Vendor: CWNP

Exam Code: CWSP-206

Exam Name: CWSP Certified Wireless Security Professional

Version: 13.01

Q & As: 60

QUESTION 1
You have a Windows laptop computer with an integrated, dual-band, Wi-Fi compliant adapter. Your laptop computer has protocol analyzer software installed that is capable of capturing and decoding 802.11ac data. What statement best describes the likely ability to capture 802.11ac frames for security testing purposes?

A. Integrated 802.11ac adapters are not typically compatible with protocol analyzers in Windows laptops. It is often best to use a USB adapter or carefully select a laptop with an integrated adapter that will work.
B. Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.
C. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.
D. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
E. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

Correct Answer: A

QUESTION 2
In order to acquire credentials of a valid user on a public hotspot network, what attacks may be conducted? Choose the single completely correct answer.

A. MAC denial of service and/or physical theft
B. Social engineering and/or eavesdropping
C. Authentication cracking and/or RF DoS
D. Code injection and/or XSS
E. RF DoS and/or physical theft

Correct Answer: B

QUESTION 3
What WLAN client device behavior is exploited by an attacker during a hijacking attack?

A. After the initial association and 4-way handshake, client stations and access points do not need to perform another 4-way handshake, even if connectivity is lost.
B. Client drivers scan for and connect to access point in the 2.4 GHz band before scanning the 5 GHz band.
C. When the RF signal between a client and an access point is disrupted for more than a few seconds, the client device will attempt to associate to an access point with better signal quality.
D. When the RF signal between a client and an access point is lost, the client will not seek to reassociate with another access point until the 120 second hold down timer has expired.
E. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.

Correct Answer: C

QUESTION 4
What software and hardware tools are used in the process performed to hijack a wireless station

from the authorized wireless network onto an unauthorized wireless network?

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

Correct Answer: C

QUESTION 5
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 hotspot with this security solution, to what type of wireless attack is a user susceptible?

A. Wi-Fi phishing
B. Management interface exploits
C. UDP port redirection
D. IGMP snooping

Correct Answer: A

QUESTION 6
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 can be looked up in a dictionary file that lists common username/password combinations.
B. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
D. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

Correct Answer: D

QUESTION 7
In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2-Personal. What statement about the WLAN security of this company is true?

A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
B. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.
C. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.
D. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
E. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.

Correct Answer: C

QUESTION 8
The Aircrack-ng WLAN software tool can capture and transmit modified 802.11 frames over the

wireless network. It comes pre-installed on Kali Linux and some other Linux distributions. Which one of the following would not be a suitable penetration testing action taken with this tool?

A. Auditing the configuration and functionality of a WIPS by simulating common attack sequences.
B. Transmitting a deauthentication frame to disconnect a user from the AP.
C. Cracking the authentication or encryption processes implemented poorly in some WLANs.
D. Probing the RADIUS server and authenticator to expose the RADIUS shared secret.

Correct Answer: D

QUESTION 9
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 attack?

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

Correct Answer: A

QUESTION 10
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?

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

Correct Answer: A

QUESTION 11
You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

A. 802.1X/EAP-TTLS