

Real-World Scenario 9-3: Wireless Security Issues

Scenario: You are tasked with securing a WAP. Examine the figure below. What four potential security issues can you identify in the configuration?

☒ WPA/WPA2 - Personal(Recommended)

Version:

Encryption:

PSK Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

Real-World Scenario 9-3 Solution

This is a fairly insecure configuration.

1. WPA2 is recommended over WPA, though that is not the worst of the offenders.
2. TKIP is considered outdated (deprecated) for most technical scenarios. It should be replaced with AES (or CCMP if necessary). The outdated protocols that the Security+ exam really focus on are WEP, TKIP, and RC4 (though that last one is debatable).
3. The password is fairly weak. Although it employs a certain level of complexity (uppercase letters and numbers), it is only 6 characters long. In fact, this password would not be accepted by this system—like it says, it requires at least 8 characters. Most organizations require 8- or 10-character passwords, and 15 for super-secure enterprise environments. As a side note, the password is showing up as plain text. If at all possible, use a system that allows for the display of asterisks (or some other symbol) in place of the actual characters. Or, if you are the only person administering this router, be sure that no one has viewing access of your screen when you enter the password, and consider a screen protector (a good idea in general for sys admins).
4. If TKIP must be used, the group key update period should be set to something. Zero (0) is the default, which means that the key for the password is not updated. Setting this to a number such as 3600 (60 minutes) is a common practice so that the key updates every hour, thereby increasing security. Setting it to the minimum of 30 seconds is not recommended because that could cause performance issues. Keep in mind that TKIP has security issues concerning technologies such as 802.11n. It should be avoided if at all possible.

Finally, a device such as this one might not be secure enough for your organization. This is something to consider. Although it can be obtained

for less than \$100, the possible lack of security and options might cause your company to pay the price in other ways. Many companies suffer from a lack of good IT equipment due to an outdated IT budget. A good tech finds ways to encourage the budgeting decision makers to upgrade the company's technology once in a while.

Video Solution: Watch the video solution "9-3: Wireless Security Issues."