

Real-World Scenario 9-5: War-driving...and the Cure

Scenario: Your boss has heard of "war-drivers" and has obvious concerns about unauthorized access to your wireless network. He wants to have proof that it will be difficult for a war-driver to access the network, and that there are no jamming devices or other interference-based devices within the perimeter of the building.

Your job is to scan the building, make any configurations necessary, and explain how you have configured the wireless network to be war-driver-proof.

Real-World Scenario 9-5 Solution

The first step is to scan the area to find out which wireless networks are visible. This can be done in several ways. For example, you could use just about any mobile device with Wi-Fi enabled and search for wireless networks. From that, you can glean the name of the wireless network, the connection speed/type, and whether encryption is used. Or, you could use a wireless-enabled desktop or laptop computer by using the built-in wireless network finding software, either by Microsoft, by another OS manufacturer, or by a network adapter manufacturer. However, one of the best ways is to use a third-party Wi-Fi scanning (or "stumbling") program. These can give very detailed information about the wireless networks that are available. In fact, they are the types of tools that war-drivers would use, so it makes sense for you, as the security administrator, to use them as well and see what your enemy sees.

Next, based on your wireless scans and physical inspections, you want to locate and shut down any unauthorized WAPs, rogue devices, or evil twins, and remove any devices causing interference or jamming.

Then, for the authorized WAPs, reduce the power level of the antennas until you can scan them from inside the perimeter of the office but not from the outside. Getting this just right might take several attempts, but it pretty much eliminates the attacker's ability to scan for your network. This is a common method, especially if you are using 802.11n or 802.11ac, which have powerful ranges. Of course, this does not address malicious insiders, but other solutions, such as authentication, NIDS/NIPS, and so on can be used to deal with them.

If possible, disable the SSID to make it invisible. The SSID broadcast is not the only way that a WAP can be located, but disabling it is a good first step.

Finally, secure the authorized WAPs in the manner you did during previous Real-World Scenarios: Update the device, set complex passwords, use strong encryption, and consider MAC filtering.

Video Solution: Watch the video solution "9-5: War-driving...and the Cure."