PL PassLeader®
Leader of IT Certifications

Vendor: CWNP

Exam Code: PW0-204

Exam Name: Certified Wireless Security Professional (CWSP)

Version: DEMO

QUESTION 1
Given: ABC company is developing an IEEE 802.11 complaint wireless security solution using 802.1X/EAP authentication. According to company policy the security should prevent an eavesdropper from decrypting data frames traversing a wireless connection.What security solution features play a role in adhering to this policy requirement? (Choose 2)

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

Answer: AF

QUESTION 2
Given: John smith uses a coffee shop's internet hot spot to transfer funds between his checking and saving accounts at his bank's website. The bank's website uses HTTPS protocol to protect sensitive account information. A hacker was able to obtain john's bank account user ID and password and transfers john's money to another account. How did the hacker obtain john's bank Account user ID and password?

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

Answer: D

QUESTION 3
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

QUESTION 4
Company's 500 employees use ABC's dual band HT 802.11 WLAN extensively general data traffic, VoWiFi, and guest access internet-only data. Size and network applications, what solution effects common and recommended security practices for this type of network?

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

Answer: B

QUESTION 5
Given:A VLAN consultant has just finished installing a WLAN controller with 15 controller based APs. Two SSIDs with separate VLANs are configured for this networkand LANs are configured to use the same RADIUS server. The SSIDs are configured as follows:

```
SSIDBlue-VLAN 10-lightweight EAP (LEAP) authentication-CCMP cipher suit
SSIDRed- VLAN 20-802.1X/PEAPv0 authentication-TKIP cipher suit
```

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

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

Answer: E

QUESTION 6
After completing the installation of new overlay WIPS, what baseline function MUST be performed?

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

Answer: C

QUESTION 7
What different security benefits are provided by endpoint security solution software? (Choose 3)

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

Answer: ADE

QUESTION 8
What software and hardware tools are used together to hijack a wireless station from the authorized wireless network in to an unauthorized wireless networks? (Choose 2)

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

Answer: BC

QUESTION 9
Given:ABC company is implementing a secure 802.11WLAN at there head quarters building in New York and at each of the 10 small, remote branch offices around the country 802.1X/EAP is ABC's preferred security solution. Where possible
At all access points (at the headquarters building and all branch offices) connect to single WLAN controller located at the head quarters building, what additional security considerations should be made? (Choose 2)

A. An encrypted connection between the WLAN controller and each controller-based AP should be used
or all branch offices should be connected to the head quarters building a VPN.
B. Remote WIPS sensors should be installed at the headquarters building and at all branch office to monitor

and enforce wireless security.

C. RADIUS service should always be provided at branch offices so that user authentication is kept on the local network.

D. Remote management via telnet, SSH, HTTP, HTTPs should be permitted across the WLAN link.

Answer: AB

QUESTION 10

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

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

A. NAV-based DoS attacks

B. RF DoS attacks

C. Layer 2 Disassociation attacks

D. Robust management frame replay attacks

E. EAPoL flood attacks

Answer: CD

QUESTION 11

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

A. Phase shift key (PSK)

B. Group master key (GMK)

C. Peerkey (PK)

D. Group temporal key (GTK)

E. Pairwise master key (PMK)

Answer: E

QUESTION 12

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

A. EAP-TTLS

B. EAP-FAST

C. LEAP

D. EAP-MD5

E. MS-CHAPv2

F. PEAPv1/EAP-GTC

Answer: ABF

QUESTION 13

Given:ABC Company has recently installed a WLAN controller and configured it to support WPA2- Enterprise security. The administrator has confirmed a security profile on the WLAN controller for each group within the company (manufacturing, sales, and engineering)
How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller?

A. The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups
after each user authentication.
B. The RADIUS server forwards a request for a group attribute to an LDAP database service, and LDAP
sends the group attribute to the WLAN controller.
C. The RADIUS server sends a group name return list attribute to the WLAN controller during every successful user authentication.
D. The RADIUS server sends the list of authenticated users and groups to the WLAN controller as a part of a 4-way handshake prior to user authentication.

Answer: B

QUESTION 14
Given:Jane Smith works primarily from home and public wireless hot spot rather than commuting to the office. She frequently accesses the office network frequently from her laptop using the 802.11 WLAN.
To safeguard her data, what wireless security policy items should be implemented? (Choose 2)

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

Answer: CF

QUESTION 15
Which of the following security protocols is supported by Wi-Fi Protected Access (WPA)?

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

Answer: C

QUESTION 16
What security weakness is presented in pre-RSNA system using 802.1X with dynamic WEP?

A. There is support for authentication of individual users.
B. All version of EAP used with dynamic WEP pass the user name across the wireless medium in clear text.

C. The session key is crackable if enough traffic is transmitted using the key.
D. With out notification, APs downgrade the security mechanism to 104-bit static WEP when the client
device does not support dynamic WEP.

Answer: C

QUESTION 17
In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking?

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

Answer: C

QUESTION 18
Given:Many corporations have guest VLANs configured on their WLAN controller that allow visitors to have wireless internet access only.
What risks are associated with implementing the guest VLAN without any protocol filtering features enabled? (Choose 2)

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

Answer: AC