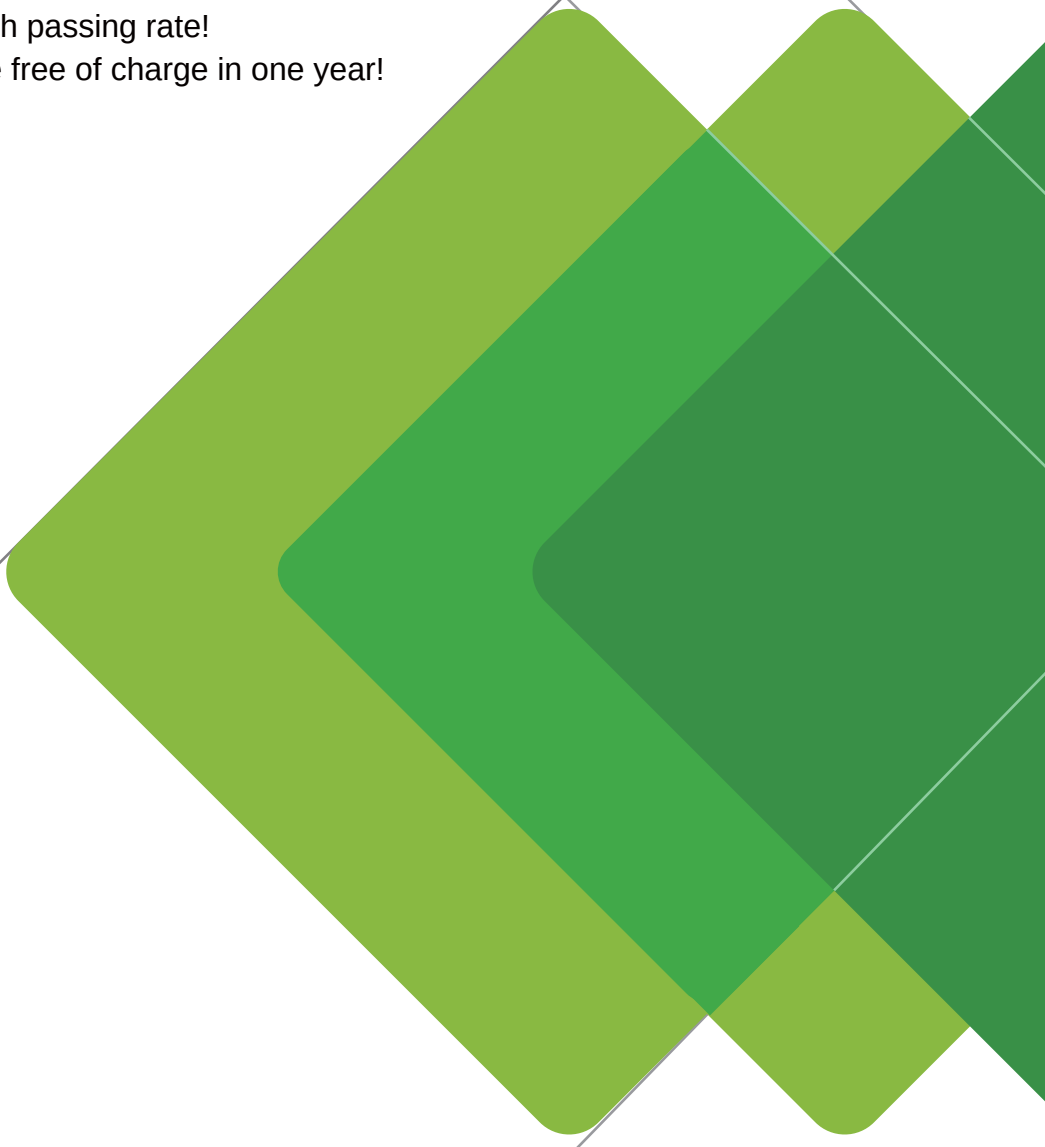
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!



http://www.it-dumps.com

Exam : **CWSP-205**

Title : Certified Wireless Security Professional

Version : DEMO

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

2.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
Answer: C

3.What 802.11 WLAN security problem is directly addressed by mutual authentication?
A. Wireless hijacking attacks
B. Weak password policies
C. MAC spoofing
D. Disassociation attacks
E. Offline dictionary attacks
F. Weak Initialization Vectors
Answer: A

4.ABC Company uses the wireless network for highly sensitive network traffic. For that reason, they intend to protect their network in all possible ways. They are continually researching new network threats and new preventative measures. 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. RF DoS attacks
B. Layer 2 Disassociation attacks
C. Robust management frame replay attacks

D. Social engineering attacks
Answer: B,C

5.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