CWNP

Exam CWSP-205

Certified Wireless Security Professional (CWSP)

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 2: Security Policy	1
Topic 3: Wireless LAN Security Design and Architecture	6
Topic 4: Monitoring, Management, and Tracking	3

Topic 2, Security Policy

Question No : 1 - (Topic 2)

What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hot-spots?

A. Require Port Address Translation (PAT) on each laptop.
B. Require secure applications such as POP, HTTP, and SSH.
C. Require VPN software for connectivity to the corporate network.
D. Require WPA2-Enterprise as the minimal WLAN security solution.

Answer: C

Topic 3, Wireless LAN Security Design and Architecture

Question No : 2 - (Topic 3)

Which one of the following describes the correct hierarchy of 802.1X authentication key derivation?

A. The MSK is generated from the 802.1X/EAP authentication. The PMK is derived from the MSK. The PTK is derived from the PMK, and the keys used for actual data encryption are a part of the PTK.
B. If passphrase-based client authentication is used by the EAP type, the PMK is mapped directly from the user’s passphrase. The PMK is then used during the 4-way handshake to create data encryption keys.
C. After successful EAP authentication, the RADIUS server generates a PMK. A separate key, the MSK, is derived from the AAA key and is hashed with the PMK to create the PTK and GTK.
D. The PMK is generated from a successful mutual EAP authentication. When mutual authentication is not used, an MSK is created. Either of these two keys may be used to derive the temporal data encryption keys during the 4-way handshake.

Answer: A

Question No : 3 - (Topic 3)

What wireless authentication technologies may build a TLS tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)

A. EAP-MD5
B. EAP-TLS
C. LEAP
D. PEAPv0/MSCHAPv2
E. EAP-TTLS

Answer: B,D,E

Question No : 4 - (Topic 3)

Given: You support a coffee shop and have recently installed a free 802.11ac wireless hot-spot for the benefit of your customers. You want to minimize legal risk in the event that the hot-spot is used for illegal Internet activity.

What option specifies the best approach to minimize legal risk at this public hot-spot while maintaining an open venue for customer Internet access?

A. Configure WPA2-Enterprise security on the access point
B. Block TCP port 25 and 80 outbound on the Internet router
C. Require client STAs to have updated firewall and antivirus software
D. Allow only trusted patrons to use the WLAN
E. Use a WIPS to monitor all traffic and deauthenticate malicious stations
F. Implement a captive portal with an acceptable use disclaimer

Answer: F

Question No : 5 - (Topic 3)

Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

A. Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.
B. Allow access to specific files and applications based on the user's WMM access category.

C. Provide two or more user groups connected to the same SSID with different levels of network privileges.
D. Allow simultaneous support for multiple EAP types on a single access point.

Answer: C

Question No : 6 - (Topic 3)

In the IEEE 802.11-2012 standard, what is the purpose of the 802.1X Uncontrolled Port?

A. To allow only authentication frames to flow between the Supplicant and Authentication Server
B. To block authentication traffic until the 4-Way Handshake completes
C. To pass general data traffic after the completion of 802.11 authentication and key management
D. To block unencrypted user traffic after a 4-Way Handshake completes

Answer: A

Question No : 7 - (Topic 3)

Given: AAA is an architectural framework used to provide three separate security components in a network. Listed below are three phrases that each describe one aspect of the AAA framework.

Option-1 — This AAA function is performed first and validates user identify prior to determining the network resources to which they will be granted access.

Option-2 — This function is used for monitoring and auditing purposes and includes the collection of data that identifies what a user has done while connected.

Option-3 — This function is used to designate permissions to a particular user.

What answer correctly pairs the AAA component with the descriptions provided above?

A. Option-1 – Access Control
Option-2 – Authorization
Option-3 – Accounting
B. Option-1 – Authentication
Option-2 – Accounting

Option-3 – Association
C. Option-1 – Authorization
Option-2 – Access Control
Option-3 – Association
D. Option-1 – Authentication
Option-2 – Accounting
Option-3 – Authorization

Answer: D

Topic 4, Monitoring, Management, and Tracking

Question No : 8 - (Topic 4)

Given: XYZ Hospital plans to improve the security and performance of their Voice over Wi-Fi implementation and will be upgrading to 802.11n phones with 802.1X/EAP authentication. XYZ would like to support fast secure roaming for the phones and will require the ability to troubleshoot reassociations that are delayed or dropped during inter-channel roaming.

What portable solution would be recommended for XYZ to troubleshoot roaming problems?

A. WIPS sensor software installed on a laptop computer
B. Spectrum analyzer software installed on a laptop computer
C. An autonomous AP mounted on a mobile cart and configured to operate in monitor mode
D. Laptop-based protocol analyzer with multiple 802.11n adapters

Answer: D

Question No : 9 - (Topic 4)

You work as the security administrator for your organization. In relation to the WLAN, you are viewing a dashboard that shows security threat, policy compliance and rogue threat charts. What type of system is in view?

A. Wireshark Protocol Analyzer
B. Wireless VPN Management Systems
C. Wireless Intrusion Prevention System

D. Distributed RF Spectrum Analyzer
E. WLAN Emulation System

Answer: C

Question No : 10 - (Topic 4)

When monitoring APs within a LAN using a Wireless Network Management System (WNMS), what secure protocol may be used by the WNMS to issue configuration changes to APs?

A. IPSec/ESP
B. TFTP
C. 802.1X/EAP
D. SNMPv3
E. PPTP

Answer: D