Vendor: CWNP

Exam Code: CWSP-205

Exam Name: Certified Wireless Security Professional (CWSP)

Version: 13.01

Q & As: 119

QUESTION 1
Given: During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text. From a security perspective, why is this significant?

A. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
B. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.
C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
D. The username can be looked up in a dictionary file that lists common username/password combinations.

Correct Answer: B

QUESTION 2
Given: ABC Corporation is evaluating the security solution for their existing WLAN. Two of their supported solutions include a PPTP VPN and 802.1X/LEAP. They have used PPTP VPNs because of their wide support in server and desktop operating systems. While both PPTP and LEAP adhere to the minimum requirements of the corporate security policy, some individuals have raised concerns about MS-CHAPv2 (and similar) authentication and the known fact that MS-CHAPv2 has proven vulnerable in improper implementations. As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication? (Choose 2)

A. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
B. MS-CHAPv2 is subject to offline dictionary attacks.
C. LEAP's use of MS-CHAPv2 is only secure when combined with WEP.
D. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.
E. MS-CHAPv2 uses AES authentication, and is therefore secure.
F. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.

Correct Answer: BD

QUESTION 3
Given: One of the security risks introduced by WPA2-Personal is an attack conducted by an authorized network user who knows the passphrase. In order to decrypt other users' traffic, the attacker must obtain certain information from the 4-way handshake of the other users. In addition to knowing the Pairwise Master Key (PMK) and the supplicant's address (SA), what other three inputs must be collected with a protocol analyzer to recreate encryption keys? (Choose 3)

A. Authenticator nonce
B. Supplicant nonce
C. Authenticator address (BSSID)
D. GTKSA
E. Authentication Server nonce

Correct Answer: ABC

QUESTION 4
What software and hardware tools are used together to hijack a wireless station from the

authorized wireless network onto an unauthorized wireless network? (Choose two)

A. RF jamming device and a wireless radio card
B. A low-gain patch antenna and terminal emulation software
C. A wireless workgroup bridge and a protocol analyzer
D. DHCP server software and access point software
E. MAC spoofing software and MAC DoS software

Correct Answer: AD

QUESTION 5
Given: Many computer users connect to the Internet at airports, which often have 802.11n access points with a captive portal for authentication. While using an airport hot-spot with this security solution, to what type of wireless attack is a user susceptible? (Choose two)

A. Man-in-the-Middle
B. Wi-Fi phishing
C. Management interface exploits
D. UDP port redirection
E. IGMP snooping

Correct Answer: AB

QUESTION 6
What is a primary criteria for a network to qualify as a Robust Security Network (RSN)?

A. Token cards must be used for authentication.
B. Dynamic WEP-104 encryption must be enabled.
C. WEP may not be used for encryption.
D. WPA-Personal must be supported for authentication and encryption.
E. WLAN controllers and APs must not support SSHv1.

Correct Answer: C

QUESTION 7
What type of WLAN attack is prevented with the use of a per-MPDU TKIP sequence counter (TSC)?

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

Correct Answer: C

QUESTION 8
Given: You manage a wireless network that services 200 wireless users. Your facility requires 20 access points, and you have installed an IEEE 802.11-compliant implementation of 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 two)

A. Encryption cracking
B. Offline dictionary attacks
C. Layer 3 peer-to-peer
D. Application eavesdropping
E. Session hijacking
F. Layer 1 DoS

Correct Answer: BF

QUESTION 9
Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose two)

A. Rogue APs
B. DoS
C. Eavesdropping
D. Social engineering

Correct Answer: CD

QUESTION 10
Given: You are using a Wireless Aggregator utility to combine multiple packet captures. One capture exists for each of channels 1, 6 and 11. What kind of troubleshooting are you likely performing with such a tool?

A. Wireless adapter failure analysis.
B. Interference source location.
C. Fast secure roaming problems.
D. Narrowband DoS attack detection.

Correct Answer: C

QUESTION 11
Given: John Smith uses a coffee shop's Internet hot-spot (no authentication or encryption) to transfer funds between his checking and savings accounts at his bank's website. The bank's website uses the HTTPS protocol to protect sensitive account information. While John was using the hot-spot, a hacker was able to obtain John's bank account user ID and password and exploit this information. What likely scenario could have allowed the hacker to obtain John's bank account user ID and password?

A. John's bank is using an expired X.509 certificate on their web server. The certificate is on John's Certificate Revocation List (CRL), causing the user ID and password to be sent unencrypted.
B. John uses the same username and password for banking that he does for email. John used a POP3 email client at the wireless hot-spot to check his email, and the user ID and password were not encrypted.
C. John accessed his corporate network with his IPSec VPN software at the wireless hot- spot. An IPSec VPN only encrypts data, so the user ID and password were sent in clear text. John uses the same username and password for banking that he does for his IPSec VPN software.
D. The bank's web server is using an X.509 certificate that is not signed by a root CA, causing the user ID and password to be sent unencrypted.
E. Before connecting to the bank's website, John's association to the AP was hijacked. The attacker intercepted the HTTPS public encryption key from the bank's web server and has decrypted