CWNP

Exam CWSP-205

Certified Wireless Security Professional (CWSP)

Version: 6.0

[Total Questions: 119]

Topic break down

Topic	No. of Questions
Topic 1: Wireless Network Attacks and Threat Assessment	24
Topic 2: Security Policy	6
Topic 3: Wireless LAN Security Design and Architecture	60
Topic 4: Monitoring, Management, and Tracking	29

Topic 1, Wireless Network Attacks and Threat Assessment

Question No : 1 - (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 802.11-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 2)

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

Answer: B,F

Question No : 2 - (Topic 1)

Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose 2)

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

Answer: C,D

Question No : 3 - (Topic 1)

Given: WLAN attacks are typically conducted by hackers to exploit a specific vulnerability within a network.

What statement correctly pairs the type of WLAN attack with the exploited vulnerability? (Choose 3)

A. Management interface exploit attacks are attacks that use social engineering to gain credentials from managers.
B. Zero-day attacks are always authentication or encryption cracking attacks.
C. RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range.
D. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP.
E. Social engineering attacks are performed to collect sensitive information from unsuspecting users
F. Association flood attacks are Layer 3 DoS attacks performed against authenticated client stations

Answer: C,D,E

Question No : 4 - (Topic 1)

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 John’s login credentials in near real-time.

Answer: B

Question No : 5 - (Topic 1)

An attack is under way on the network. The attack is preventing users from accessing resources required for business operations, but the attacker has not gained access to any files or data. What kind of attack is described?

A. Man-in-the-middle
B. Hijacking
C. ASLEAP
D. DoS

Answer: D

Question No : 6 - (Topic 1)

Given: 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.

What are three uses for such a tool? (Choose 3)

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

Answer: A,B,D

Question No : 7 - (Topic 1)

Given: 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. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
B. 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.
C. Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.
D. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.
E. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

Answer: B

Question No : 8 - (Topic 1)

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
B. Open 802.11 authentication with IPSec
C. 802.1X/PEAPv0/MS-CHAPv2
D. WPA2-Personal with AES-CCMP
E. EAP-MD5

Answer: B

Question No : 9 - (Topic 1)

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.

Answer: B,D

Question No : 10 - (Topic 1)

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.

Answer: C

Question No : 11 - (Topic 1)

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 2)

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

Answer: A,B

Question No : 12 - (Topic 1)

Given: 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. 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.
C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
D. 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.
E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.

Answer: B

Question No : 13 - (Topic 1)

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

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

Answer: A,D

Question No : 14 - (Topic 1)

You are configuring seven APs to prevent common security attacks. The APs are to be installed in a small business and to reduce costs, the company decided to install all consumer-grade wireless routers. The wireless routers will connect to a switch, which connects directly to the Internet connection providing 50 Mbps of Internet bandwidth that will be shared among 53 wireless clients and 17 wired clients.

To ensure the wireless network is as secure as possible from common attacks, what security measure can you implement given only the hardware referenced?

A. WPA-Enterprise
B. 802.1X/EAP-PEAP
C. WPA2-Enterprise
D. WPA2-Personal

Answer: D

Question No : 15 - (Topic 1)

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

A. 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.
B. 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.
C. 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.
D. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.
E. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.

Answer: A

Question No : 16 - (Topic 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.

Answer: B

Question No : 17 - (Topic 1)

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

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

Answer: A

Question No : 18 - (Topic 1)

Given: In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation’s wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized