**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | Which of the following security solutions uses the same key for both encryption and authentication?   1. WPA 2. WPA2 3. WEP 4. 802.11i | [WEP uses the same key for encryption and authentication.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | What does WEP stands for?   1. Wireless Encryption Protocol 2. Wired Equivalent Privacy 3. Wireless Encryption Privacy 4. Wired Encryption Protocol | [WEP is an acronym for Wired Equivalent Privacy.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | What makes WEP crackable?   1. Same key used for encryption and authentication 2. Length of the key 3. Weakness of IV 4. RC4 | [WEP is crackable because of the lack of sophistication in using the IV when deploying RC4.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N64) |
| **4.** | Which form of encryption does WPA use?   1. AES 2. TKIP 3. LEAP 4. Shared key | [Image from book](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N89) |
| **5.** | Which form of authentication does WPA2 use?   1. Passphrase only 2. 802.1x/EAP/RADIUS 3. Passphrase or 802.1x/EAP/RADIUS 4. AES | [WPA2 uses either a passphrase in personal mode or 802.1x/EAP/RADIUS in enterprise mode.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N114) |
| **6.** | 802.11i is most similar to which wireless security standard?   1. WPA2 2. WPA 3. TKIP 4. AES | [802.11i is almost the same as WPA2.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N139) |
| **7.** | Which of the following is a Layer 3 security solution for WLANs?   1. MAC filter 2. WEP 3. WPA 4. VPN | [A VPN is a Layer 3 security solution for WLANs.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N164) |
| **8.** | A device that sends deauth frames is performing which type of attack against the WLAN?   1. Denial of service 2. Cracking 3. Sniffing 4. MAC spoofing | [A DoS can be performed by a device sending constant deauth frames.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N189) |
| **9.** | What is the most dangerous type of attack against a WLAN?   1. WEP cracking 2. Rogue access point 3. Eavesdropping 4. MAC spoofing | [A rogue AP is the most dangerous attack against a WLAN because it gives a hacker an open door into the network.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N214) |
| **10.** | 802.11i is implemented at which layer of the OSI model?   1. Layer 1 2. Layer 2 3. Layer 3 4. Layer 7 | [802.11i is a Layer 2 technology.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N239) |
| **11.** | Which of the following is the best option for securing a home wireless network?   1. WEP 2. Shared-key authentication 3. WPA-Personal 4. WPA-Enterprise | [WPA-Personal has the strongest authentication and encryption usable on a home network. WPA-Enterprise requires a RADIUS server, which most home users would not have the ability to set up and configure.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N264) |
| **12.** | You just installed a new wireless access point for your home office. Which of the following steps should you take immediately to secure your WLAN?   1. Spoof your clients MAC address. 2. Change the Admin password on the AP. 3. Change the channel on the AP to Channel 11. 4. Set the SSID to SECURE. | [You should immediately change the Admin password on an AP's web interface when installing a new AP.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N289) |
| **13.** | What can be done on a wireless laptop to increase security when connecting to any WLAN? (Choose two.)   1. Install and configure personal firewall software. 2. Disable auto-connect features. 3. Use WEP. 4. Use MAC filtering. | [Installing and configuring personal firewall software and disabling auto-connect features are two ways to increase the security of WLAN connections.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N314) |
| **14.** | What is an SSID used for on a WLAN?   1. To secure the WLAN 2. To manage the WLAN settings 3. To identify the WLAN 4. To configure the WLAN AP | [A Service Set Identifier (SSID) is used to identify the WLAN to wireless users.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N339) |
| **15.** | What is the best way to enforce a "no wireless" policy?   1. Install a personal firewall. 2. Disable WLAN client adapters. 3. Use a WIDS/WIPS. 4. Only connect to open APs. | [Using a wireless intrusion detection system or protection system is the best way to enforce a no wireless policy.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N364) |
| **16.** | Which of the following is a program used to spoof a MAC address?   1. MAC Again 2. Big MAC 3. TMAC 4. WZC | [TMAC is a program used to spoof a MAC address.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N395) |
| **17.** | Which of the following are Layer 7 application-secure protocols used to secure data on WLAN hotspots?   1. HTTPS 2. HTTP 3. FTP 4. VPN | [HTTPS is a secure version of HTTP commonly used to secure data on WLAN hotspots.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N420) |
| **18.** | Which type of frame is used by a WIPS to prevent WLAN users from connecting to rogue access points?   1. Disconnect 2. Deauthentication 3. Disable 4. Reject | [Deauthentication frames are used by a WIPS to prevent users from connecting to rogue APs.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N445) |
| **19.** | WPA passphrases can consist of which of the following character sets?   1. Only a–z and A–Z 2. Only a–z 3. Only a–z, A–Z, and 0–9 4. Only 0–9 | [WPA passphrases can be alphanumeric and include a z, A Z, and 0 9.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N470) |
| **20.** | Which of the following is a countermeasure to using WEP?   1. Use a strong WEP key of at least 20 characters. 2. Use a WEP key that does not repeat any of the same characters. 3. Use WPA instead of WEP. 4. Implement a preshared key with WEP. | [Using WPA is a countermeasure to the weakness of WEP.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=570260583&rowid=358&noteMenuToggle=0&leftMenuState=1#answer.N495) |

**Answers**

|  |  |
| --- | --- |
| **1.** | WEP uses the same key for encryption and authentication. |
| **2.** | WEP is an acronym for Wired Equivalent Privacy. |
| **3.** | WEP is crackable because of the lack of sophistication in using the IV when deploying RC4. |
| **4.** | WPA uses TKIP. |
| **5.** | WPA2 uses either a passphrase in personal mode or 802.1x/EAP/RADIUS in enterprise mode. |
| **6.** | 802.11i is almost the same as WPA2. |
| **7.** | A VPN is a Layer 3 security solution for WLANs. |
| **8.** | A DoS can be performed by a device sending constant deauth frames. |
| **9.** | A rogue AP is the most dangerous attack against a WLAN because it gives a hacker an open door into the network. |
| **10.** | 802.11i is a Layer 2 technology. |
| **11.** | WPA-Personal has the strongest authentication and encryption usable on a home network. WPA-Enterprise requires a RADIUS server, which most home users would not have the ability to set up and configure. |
| **12.** | You should immediately change the Admin password on an AP's web interface when installing a new AP. |
| **13.** | Installing and configuring personal firewall software and disabling auto-connect features are two ways to increase the security of WLAN connections. |
| **14.** | A Service Set Identifier (SSID) is used to identify the WLAN to wireless users. |
| **15.** | Using a wireless intrusion detection system or protection system is the best way to enforce a "no wireless" policy. |
| **16.** | TMAC is a program used to spoof a MAC address. |
| **17.** | HTTPS is a secure version of HTTP commonly used to secure data on WLAN hotspots. |
| **18.** | Deauthentication frames are used by a WIPS to prevent users from connecting to rogue APs. |
| **19.** | WPA passphrases can be alphanumeric and include a–z, A–Z, and 0–9. |
| **20.** | Using WPA is a countermeasure to the weakness of WEP. |