Snemanje Wi-Fi prometa

V osnovi gre za dva precej različna pristopa:

A) povežemo se z dostopno točko ali drugim računalnikom 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

Ko je Wi-Fi kartica v monitorskem načinu enostavno poženemo Wireshark in ves promet, ki ga ta kartica sliši, se bo zajemal. 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 smo pri snemanju omejeni le na en kanal (frekvenco).

Kismet

To je namenski program za snemanje Wi-Fi prometa. V osnovi dela isto, kot Wireshark, le da omogoča, da lahko hkrati spremljamo promet na vseh kanalih. 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.

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`“)

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`“)