WIFI MEDLEY & DIY ROUTER

PAR MAXIME LEBLANC

PLAN

> $ TREE

- Intro
- Get Physical
- Get Connected
- Get Nasty
- Get High
- Do It Yourself!

INTRO

> $ WHOAMI

- Maxime Leblanc - @maxwhite
  - B.Sc USherbrooke
    - Informatique (Sciences)
  - M.Sc. ULaval – sous Pr. Mejri
    - Sécurité Informatique
  - M.B.A. ULaval + UKoç
    - Affaires électroniques
  - Now working for Poka inc.
  - Infosec Convention Enthousiast®

INTRO

> $ CONTEXTE

- J'aime déménager souvent
  - Souvent une période de transition sans WiFi installé
- Je voyage beacoup
  - HotSpots, AccessPoints, Hotels, Bars...
- J'ai donc développé certaine "résilience" face à mon environnement WiFi
  - Pas un professionnel
  - Appris "sur le tas"

INTRO

> $ TECHNOLOGIES

- Open WiFi
  - Captive Portal
- WEP
- WPA/WPA2
  - Pre-Shared Key
  - WiFi Protected Setup
  - WPA2-Enterprise

GET PHYSICAL

> $ HARDWARE

- Testé plusieurs adapteurs WiFi dernièrement
  - Sur Kali Linux en utilisant mon laptop personnel ainsi qu'un RasPi3

GET PHYSICAL

> $ HARDWARE

- Cartes WiFi intégrées
- Intel N6200 (Lenovo W510)
  - Les drivers Kali supportent les modes monitor et l'injection ainsi que le master mode. Portée raisonnable
- Broadcom BCM2837 (Raspberry Pi)
  - Simple d'utilisation, bonne portée
  - Les drivers Kali ne supportent pas le monitor mode par défaut
  - Les drivers Kali supportent le master mode, mais laborieusement

GET PHYSICAL

> $ HARDWARE

- CanaKit's Ralink 5370
  - Kali supporte les modes Monitor, Master et l'injection
  - Cheap (9$)
  - Ne nécessite pas de powered-hub sur un RaspberryPi

GET PHYSICAL

> $ HARDWARE

- Alfa's AWUS036NH
- SimpleWifi's N124-700
  - Semblent être le même modèle "under the hood"
  - Un grand classique pour les amateurs de WiFi hacking
  - De ce fait, Kali supporte parfaitement tous les "features" que l'on recherche, soit les modes Monitor et Master, ainsi que l'Injection de paquets
  - Pourrait nécessiter un "powered hub" sur RaspBerry Pi

GET PHYSICAL

> $ HARDWARE

- Alfa's AWUS036NH
  - La nouvelle "bête" signée Alfa
  - Drivers faciles à trouver sur architecture x86
  - Pas-mal moins évident sur ARM (RasPi)
  - Sur GitHub, la bonne version des drivers se trouve ici:
    - https://github.com/aircrack-ng/rtl8812au
    - Plusieurs tentatives avec d'autres versions, sans succès
  - Une fois les drivers bien installés, fonctionne comme un charme :-)
  - Nécessite un "powered hub" pour une utilisation stable sur RasPi

GET PHYSICAL

> $ HARDWARE

- SimpleWifi's parabolic COM-2424
  - Compatible avec les adapteurs populaires
    - (N-type connector)
  - 7 degrés de largeur de rayon
  - 24 dBi de *Gain*
  - Testée en combinaison avec la Alfa AWUS036NH
  - Résultats mitigés...

GET CONNECTED

> $ CONNECT OPEN

- Première couche de (non)-sécurité
  - Parfois protégés par un "captive-portal"
  - Parfois protégés par un filtre MAC
  - Souvent déçus par de simple imprimantes...

GET CONNECTED

> $ CONNECT OPEN CAPTIVE-PORTAL

- Un "captive portal" est un point d'accès qui bloque l'accès aux utilisateurs tant qu'ils n'ont pas effectué une certaine action
  - Accepté les conditions d'utilisation
  - Payé un droit d'accès
  - Confirmé son identité

GET CONNECTED

> $ CONNECT OPEN CAPTIVE-PORTAL

- Plusieurs manières pour contourner les limitations imposées
  - Copier l'addresse MAC d'un appareil déjà connecté
    - Utiliser airomon-ng + network settings
  - Utiliser un VPN
    - Parfois le "blocage" ne bloque que les requêtes DNS
    - Utiliser un VPN avec addresse directe (sans DNS) fonctionne dans ces cas-là
  - Utiliser un tunnel DNS
    - Nécessite une préparation préalable

GET CONNECTED

> $ CONNECT WEP

- WEP est une technologie désuète, craquable en 15 minutes environs dans de bonne conditions
  - De moins en moins fréquent "in the wild", pour des raisons évidentes
  - Les fournisseurs d'accès les on éliminé par attrition
  - Nécessite un driver de carte qui gère l'injection de paquets
- Il existe des logiciels qui automatisent les attaques WEP
  - WiFite
  - Résultats mitigés
- Je recommande la bonne vieille technique de suivre un tutoriel trouvé via Google

GET CONNECTED

> $ CONNECT WPA2

- Le "state-of-the-art" en matière de sécurité WiFi
- Aucune attaque connue sur le protocole "vanille" permettant de craquer en un temps raisonnable
- Nécessite un minimum de 8 caractères comme mot de passe
- Mais il existe certaines techniques...

GET CONNECTED

> $ CONNECT WPA2/PSK

- Il est possible de craquer un WiFi WPA2/PSK en utilisant une attaque par dictionnaire
  - Il faut utiliser airomon-ng (ou un autre logiciel de capture) et attendre de capturer un "handshake" (un échange d'initialisation de connection)
  - Une fois le "handshake" capturé, il est possible de le cracker "offline"
  - Afin que ce soit possible en un temps raisonnable, un bon dictionaire est nécessaire
  - Il est peut-être possible de brute-forcer avec un pattern connu (ie: Bell) via un masque hashcat

GET CONNECTED

> $ CONNECT WPA2/WPS

- Aux alentours de 2012, il est découvert que les routeurs ayant le WPS (WiFi Protected Setup) activé sont vulnérable à des attaques par brute-force
  - Les logiciels "wash" et "reaver" viennent de base avec Kali et permettent d'exploiter cette vulnérabilité
  - Encore à ce jour, c'est définitivement la technique avec laquelle j'ai le plus de succès
  - Prend environs 1-2 jours à brute-forcer
  - Le brute-force doit se faire "online"

GET CONNECTED

> $ CONNECT WPA2/ENTERPRISE

- Dans le cas d'un réseau WPA2/Enterprise, les appareils clients utilisent des informations de connexion centralisées (style ActiveDirectory)
- Il est possible de se faire passer pour un AccessPoint légitime d'entreprise et récupérer ces informations sous forme d'échange EAP/MSCHAP
- Le logiciel hostapd-wpe (entre-autres) peut être utilisé à cette fin
- Combinaison symbiotique avec la technique Karma

GET CONNECTED

> $ CONNECT WPA2/ENTERPRISE

- L'attaque par Karma consiste à imiter des "probes" légitimes reçus via les cartes réseau environnantes
- Les ordinateurs cherchent en permanence des Points d'Accès connus auxquels ils se sont connectés précédemment
- Dans le cas de WPA2/Enterprise, si le client ne vérifie pas le certificat du point d'accès auquel il se connecte, il risque d'envoyer des informations de connection à un point d'accès malicieux

GET NASTY

```
> $ DENY *
```

- La couche physique WiFi est facilement perturbée par les interférences
- Voyez l'effet du micro-ondes sur vos appareils, par exemple
- Il est possible de provoquer ces interférences via SDR
  - Probablement d'autres techniques plus "primitives" fonctionnent aussi afin de perturber les bandes 2.4Ghz et 5.2Ghz
  - La bande 2.4Ghz est déjà elativement saturée.

GET NASTY

> $ DENY THAT_GUY

- Une méthode un peu plus subtile est l'attaque par dé-authentification
- Il est possible pour un attaquant de dé-authentifier un autre client sans lui-même être connecté au Access Point
- Cette attaque peut être utile pour forcer des clients à se reconnecter et ainsi:
  - Récupérer des "handshakes" WPA2
  - Récupérer des ESSID non-broadcastés
  - Troller

GET NASTY

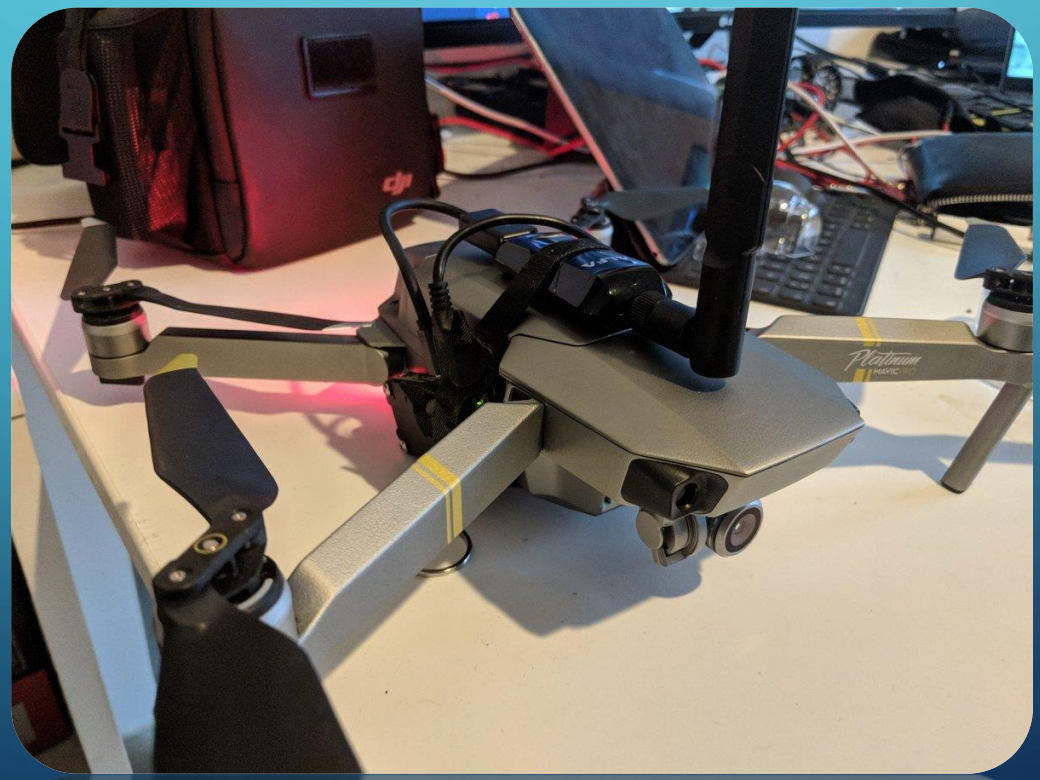
> $ ROGUE AP

- Il est aussi possible de se monter un AccessPoint malicieux
  - Hostapd-wpe + Karma mode
  - SSLStrip + traffic sniffing
  - Captive portal + Social login
  - MiTM + SSL CCS Injection
  - My personal favorite: DHCP+ShellShock
    - Option DHCP malicieuse exploitant ShellShock
    - L'ordinateur victime se connecte et a Internet normalement
    - Pendant l'échange DHCP, un reverse-shell (as root) a été poppé

GET HIGH

> $ LIFTOFF

- Ces Access Points malicieux peuvent aussi devenir "airborne"



GET HIGH

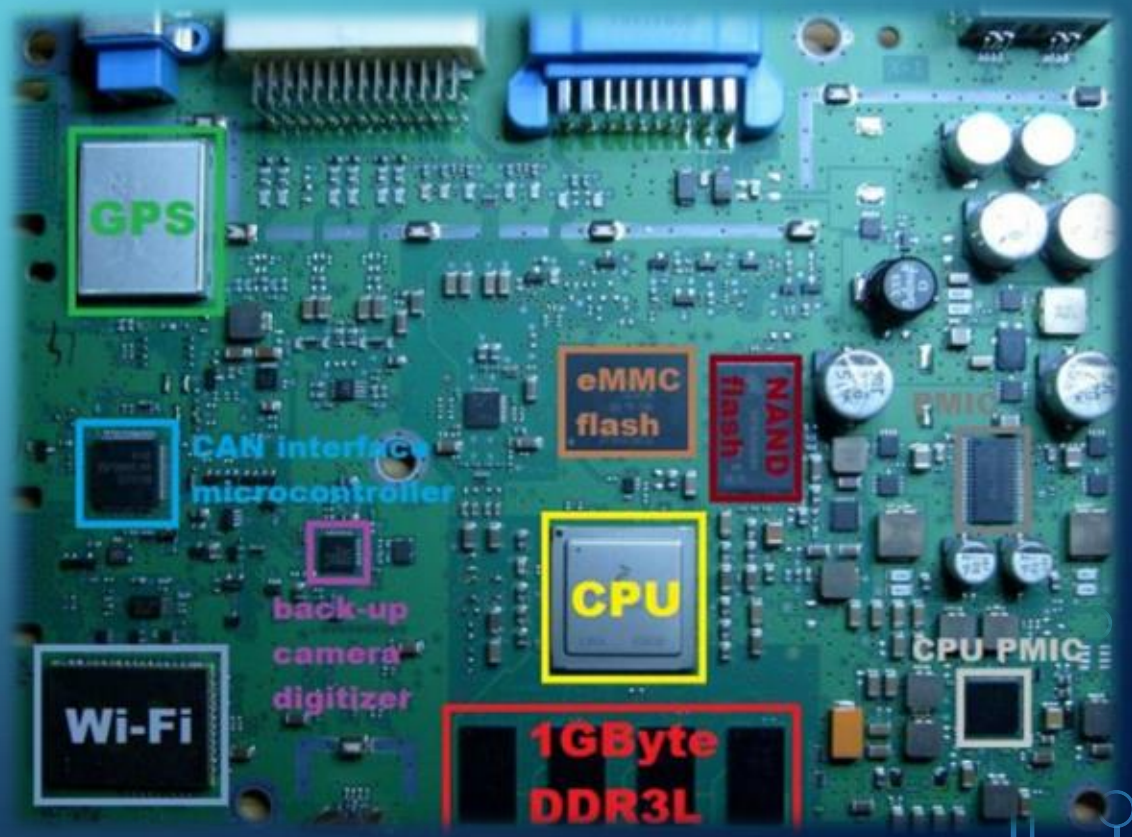
> $ USE_CAR

- Le phénomène du wardriving consiste à chercher et répertorier les différents réseaux WiFi d'une ville ou d'un quartier, habituellement en se promenant en véhicule à moteur

GET HIGH

> $ USE_ONLY_CAR

- **Stefan Tanase** et **Gabriel Cirlig** ont récemment démontré qu'une voiture moderne a tout ce qu'il faut pour faire du wardriving par elle-même
- Pas besoin d'ordinateur ou même e RasPi



GET HIGH

> $ USE_ONLY_CAR

- Une voiture moderne (une Mazda dans ce cas-ci) a toutes les facilités d'un Linux minimaliste via le système de divertissement
- Incluant des symboles de debugging, etc...

GET HIGH

> $ USE_ONLY_CAR

- Les chercheurs in "infecté" leur voiture avec un spyware
- La voiture enregistrait ses positions GPS régulièrement
- Lorsqu'elle détectait un WiFi open, la voiture uploadait automatiquement les données recueillies

DO IT YOURSELF

> $ SELF_SERVE

- Le magasine 2600 cet hiver relatait les aventures rocambolesques d'un gars qui n'arrêtait pas de se faire hacker son WiFi fourni par sa compagnie de télécom
- Je me suis dit que si seulement il avait su comment s'en fabriquer un, il aurait économisé bien des ennuis
- En plus d'être sécuritaire, c'est un projet amusant et pédagogique :-)

DO IT YOURSELF

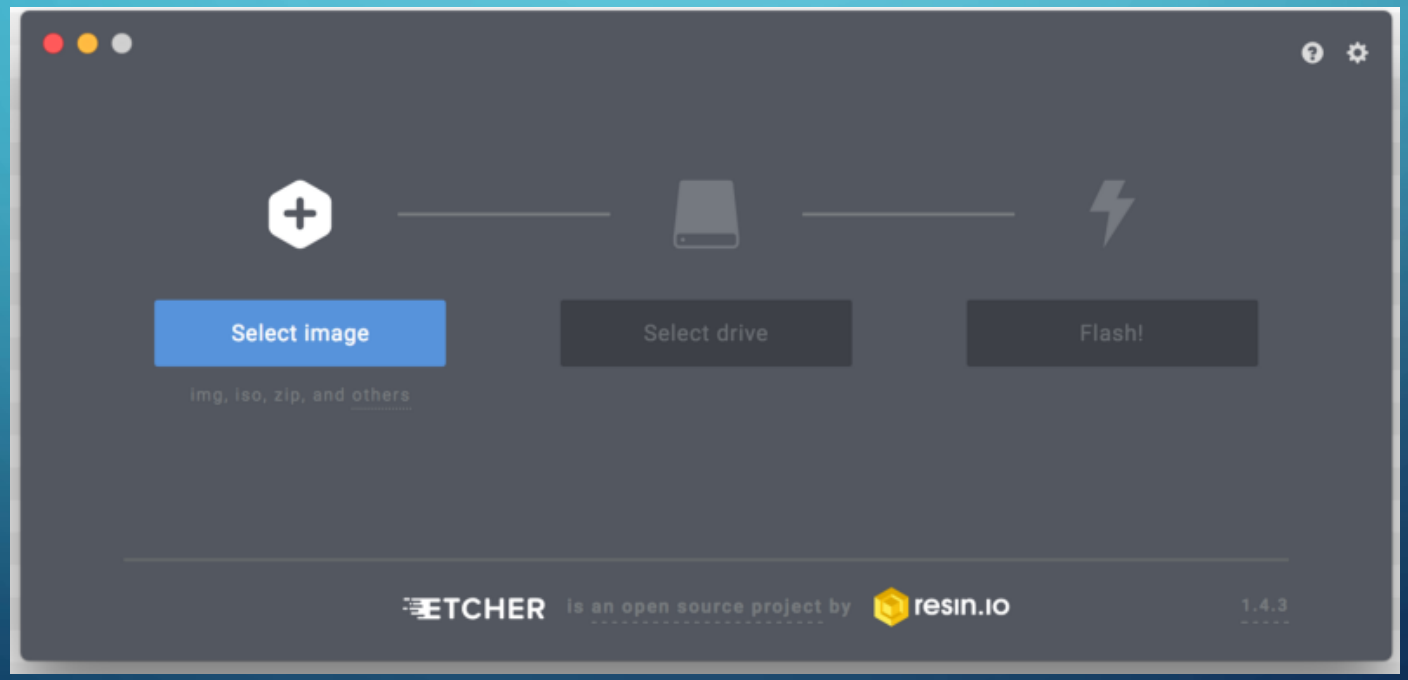
> $ SELF_SERVE

- Prerequisites
  - 1 x Raspi
  - 1 x WiFi Adapter
  - Etcher software
  - Re4son-Pi's Kali Linux stable version
    - https://re4son-kernel.com/re4son-pi-kernel/

DO IT YOURSELF

> $ SELF_SERVE

- Step 1 – Burn Re4son-Pi to your SD-Card



DO IT YOURSELF

> $ SELF_SERVE

- Step 2 – Choose your weapon

DO IT YOURSELF

> $ SELF_SERVE

- Step 3 – Setup local static IP addresses and a DHCP server

```
# apt-get install dhcpd
```

/etc/network/interfaces

```
auto wlan1
iface wlan1 inet static
address 192.168.0.1/24
gateway 192.168.0.1
```

/etc/udhcpd

```
start              192.168.0.100
end                192.168.0.254
interface          wlan1#
Optional
opt      dns       1.1.1.1
option   subnet    255.255.255.0
opt      router    192.168.0.1
option   domain    local
```

DO IT YOURSELF

> $ SELF_SERVE

- Step 4 – Install HostAPD

```
# apt-get install hostapd
```

/etc/hostapd/hostapd.conf

```
interface=wlan1
driver=nl80211
ssid=MyKaliWiFiNetwork
hw_mode=g
channel=6
wmm_enabled=1
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_passphrase=SecretPass
rsn_pairwise=CCMP
```

DO IT YOURSELF

> $ SELF_SERVE

- Step 5 – Configure IPTables

```
# sysctl -w net.ipv4.ip_forward=1
# iptables -t nat -A  POSTROUTING -o eth0 -j MASQUERADE
# apt-get install iptables-persistent
# iptables-save > /etc/iptables/rules.v4
```

DO IT YOURSELF

> $ SHAMELESS_PLUG

- https://medium.com/poka-techblog/diy-wifi-router-using-kali-linux-on-a-raspberry-pi-3-model-b-89b8e5497cbf

CONCLUSION

> $ SHUTDOWN

- Le hacking WiFi n'est pas *si* déterministe
  - Plusieurs facteurs imprévisibles semblent influencer les résultats
  - La même expérience peut marcher un jour mais pas le lendemain
- J'ai mon propre projet de WarDriving en cours
  - Wishful Thinking: Penser que j'allais coder ça entre le PHDays et le NorthSec

- Circle of Hope: 20 au 22 Juillet, NYC