what is Reaver

Reaver implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, as described in Brute forcing Wi-Fi Protected Setup.

Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations.

On average Reaver will recover the target AP's plain text WPA/WPA2 passphrase in 4-10 hours, depending on the AP. In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase.

Reaver Features

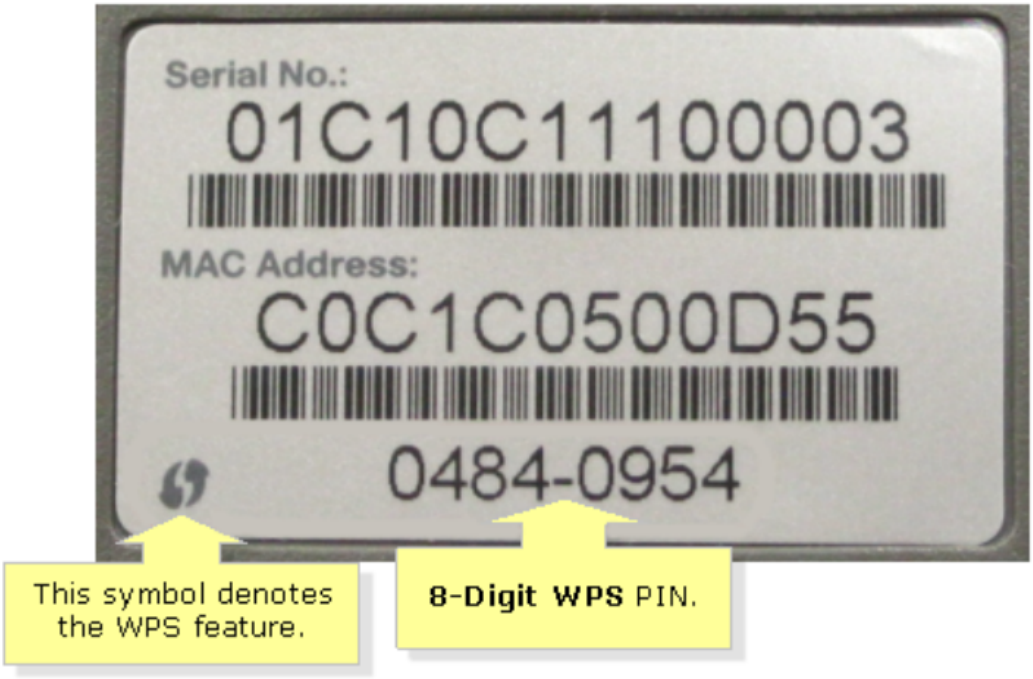
- Brute force attack against Wifi Protected Setup
- Detects and reacts to lock outs
- Pixie Dust Attack
- WPS Registrar PINs are locked after 0-11 attempts

WPS

WPS stands for Wi-Fi Protected Setup. It is a wireless network security standard that tries to make connections between a router and wireless devices faster and easier. WPS works only for wireless networks that use a password that is encrypted with the WPA Personal or WPA2 Personal security protocols.

WPS PIN

A WPS PIN is an eight-digit number used to connect a device to the router. A successful WPS PIN bruteforce attack provides an attacker access to the router's WPS functionality and the network's WPA/WPA2 passphrase.



How to use Reaver

Install Reaver

```
sudo apt-get update
sudo apt-get aircrack-ng libssl-dev sqlite3 libsqlite3-dev aircrack-ng pixiewps
sudo apt-get install reaver
```

install video link: https://www.youtube.com/watch?v=NLiRSowIw7E

Run Reaver

```
reaver -i wlan0mon -b 00:01:02:03:04:05 -vv
```

- -i: interface which is in monitor mode
- -b: BSSID of the target AP
- -vv: verbose mode
- -c: channel of the target AP
- -a: automatically detect the best advanced options for the AP
- -d: delay in seconds between pin attempts
- -e: use external registrar's PIN

Reaver options

```
reaver --help
```

- -a: automatically detect the best advanced options for the AP
- -b: target AP's BSSID
- -c: target AP's wireless channel
- -d: delay in seconds between pin attempts
- -e: use external registrar's PIN

wash - scan for WPS enabled APs

what is wash

Wash is a utility for identifying WPS enabled access points. It can survey the current channel and neighboring channels, identifying WPS-enabled APs and the manufacturer set default SSID prefixes. Wash can be used to scan for WPS-enabled APs and to attack those WPS access points that are vulnerable to the WPS brute force attack.

```
wash -i wlan0mon
```

- -i: interface which is in monitor mode
- -C: colorize output
- -s: skip wash's check for a WPS locked state
- -o: output only the AP's that have WPS enabled
- -W: wait for a WPS locked state to be cleared before scanning
- -a: automatically detect the best advanced options for the

References

- https://www.hackthebox.com/blog/wps-pin-attacks-and-cracking-wps-with-reaver
- https://www.youtube.com/watch?v=_H9zB1ZWkvQ
- https://github.com/t6x/reaver-wps-fork-t6x
- https://www.geeksforgeeks.org/brute-forcing-wps-pins-with-reaver-in-linux/