[Exploitation/Wifi] HackrfOne

Introduction

Ce boitier permet d'effectuer diverses attaques sur les ondes radios.

Manuel

Firmwares

Téléchargez les firmwares .bin à cette adresse :

- https://github.com/greatscottgadgets/hackrf/releases/

Puis balancez le firmware sur l'équipement après l'avoir branché en USB :

```
hackrf_spiflash -Rw hackrf_one_usb.bin
```

Fake GPS

Cette technique permet d'envoyer un faux signal GPS aux appareils environnants.

Tout d'abord, installez le paquet **hackrf** :

```
sudo apt install hackrf
```

Puis connectez le boitier et vérifier qu'il soit détecté avec la commande suivante :

```
hackrf_info
```

Ensuite, clonez ce dépôt :

```
git clone https://github.com/osqzss/gps-sdr-sim.git
```

Compilez pour obtenir le binaire :

```
make
```

Puis téléchargez la dernière éphéméride sur le site de la NASA :

- https://cddis.nasa.gov/archive/gnss/data/daily/2025/brdc/

Et lancez l'outil pour générer un fichier **gpssim.bin** à partir d'une position GPS :

```
./gps-sdr-sim -b 8 -e brdc3540.21n -l 48.858844,2.294351,100
```

Puis lancez hackrf pour propager les ondes :

```
hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 40
```

Jamming

Pour brouiller un signal wifi :

```
hackrf_transfer -t /dev/urandom -f 2442000000 -s 20000000 -a 1
```

Revision #3
Created 1 April 2025 11:58:44 by Elieroc
Updated 2 April 2025 12:22:18 by Elieroc