Snemanje Wi-Fi prometa

V osnovi gre za dva precej različna pristopa:
A) povežemo se z dostopno točko in snemamo promet od/do svojega računalnika,
B) snemamo ves promet, ki ga sliši naša kartica, ne glede na to, komu je namenjen.

Točka A je dokaj enostavno izvedljiva. Okvirje, ki pridejo od/do računalnika, aplikacije na računalniku (npr. Wireshark) vidijo v enaki obliki, kot okvirje na ožičenem ethernetu. Okvirji torej imajo IEEE 802.3 glavo in rep. Če je komunikacija šifrirana to ne moti, saj oddane okvirje vidimo pred šifriranjem, sprejete pa po dešifriranju.

Točka B je težje izvedljiva. V ožičenem ethernetu kartico enostavno postavimo v promiskuitetni način (sprejemanje vseh paketov ne glede na cilj). V Wi-Fi omrežjih pa to ni dovolj, ker okvirje, ki niso namenjeni nam, kartica zavrže že na nižjem sloju. Da omogočimo zajemanje, moramo kartico postaviti v monitorski način (RFMON). Večina Wi-Fi kartic ne omogoča, da bi bili povezani na dostopno točko in hkrati delovali v monitorskem načinu, zato ne moremo posneti sami sebe. V načinu RFMON Wi-Fi kartica dobljenih okvirjev ne pretvarja v IEEE 802.3 okvirje, zato se ohranita 802.11 glava in rep. Prav tako se ne izvede dešifriranje, zato v primeru šifriranega prometa ne moremo enostavno ugotoviti vsebine.

Opomba glede monitorskega načina

Način RFMON je možen le, če gonilnik za Wi-Fi kartico to funkcijo podpira. Žal so vsi gonilniki v operacijskem sistemu Windows napisani brez te funkcije – z redkimi izjemami, ki pa zahtevajo točno določeno strojno opremo in se težko kupijo. V operacijskem sistemu Linux je snemanje prometa bolj izvedljivo, vendar tudi tam ne deluje čisto z vsako kartico in gonilnikom. Tipično vsi gonilniki komercialnih proizvajalcev (npr. HP-jevi za njihove prenosnike s SUSE Linuxom) nimajo funkcije RFMON. Zato jih moramo nadomestiti z odprtokodnimi, ki pa ne obstajajo za vse modele kartic/prenosnikov. Hkrati so odprtokodni gonilniki pogosto manj zmogljivi/zanesljivi za običajno delo, zato je uporabnik v dilemi, ali je snemanje prometa zanj tako pomembno, da si zaradi tega pokvari dobro delujoč sistem. Lepa rešitev je nakup dodatnega USB ključka (še pred nakupom se prepričamo, da za njega obstaja primeren gonilnik), ki ga potem uporabljamo za snemanje, medtem ko gonilnike za vgrajeno kartico pustimo lepo pri miru. Posebej velja opozoriti, da veliko Wi-Fi kartic deluje na Linuxu tako, da uporabljajo Windows gonilnik. Pri takih karticah lahko v specifikaciji na veliko piše, da podpirajo Linux (saj ga res, a le za običajno delo), pa nam to nič ne pomaga, ker ob uporabi Windows gonilnika snemanje ne bo možno.

Wireshark

Če je Wi-Fi kartica v monitorskem načinu bo Wireshark zajemal ves promet, ki ga ta kartica sliši. To je lahko zelo veliko prometa. Ker je v praksi ves promet šifriran, iz tako na slepo posnete „solate“ prometa le težko kaj izluščimo. Dodatni problem je, da ne moremo nastaviti filtra za zajemanje iz le določenega vmesnika, razen če je promet nešifriran oz. poznamo ključ za šifriranje. Če poznamo ključ za šifriranje, ga vnesemo v meniju Edit → Preferences → Protocols → IEEE 802.11. Izberemo “Enable decryption” in podamo ključ.

Ko je prometa veliko, uporabimo filtre. Ločimo filtriranje med zajemanjem (capture filter) in filtriranje med prikazovanjem zajetega prometa (display filter). Sintaksa je teh dveh primerih različna. Nekaj uporabnih filtrov za zajemanje:
`host 172.18.5.4` (zajemanje prometa le od določenega IP)
`ether host 00:21:00:f2:40:d1` (zajemanje prometa le od določenega MAC)
`link[0] != 0x80` (zajemanje Wi-Fi prometa brez okvirjev Beacon)

Kismet

To je namenski program za snemanje Wi-Fi prometa. V osnovi dela isto, kot Wireshark, le da zna iz zajetega prometa izluščiti več informacij. Že pred snemanjem si lahko ogledamo, kakšni signali so prisotni in tako ugotovimo, če je snemanje za nas sploh zanimivo. Lahko tudi določimo točno določen računalnik in snemamo le promet od/do njega.

Program Kismet je bil leta 2009 prenovljen. Večina spletnih strani še vedno vsebuje opis starega GUI in stare arhitekture. V novi verziji je bolj natančno ločena funkcionalnost strežnika (zbira podatke, imenuje se tudi "Kismet drone") in odjemalca (prikazuje podatke). Strežnik zaženemo z adminstratorskimi pravicami v terminalu z ukazom:

```
sudo kismet_server
```

V konfiguracijski datoteki `/etc/kismet.conf` lahko že prej določimo, na katerem fizičnem vmesniku bo strežnjik poslušal, vendar to ni nujno. To nastavitev lahko naknadno opravimo z odjemalcem.

Odjemalca poženemo z ukazom kismet. Če v konfiguracijski datoteki nč ne spremenimo, se bo povezal na naš lokalni strežnik (lahko bi se kam drugam). Če lokalni strežnik še nima določenega vira podatkov, nas bo najprej pozval, naj vnesemo oznaklo vmesnika. Vnesemo pravo ime (npr. eth0, wlan0, itd.). Strežnik bo potem poskušal navedeni vmesnik postaviti v monitorski način. Dobili bomo obvestilo o neuspehu ali pa bo kismet začel prikazovati promet.

Obićajno kismet začne v načinu *hop*, kar pomeni, da preklaplja med vsemi kanali. Če želimo slediti prometu na enem kanalu, moramo to preklapljanje ustaviti. To storimo tako, da najprej v meniku *Sort* izberemo en vrstni red (katerikoli razen *Auto-fit*) in potem z miško enega izberemo (enojni klik). Nato v meniju Windows izberemo pogled, kaj nas zanima (podatki o omrežju, podatki o uporabnikih, itd.) Za nadaljna navodila glej dokumentacijo na domači strani program kismet (`http://www.kismetwireless.net/`).

Wireless Extension in Wireless Tools

Wireshark, Kismet in večina drugih programov uporabljajo za snemanje Wi-Fi prometa isto kodo, ki je del Linux jedra. Ta koda je bila razvita v okviru projekta, katerega glavni sponzor je bil in je še podjetje HP. Uporabniku viden del te kode je API z imenom **Wireless Extension.** Nekateri gonilniki (predvsem komercialni) za Wi-Fi kartice ne podpirajo Wireless Extension.

Da ne bi za vsako majhno opravilo potrebovali namenskega komplesnega programa kot sta npr. Wireshark in Kismet, je na voljo tudi zbirka preprostih terminalskih orodij z imenom **Wireless Tools**. Tukaj je nekaj primerov uporabe paketa Wireless Tools na sistemu SUSE Linux (pri spremembah nastavitev moramo na začetku ukaza dodati „`sudo`“, saj je potreben administratorski dostop):

Izpis vmesnikov na računalniku (če smo povezani, se izpišejo podatki o povezavi):
`/usr/sbin/iwconfig`

Izpis vseh javnih dostopnih točk, katerih signal sprejemamo:
`/usr/sbin/iwlist wlan0 scan`

Postavimo vmesnik na določen kanal/frekvenco:
`/usr/sbin/iwconfig wlan0 channel 3`

Postavljanje vmesnika v monitorski oz. navadni način:
`/usr/sbin/iwconfig wlan0 mode Monitor`
`/usr/sbin/iwconfig wlan0 mode Managed`

Pri večini kartic je potrebno pred spremembo načina vmesnik najprej onemogočiti, potem pa spet vklopiti. Torej moramo tipično izvesti tri ukaze:
`/sbin/ifconfig wlan0 down` (ali pa „`ip link set wlan0 down`“)
`/usr/sbin/iwconfig wlan0 mode Monitor`
`/sbin/ifconfig wlan0 up` (ali pa „`ip link set wlan0 up`“)

Administracija dostopne točke Cisco Aironet 1130 AG Access Point

V tovarniških nastavitvah dostopna točka nima določene številke IP, zato jo moramo najprej konfigurirati preko vhoda za administracijo oz. konzole (Console). Na konzolo se povežemo preko serijskega porta. Na Linuxu potem poženemo program screen (v našem primeru imamo pretvornik USB na RS-232):

```
sudo screen /dev/ttyUSB0
```

Na dostopni točki je sistem Cisco IOS, zato so ukazi podobni tistim na stikalu in usmerjevalniku.

`>enable` (password je npr. "Cisco")
`#show ip interface brief`
`#configure terminal`
`#interface bvi1`
`#ip address` *`address mask`* (npr. 1.2.3.4 255.255.255.0)

Nastavitve lahko potem nadaljujemo grafično tako, da se na dostopno točko povežemo z brskalnikom (če se moramo avtenticirati poskusimo npr. prazno uporabniško ime in geslo "Cisco").

Če želimo, da dostopna točka omogoča prijavo uporabnikov moramo nujno v meniju EXPRESS SECURITY nastaviti SSID in izbrati vrsto zaščite. Dostopna točka ima lahko hkrati več SSID-jev, ne moremo pa imeti hkrati nezaščitena in zaščitena omrežja. Če želimo, v meniju EXPRESS SETUP nastavimo tudi Host Name, ki ni nujno enak kot SSID.

Pa še nekaj o ožičenem ethernetu in nastavitvah IP

Pri delu z brezžičnimi omrežji potrebujemo tudi nekaj znanja o ožičenih omrežjih in nastavitvah IP (npr. da se preko kabla povežemo na dostopno točko ali usmerjevalnik, da preizkusimo delovanje omrežja itd.). Zato je tukaj še nekaj koristnih Linux ukazov (tudi tukaj za SUSE Linux):

Izpis podatkov o vseh vmesnikih:
`/sbin/ifconfig` (ali pa „`ip link show“ in „ip addr show`“)

Izpis podatkov o ožičenem vmesniku (mrežni kartici):
`/sbin/ethtool eth0`

Nastavitev statične številke IP:
`/sbin/ifconfig eth0 1.2.3.4 netmask 255.255.255.0`
(ali pa „`ip addr add 1.2.3.4/24 brd + dev eth0`“)

Izpis usmerjevalne tabele:
`/sbin/route` (ali pa „`ip route show`“)

Nastavitev privzetega prehoda:

```
/sbin/route add default gw 192.168.1.1 eth0
```

Začasno nastavitev strežnikov DNS na Linuxu najhitreje opravimo tako, da v datoteko `/etc/resolv.conf` dodamo eno ali več vrstic naslednje oblike (komentarje na začetku ne spreminjamo):

```
nameserver 164.8.100.100
```