考試編碼:PW0-204

考試名稱:Certified Wireless Security Professional (CWSP)

版本: Demo

QUESTION NO: 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 GreenfieldThe 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
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:Exehyw9ijwJ: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
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
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
The following numbered items show the contents of the four frames exchanged during the 4-way handshake.
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
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
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
What statement accurately describes the functions of the IEEE 802.1X standard?

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

Answer: A

Explanation: the 802.1X standard is a port -
based access control standard.A Layer 2 authentication protocol
called Extensible Authentication Protocol (EAP) is used within the 802.1X framework
to validate users at Layer 2.The 802.11 - 2007 standard also requires the use of

strong, dynamic encryption - key generation methods. CCMP/AES encryption is the default encryption method, while TKIP/RC4 is an optional encryption method.
0470438916.pdf
Pg- 17

QUESTION NO: 9
Given:You manage a wireless network that services 200 wireless users. Your facility requires 20 access points and you have installed an IEEE 802.1X LEAP with AES CCMP as an authentication and encryption solution.
In this configuration the wireless network is initially susceptible to what type of attacks? (Choose 2)

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

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
You own a coffee shop and have recently installed a 802.11g wireless hot spot for the benefit of your customers. For legal reasons you want to minimize your network and avoid liability related to the operations of hot spots.
What option specifies the best approach to achieve this goal at your public hotspot?

A. Allow only trusted patrons to use the WLAN
B. Use a WIPS to deauthenticate the malicious stations
C. Require clients STAs to have updated firewall and antivirus software
D. Disable the WLAN during non business hours

E. Use the captive portal to force users to agree to an acceptable use disclaimer
F. Configure WPA2-personal security on your access point
G. Block TCP port 25out bound on the internet router

Answer: E

Explanation:
The benefi t of a captive portal over an open SSID is that most networks with captive portals have an acceptable use policy. When the user connects to the captive portal, the acceptable use policy or a link to it is usually displayed on the captive portal page, along with a statement such as “ Logging in as a registered user indicates that you have read andaccepted the Acceptable Use Policy. ” This disclaimer, along with the acceptable use policy,may provide the organization with some legal protection if the user did something illegalwhile connected to the network. This disclaimer can also give the organization the right todisconnect the user from the network if they violate the rules of the acceptable use policy.
Page 443-444
0470438916.pdf