to understand and respond to potential security threats.

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

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

Answer: A,B,C

Explanation:

HT Greenfield The Greenfield PHY header is not backward compatible with legacy 802.11a/g radios and can only be interpreted by 802.11n HT radios

0470438916.pdf,Page 410

Laptop Analyzer automatically identifies hundreds of performance problems, such as 11b/g conflicts, 802.11e problems, and QoS, as well as dozens of wireless intrusions and hacking strategies, including Rogue devices. With the Laptop Analyzer, users can classify and decode Non-HT (legacy), HT mixed format and HT greenfield format traffic and identify backward compatibility issues with legacy 802.11a/b/g devices operating in the same environment.

http://www.njbo.net/tools/Laptop%20Analyzer%20-%20WLAN%20Monitoring%20and%20Troubleshooting%20Tool%20-%20AirMagnet.htm

The HT Greenfi eld PHY header cannot be detected by a WIPS that is using legacy 802.11a/g sensors. The solution to this problem is to upgrade the WIPS with new

sensors that also have 802.11n HT radios. (**the company has already upgraded to 802.11n so C is correct**)

0470438916.pdf,Page 411

Question No : 2 - (Topic 1)

Given:A new Access point is connected to an authorized network segment and is detected wirelessly by a WIPS.

By what method does the WIPS apply a security classification to newly discovered AP?

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

Answer: B

Explanation: http://webcache.googleusercontent.com/search?q=cache:E-xehyw9ijwJ:www.nhbook.com/exam/PW0-200.pdf+A+new+Access+point+is+connected+to+an+authorized+network+segment+and+is+detected+wirelessly+by+a+WIPS.+WIPS+uses+location+service+profile&cd=9&hl=en&ct=clnk&gl=in&source=www.google.co.in

Question No : 3 - (Topic 1)

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

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

E. Social engineering recognition and mitigation technique.

Answer: D,E

Explanation:

A proper password security policy for wireless access should be ensured, and the baseline for secure password and secret key selection should be enforced.

As part of a more general corporate security policy, users should be informed about social engineering attacks and not disclosing information about the network to potential attackers.

http://e-articles.info/e/a/title/Wireless-Security-Policy/

Question No : 4 - (Topic 1)

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

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

Answer: D

Explanation: http://dnscoinc.com/bradfordidentity.pdf

Question No : 5 - (Topic 1)

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

- Encrypted GTK sent
- Confirmation of temporal key installation

- Announce sent from authenticator to supplicant, unprotected by MIC
- Snonce sent from applicant to authenticator, protected by MIC.

Arrange the frames in the correct sequence beginning with the start of the 4-way handshake

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

Answer: A

Explanation: 0470438916.pdf,Page199

Question No : 6 - (Topic 1)

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

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

Answer: F

Explanation: The only way to prevent a wireless hijacking, man-in-the-middle, and/or Wi-Fi phishing attack is to use a mutual authentication solution.802.1X/EAP authentication solutions require that mutual authentication
credentials be exchanged before a user can be authorized.

Page 319

Question No : 7 - (Topic 1)

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

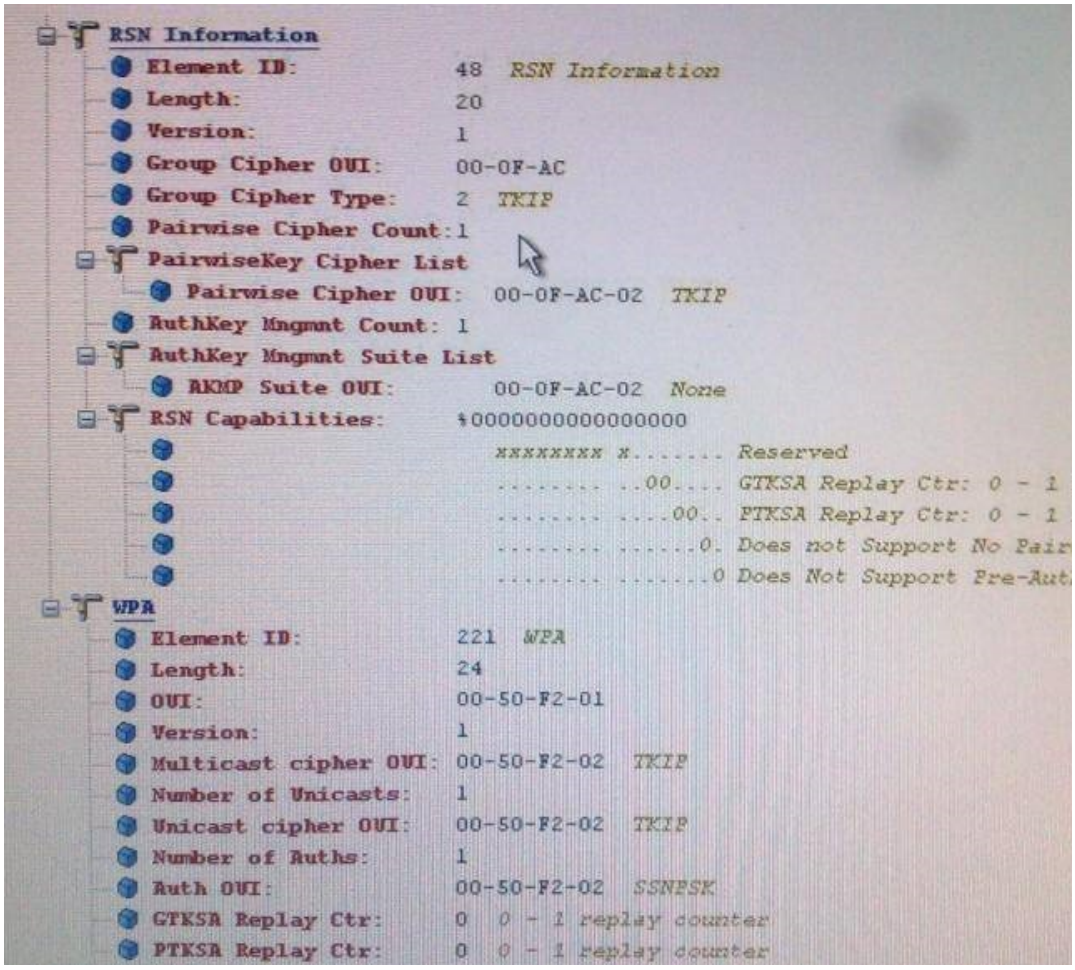
A. EAP-TLS requires a PKI to create X509 certificates for both the server and client, which increases administrative overhead.
B. EAP-TLS does not use SSL to establish a secure tunnel for internal EAP authentication.
C. Fast/secure roaming in an 802 11 RSN is significantly longer when EAP-TLS is use.
D. EAP-TLS does not protect the client's username and password in side an encrypted tunnel.
E. Though more secure EAP-TLS is not widely supported by wireless infrastructure or client vendors.
F. Initially mobility authentication with EAP-TLS is significantly longer due to X509 certificate verification.

Answer: A

Explanation: EAP - TLS requires the use of client - side certifi cates in addition to a server certifi cate.The biggest factor when deciding to implement EAP - TLS is whether an enterprise PKI infrastructure is already in place. This would usually, and optimally, include separate
servers in a high - availability server cluster.
0470438916.pdf
Page 151

Question No : 8 - (Topic 1)

Exhibit



Given:The illustration shows a WLAN protocol analyzer decoding an 802.11 beacon frame.

What statement about the access points BSSistrue and can be confirmed with this illustration?

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

Answer: E

Explanation: Page 186-187
-0470438916.pdf

Question No : 9 - (Topic 1)

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

In this configuration the wireless network is initially susceptible to what type of attacks?

(Choose 2)

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

Answer: B,E

Explanation: LEAP was developed by Cisco in 2001 as an improved version of Extensible Authentication Protocol-MD5 was and it was released as an IEEE 802.1X Extensible Authentication Protocol (EAP) authentication type

LEAP transmits Challenge-Handshake Authentication Protocol (CHAP) negotiations in the open without the benefit of an encrypted tunnel. Thus, LEAP is prone to offline dictionary and brute force attacks

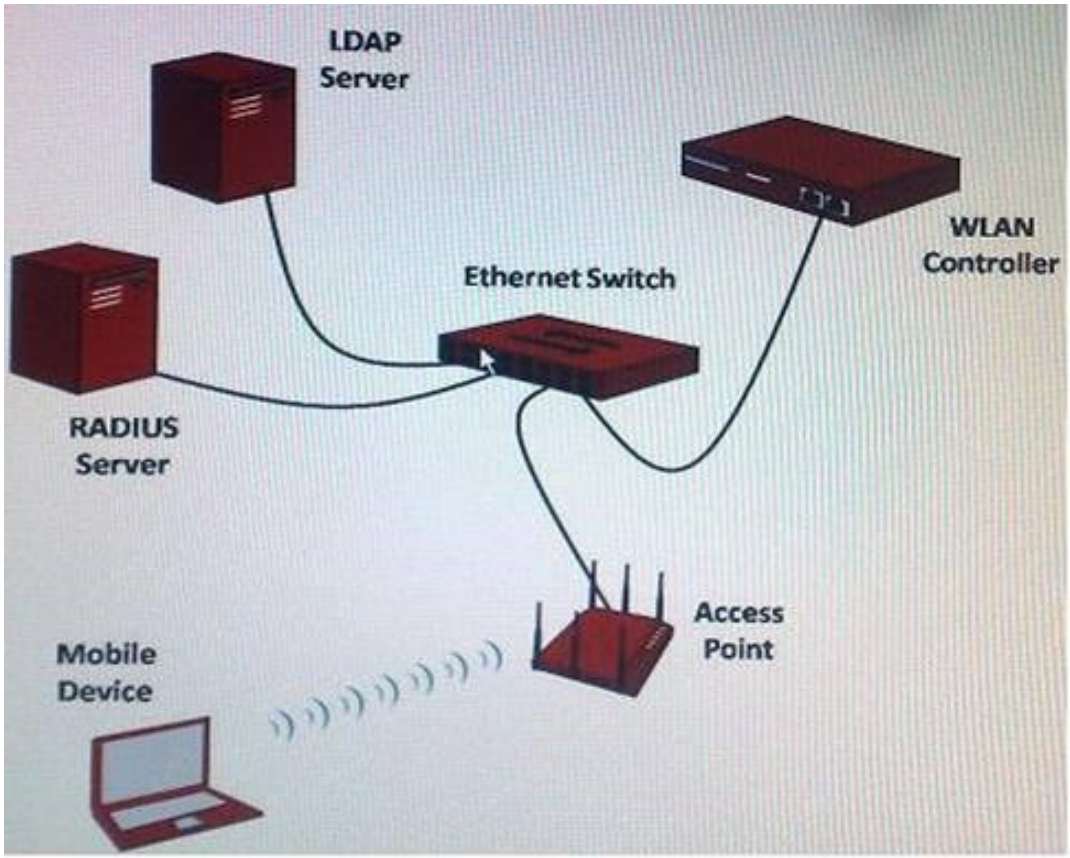
http://www.infinitel00p.com/library/wifisecHTML/WiFi.Security.htm

The systems protected by LEAP are still vulnerable to MITM attacks

http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack

Question No : 10 - (Topic 1)

Exhibit



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

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

Answer: E

Explanation: supplicant is often the laptop or wireless handheld device trying to access the network

A device that blocks or allows traffi c to pass through its port entity. Authentication traffi c is normally allowed to pass through the authenticator, while all othertraffi c is blocked until the identity of the supplicant has been verifi ed. The authenticatormaintains two virtual ports: an*uncontrolled port*and a*controlled port*. The uncontrolledport allows EAP authentication traffi c to pass through, while the controlled port blocks allother traffi c until the supplicant has been authenticated. In a WLAN, the authenticator isusually either an AP or a WLAN controller.

Theauthenticator plays the role of the intermediary, passing messages between the supplicantand the authentication server.

In the centralized WLAN
architecture, autonomous APs have been replaced with controller - based access points alsoknown as thin APs. A*controller - based AP*has minimal intelligence, and functionally is justa radio card and an antenna. All the intelligence resides in a centralized*WLAN controller*,and all the AP confi guration settings, such as channel and power, are distributed to thecontroller - based APs from the WLAN controller and stored in the RAM of the controller -
based AP.

In this fig WLAN Controller is used with thin AP therefore the authenticator is WLAN Controller

0470438916.pdf
Page 110- 116
Page 460

Question No : 11 - (Topic 1)

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

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

Answer: A

Explanation:
EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extendsTLS. It is widely supported across platforms; although there is no native OS support for this EAP protocol in Microsoft Windows, it requires the installation of small extra programs such as SecureW2. EAP-TTLS offers very good security. The client can but does not have to be