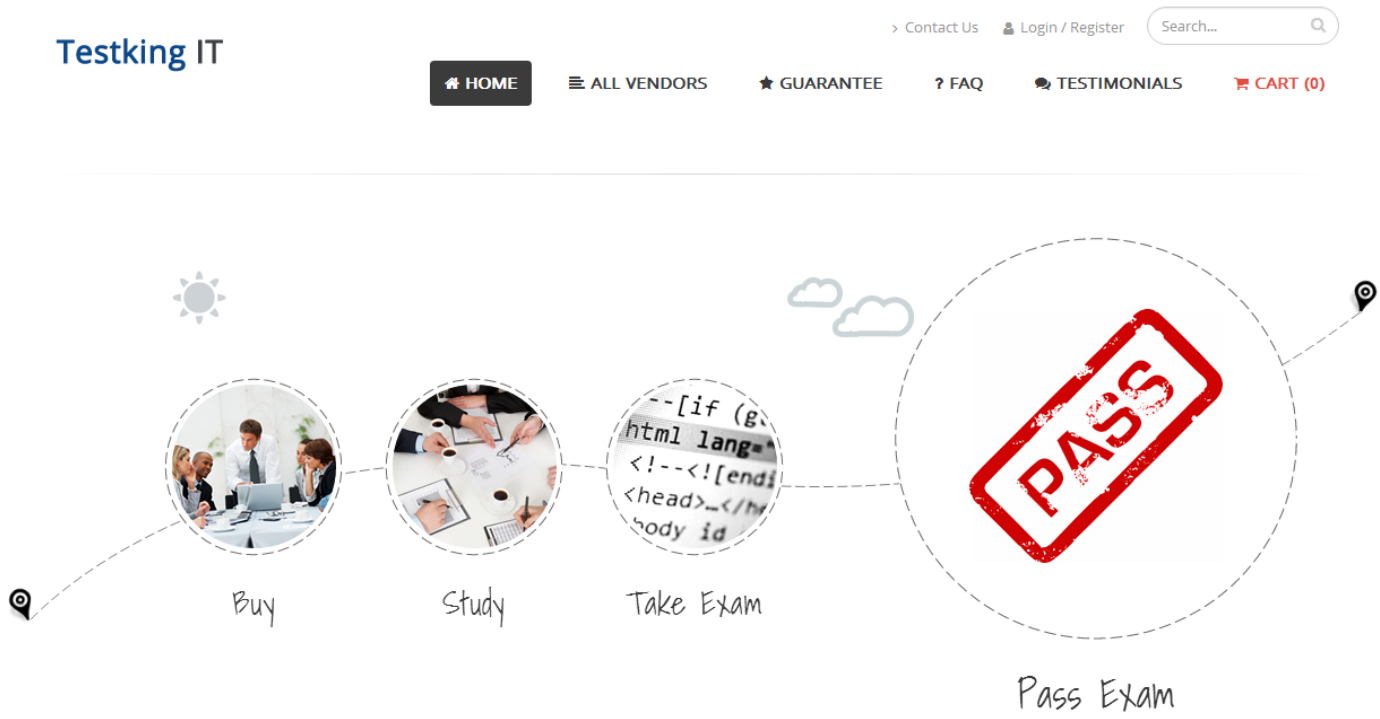
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **CWSP-206**

Title : CWSP Certified Wireless Security Professional

Vendor : CWNP

Version : DEMO

NO.1 Which of the following are the security measures that are needed to maintain the security of wireless LAN?
Each correct answer represents a complete solution. Choose all that apply.
A. WIDS
B. Firewalls
C. WLAN controller
D. WIPS
Answer: A,B,D

NO.2 Which of the following protocols is designed to provide more secure encryption than the weak wired encryption privacy?
A. LEAP
B. TKIP
C. PEAP
D. CCMP
Answer: B

NO.3 XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization. What RADIUS feature could be used by XYZ to assign the proper network permissions to users during authentications?
A. RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to- SSID mapping table in the LDAP user database.
B. RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.
C. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
D. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.
Answer: D

NO.4 You are using a utility that takes input and generates random output. For example, you can provide the input of a known word as a secret word and then also provide another known word as salt input. When you process the input it generates a secret code which is a combination of letters and numbers with case sensitivity. For what is the described utility used?
A. Generating PMKs that can be imported into 802.11 RSN-compatible devices.
B. Generating GTKs for broadcast traffic encryption.
C. Generating passwords for WLAN infrastructure equipment logins.
D. Generating dynamic session keys used for IPSec VPNs.
Answer: C

NO.5 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. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
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: A

NO.6 Which of the following provides the best protection against a man-in-the-middle attack?
A. Strong encryption
B. Firewall
C. Strong password
D. Fiber-optic cable
Answer: A

NO.7 The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?
A. Group Master Key (GMK)
B. Group Temporal Key (GTK)
C. PeerKey (PK)
D. Pairwise Master Key (PMK)
E. Key Confirmation Key (KCK)
F. Phase Shift Key (PSK)
Answer: D

NO.8 Which of the following keys is derived from a preshared key and Extensible Authentication Protocol (EAP)?
A. Pairwise Master Key
B. Group Temporal Key
C. Pairwise Transient Key
D. Private Key
Answer: A

NO.9 Which of the following attacks is used to obtain a user's authentication credentials?
A. Teardrop attack
B. Bonk attack
C. Phishing attack
D. Brute force attack
Answer: D

NO.10 Which of the following protocols is used for authentication in an 802.1X framework?
A. IPSec
B. TKIP
C. EAP
D. L2TP
Answer: C

NO.11 What WLAN client device behavior is exploited by an attacker during a hijacking attack?
A. Client drivers scan for and connect to access point in the 2.4 GHz band before scanning the 5 GHz band.
B. 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.
C. 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.
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. 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.
Answer: E

NO.12 What field in the RSN information element (IE) will indicate whether PSK- or Enterprise-based WPA or WPA2 is in use?
A. RSN Capabilities
B. Pairwise Cipher Suite List
C. AKM Suite List
D. Group Cipher Suite
Answer: C