1. 1 / 1 point

What are some weaknesses of the WEP scheme? Select all that apply.

- [x] Its small IV pool size

Correct
The RC4 stream cipher had a number of design flaws and weaknesses. WEP also used a small IV value, causing frequent IV reuse. Lastly, the way that the encryption keys were generated was insecure.

- [ ] Its use of ASCII characters for passphrases
- [x] Its poor key generation methods

Correct
The RC4 stream cipher had a number of design flaws and weaknesses. WEP also used a small IV value, causing frequent IV reuse. Lastly, the way that the encryption keys were generated was insecure.

- [x] Its use of the RC4 stream cipher

Correct
The RC4 stream cipher had a number of design flaws and weaknesses. WEP also used a small IV value, causing frequent IV reuse. Lastly, the way that the encryption keys were generated was insecure.

2. 1 / 1 point

What symmetric encryption algorithm does WPA2 use?

- ○ DSA
- ◉ AES
- ○ RSA
- ○ DES

Correct
WPA2 uses CCMP. This utilizes AES in counter mode, which turns a block cipher into a stream cipher.

3. 1 / 1 point

How can you reduce the likelihood of WPS brute-force attacks? Check all that apply.

- [ ] Use a very long and complex passphrase.
- [x] Implement lockout periods for incorrect attempts.

Correct
Ideally, you should disable WPS entirely if you can. If you need to use it, then you should use a lockout period to block connection attempts after a number of incorrect ones.

- [ ] Update firewall rules.
- [x] Disable WPS.

Correct
Ideally, you should disable WPS entirely if you can. If you need to use it, then you should use a lockout period to block connection attempts after a number of incorrect ones.

4. 1 / 1 point

Select the most secure WiFi security configuration from below:

- (●) WPA2 enterprise
- ( ) WPA personal
- ( ) WEP 128 bit
- ( ) WPA enterprise
- ( ) WPA2 personal
- ( ) None

Correct
WPA2 Enterprise would offer the highest level of security for a WiFi network. It offers the best encryption options for protecting data from eavesdropping third parties, and does not suffer from the manageability or authentication issues that WPA2 Personal has with a shared key mechanism. WPA2 Enterprise used with TLS certificates for authentication is one of the best solutions available.

5. 1 / 1 point

What process authenticates clients to a network?

- ( ) TKIP
- ( ) WPA2
- (●) Four-way handshake
- ( ) HMAC-SHA1

Correct
This process is called the Four-Way Handshake, since it's made up of four exchanges of data between the client and AP. It's designed to allow an AP to confirm that the client has the correct pairwise master key, or pre-shared key in a WPA-PSK setup without disclosing the PMK.