We offer free update service for one year!
https://www.certqueen.com

Exam : **CWSP-206**

Title : CWSP Certified Wireless Security Professional

Version : DEMO

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.
Answer: A

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
Answer: B

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-toclient connections, even in an infrastructure BSS.
Answer: C

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
Answer: C

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
Answer: A