



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Réseaux Wi-Fi et logiciel libre

Solutions Linux 2003

Jérôme Poggi

<Jerome.Poggi@hsc.fr>





Plan

- Qu'est ce que le Wi-Fi
- Exemples de logiciels libres pour le Wi-Fi
 - Driver Prism wlan-ng
 - HostAP
 - NoCat Auth / NoCat Splash
 - Kismet
 - WifiScanner



Qu'est ce que le Wi-Fi

- Wi-Fi ou norme IEEE 802.11b
 - Réseau local radio à 11 Mb/s
 - 54 Mb/s en version 802.11g
 - 14 canaux dont 13 autorisés en France
 - Libéralisation en cours
 - Portées
 - Sans antennes "à vue" : 100m
 - Avec antennes "à vue" > 50km
 - Prix Faibles
 - Carte : à partir de 60€
 - Borne : à partir de 130 €



Technologies WLAN

- IEEE 802.11b (Wi-Fi), sur 2,4 GHz, 11 Mb/s
 - La principale technologie, disponible depuis 1997
- IEEE 802.11a (Wi-Fi5), sur 5 GHz, 54 Mb/s
 - Disponible depuis fin 2001
- IEEE 802.11g, IEEE 802.11e
 - Remplaceront respectivement IEEE 802.11b et IEEE 802.11a
 - Non disponible sur le marché
 - 802.11g prévue fin 2002
 - Possibilité de mise à jour logicielle de 802.11b vers 802.11g
 - Qualité de service définie dans IEEE 802.11f
 - Gestion dynamique puissance / fréquences dans IEEE 802.11h



Trois types de trames

- Trames d'administration
 - Beacon
 - Probe request/reply
 - Association
 - Authentification
- Trames de contrôle
 - Request to send / Clear to send
 - ACK
- Trames de données
 - Données en clair ou chiffrée



Le Wi-Fi et la sécurité

- Support radio
 - Écoutes aisées
 - Brouillage simple et non perturbation non garanti
- Chiffrement avec le WEP
 - Besoins d'améliorer la confidentialité
 - Mauvaise implémentation de RC4
 - Problèmes corrigés dans la norme IEEE 802.11g
 - Méthodes de cassage du WEP connues et publiques
 - De simples à compliquées



Wardriving

- Avertissement :

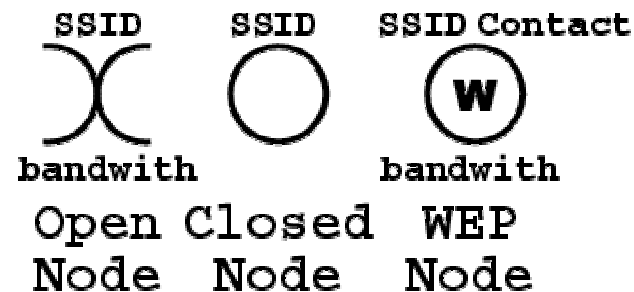
Auditer, surveiller, écouter, faire du wardriving sur un réseau, qui ne vous appartient pas, est illégal.

- Warchalking

- Marquage de réseau sans fil

- Wardriving

- Extension du WarDialing
 - Recherche de réseaux sans fil depuis une voiture





Exemples de développement

- Linux Wlan-NG
 - Pilote de carte WLAN avec chipset Prism
- HostAP
 - Création de borne WLAN sous Linux
- Nocat Auth / No Splash
 - Authentification, filtrage pour Hotspot public
- Kismet, WifiScanner
 - Outil de détection, d'audit et d'analyse de Wi-Fi



Pilote WLAN-NG

- Pilote Linux pour carte WLAN
 - Chipset Prism/Intersil
 - <http://www.linux-wlan.org/>
 - Mozilla Public License
- Évolution rapide
- Paramétrage très étendu (MIB complète)
- Liste de diffusion dynamique
- Intégré dans de multiple distributions



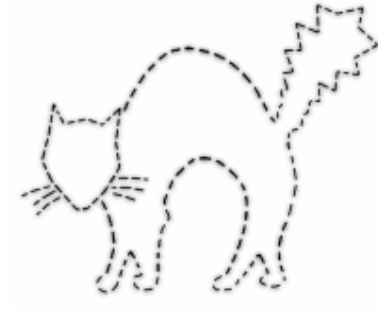
Pilote HostAP

- Pilote permettant de transformer un PC en borne
 - Chipset Prism/Intersil
 - <http://hostap.epitest.fi/>
 - Licence GPL
- Permet pour un moindre coût de faire :
 - Du filtrage
 - De la journalisation
 - De l'authentification
 - Hotspot publique ou communautaire



NoCat Auth/Splash

- Portail d'authentification en Perl
 - <http://nocat.net/>
 - Fonctionne sous Linux 2.2 (ipchains)
 - Version portable en C en développement
- Assure l'authentification avec GPG
- Assure la mobilité (*roaming*)
- Qualité de service minimum





WifiScanner

- Outil d'audit et d'analyse de réseaux 802.11b
 - Chipset Prism avec pilote Wlan-NG sous Linux
 - <http://wifiscanner.sf.net/>
 - Licence GPL
- Affichage compact
- Interface curses temps réel
- Analyse d'anomalies
- Triangulation possible

```

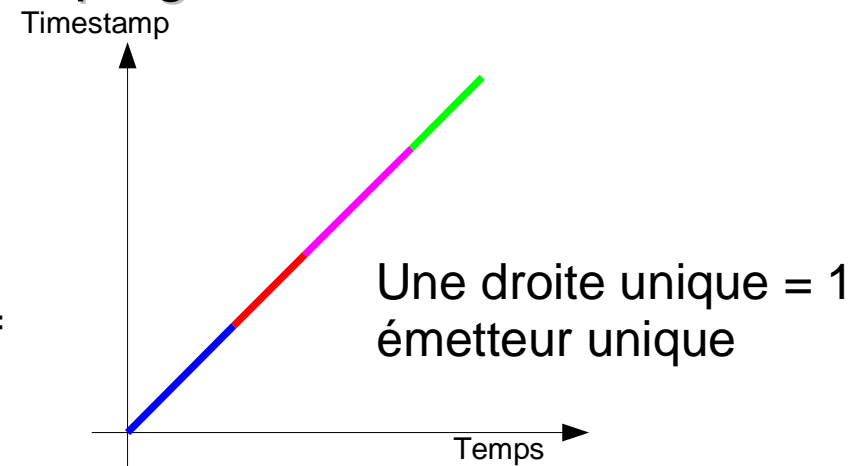
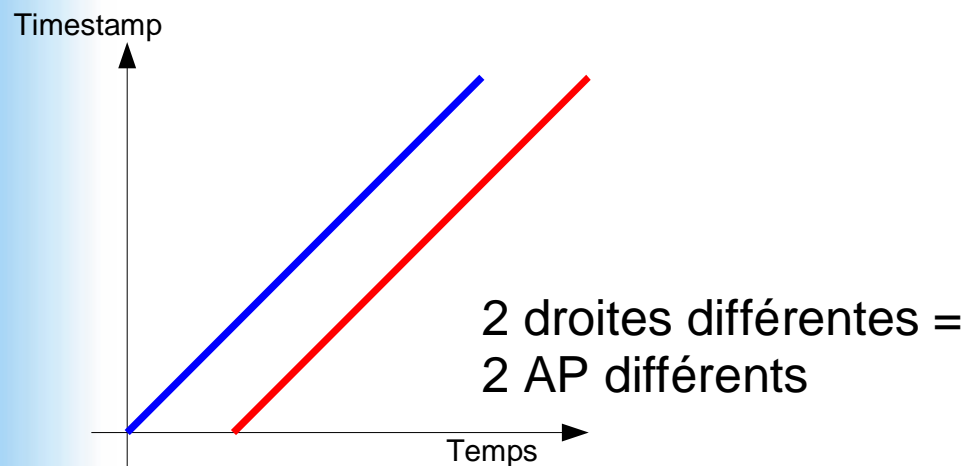
WifiScanner v0.3.0 (Wlan driver version >= 0.14) (c) 2002 Hervé Schauer Consultants (terowe,peggi@hsc-1abs.com)
[AP: 00106125711CB: "" (117,129) Summary
[STA: 00140196133190: "" (0,243)
| AP: 1
| STA: 1
| BECON: 95
| SSID: 0
| Channel: 1
| Invalid: 4
| Created: 6
| Mean: 0
| Last IVI: 2010222
| Packets: 104
| Scan
| 000000001111 1
| 1234567890123 4
| IDS is OFF
-----
Last Updt: 10198102
11/27/2002 10198100,821 "" 11,HeP,AP,414,000,FFFFFFFFFFFFFF,00106125711C,00106125711CB,2Mbps,AP Base (dedicated),Radio only,BECON
11/27/2002 10198100,823 "" 00,HeP,AP,099,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,866 "" 00,HeP,AP,123,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,869 "" 00,HeP,STA,105,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,916 "" 00,HeP,STA,132,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,919 "" 00,HeP,STA,141,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,965 "" 00,HeP,STA,247,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,969 "" 00,HeP,STA,153,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,979 "" 00,HeP,STA,162,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198100,974 "" 00,HeP,AP,117,000,001401961331,00106125711CB,00106125711CB,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198101,022 "" 00,HeP,STA,210,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198101,024 "" 00,HeP,AP,114,000,001401961331,00106125711CB,00106125711CB,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198101,024 "" 00,STA,204,000,00106125711CB,0010010010010010,0010010010010010,4Mbps,Client,Radio only,ACK
11/27/2002 10198101,069 "" 00,HeP,STA,240,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198101,069 "" 00,HeP,AP,117,000,001401961331,00106125711CB,00106125711CB,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198101,076 "" 00,STA,240,000,00106125711CB,0010010010010010,0010010010010010,4Mbps,Client,Radio only,ACK
11/27/2002 10198101,110,MAINEN
11/27/2002 10198101,119 "" 00,STA,111,000,001401961331,0010010010010010,0010010010010010,4Mbps,Client,Radio only,ACK
11/27/2002 10198101,120,MAINEN
11/27/2002 10198101,120 "" 00,STA,240,000,00106125711CB,0010010010010010,0010010010010010,4Mbps,Client,Radio only,ACK
11/27/2002 10198101,121,HSRREQ
11/27/2002 10198101,122 "" 00,STA,111,000,001401961331,0010010010010010,0010010010010010,4Mbps,Client,Radio only,ACK
11/27/2002 10198101,122,HSRRES
11/27/2002 10198101,122 "" 00,STA,243,000,00106125711CB,0010010010010010,0010010010010010,4Mbps,Client,Radio only,ACK
11/27/2002 10198101,216 "" 11,HeP,AP,117,000,FFFFFFFFFFFFFF,00106125711CB,00106125711CB,2Mbps,AP Base (dedicated),Radio only,BECON
11/27/2002 10198101,666 "" 00,HeP,STA,243,000,32323FF32390,0010010010010010,0010010010010010,4Mbps,STA Activity Data to BS,DATA
11/27/2002 10198101,670 "" 00,STA,114,000,001401961331,0010010010010010,0010010010010010,2Mbps,Client,Radio only,ACK
11/27/2002 10198101,769 "" 11,HeP,AP,115,000,FFFFFFFFFFFFFF,00106125711CB,00106125711CB,2Mbps,AP Base (dedicated),Radio only,BECON
11/27/2002 10198102,286 "" 11,HeP,AP,117,000,FFFFFFFFFFFFFF,00106125711CB,00106125711CB,2Mbps,AP Base (dedicated),Radio only,BECON
11/27/2002 10198102,286 "" 00,HeP,STA,114,000,32323FF32390,001401961331,00106125711CB,2Mbps,STA Activity Data From BS,DATA
11/27/2002 10198102,286 "" 00,HeP,STA,243,000,FFFFFFFFFFFFFF,001401961331,FFFFFFFFFFFFFF,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198102,286 "" 00,STA,114,000,001401961331,0010010010010010,0010010010010010,2Mbps,Client,Radio only,ACK
11/27/2002 10198102,286 "" 00,HeP,STA,114,000,32323FF32390,00106125711CB,00106125711CB,4Mbps,STA Activity Data to BS,DATA
11/27/2002 10198102,287 "" 00,STA,240,000,00106125711CB,0010010010010010,0010010010010010,2Mbps,Client,Radio only,ACK
11/27/2002 10198102,287 "" 00,HeP,STA,240,000,00106125711CB,0010010010010010,0010010010010010,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198102,287 "" 00,STA,114,000,001401961331,0010010010010010,0010010010010010,2Mbps,Client,Radio only,ACK
11/27/2002 10198102,287 "" 00,STA,114,000,001401961331,0010010010010010,0010010010010010,4Mbps,Client,Radio only,PREREQ
11/27/2002 10198102,287 "" 00,STA,243,000,32323FF32390,001401961331,00106125711CB,4Mbps,STA Activity Data to BS,DATA
11/27/2002 10198102,287 "" 00,STA,114,000,001401961331,0010010010010010,0010010010010010,2Mbps,Client,Radio only,ACK
11/27/2002 10198102,766 "" 11,HeP,AP,117,000,FFFFFFFFFFFFFF,00106125711CB,00106125711CB,2Mbps,AP Base (dedicated),Radio only,BECON

```



Détection des anomalies

- Étude des variations des champs :
 - TimeStamp
 - Sequence number
- Corrélation
 - Détection d'usurpation d'identité
 - Détection de fausse borne ou piège à *wardriver*





Conclusions

- Existence de beaucoup de logiciels libres pour le Wi-Fi
 - Pour auditer, sécuriser, et travailler
- Un excellent pilote de carte
 - Très paramétrable
- Évolution rapide possible
- Ouverture, transparence du code