Reaver_Bully Documentation

Introduction

Reaver and Bully are tools for brute-forcing WPS (Wi-Fi Protected Setup) PINs on wireless networks. They are used in penetration testing to audit WPS-enabled routers.

Features

- Reaver: WPS PIN brute force with support for pixie-dust attacks.
- Bully: Faster, alternative implementation supporting more chipsets.
- Both support verbose logging and external WPS pin lists.

Installation

Reaver:

sudo apt install reaver

Bully:

sudo apt install bully

Usage

Reaver:

sudo reaver -i wlan0mon -b [BSSID] -vv

Bully:

sudo bully wlan0mon -b [BSSID]

Disclaimer

Brute-forcing WPS PINs is highly intrusive. Only use these tools with permission.

Conclusion

Reaver and Bully are efficient tools for testing the security of WPS-enabled networks.