Øving 17 - Wifi

Scan etter trådløse nett

```
madsen@MadsenPc:~/Documents/dataing/TDAT3020 Sikkerhet i programvare og nettverk/ovinger/oving17 - wifi$ nmcli dev wifi
IN-USE  BSSID              SSID           MODE   CHAN  RATE        SIGNAL  BARS  SECURITY
*       88:41:FC:D7:53:59  Romskip        Infra  52    405 Mbit/s  89      ▂▄▆█  WPA2
        00:22:07:72:72:CD  Get-7272CC     Infra  136   540 Mbit/s  62      ▂▄▆_  WPA2
        00:22:07:72:72:CE  Get-2G-7272CC  Infra  6     130 Mbit/s  40      ▂▄__  WPA2
        88:41:FC:D7:54:14  Romskip        Infra  11    130 Mbit/s  32      ▂▄__  WPA2
        44:D4:37:31:4A:6D  Get-314A6C     Infra  136   540 Mbit/s  30      ▂___  WPA2
        08:02:8E:96:4C:9F  NETGEAR88      Infra  13    260 Mbit/s  19      ▂___  WPA2
        88:41:FC:D7:4F:CC  Romskip        Infra  11    130 Mbit/s  0       ____  WPA2
```

Sikkerhetstest

- Kan teste injection
- Kan kjøre besside
- Kan ikke kjøre monitor mode på nettverks kortet

```
madsen@MadsenPc:~$ sudo aireplay-ng --test wlx049226868a88
[sudo] password for madsen:
09:38:34  Trying broadcast probe requests...
09:38:34  Injection is working!
09:38:36  Found 8 APs

09:38:36  Trying directed probe requests...
09:38:36  1E:74:0D:09:3F:B8 - channel: 1 - 'Leilighet5'
09:38:42   0/30:   0%

09:38:42  38:D5:47:21:EA:D0 - channel: 3 - 'ASUS'
09:38:48   0/30:   0%

09:38:48  44:D4:37:31:4A:6E - channel: 6 - 'Get-2G-314A6C'
09:38:54   0/30:   0%

09:38:54  88:41:FC:D7:53:58 - channel: 6 - 'Romskip'
09:39:00   0/30:   0%

09:39:00  00:22:07:72:72:CE - channel: 6 - 'Get-2G-7272CC'
09:39:06   0/30:   0%

09:39:06  88:41:FC:F3:15:05 - channel: 11 - 'YupItsGamerTime'
09:39:12   0/30:   0%

09:39:12  88:41:FC:D7:54:14 - channel: 11 - 'Romskip'
09:39:18   0/30:   0%

09:39:18  5C:E2:8C:F0:E9:48 - channel: 12 - 'Lincoln_'
09:39:24   0/30:   0%
```

```
madsen@MadsenPc:~$ sudo besside-ng -R 'Romskip' wlx049226868a88
[09:40:32] Let's ride
[09:40:32] Logging to besside.log
[09:40:40] TO-OWN [] OWNED []
[09:40:48] TO-OWN [] OWNED []
[09:40:57] TO-OWN [] OWNED []
[09:41:05] TO-OWN [] OWNED []
[09:41:13] TO-OWN [] OWNED []
[09:41:22] TO-OWN [] OWNED []
[09:41:30] TO-OWN [Romskip*, Romskip*, Romskip*] OWNED []
[09:41:31] Crappy connection - Romskip unreachable got 0/10 (100% loss) [-47 dbm]
[09:41:32] Crappy connection - Romskip unreachable got 0/10 (100% loss) [-70 dbm]
[09:41:33] Crappy connection - Romskip unreachable got 0/10 (100% loss) [-86 dbm]
[09:41:41] TO-OWN [] OWNED []
[09:41:49] TO-OWN [] OWNED []
[09:41:57] TO-OWN [] OWNED []
[09:42:06] TO-OWN [] OWNED []
[09:42:14] TO-OWN [] OWNED []
[09:42:22] TO-OWN [Romskip*] OWNED []
[09:42:23] Crappy connection - Romskip unreachable got 0/10 (100% loss) [-86 dbm]
[09:42:31] TO-OWN [] OWNED []
^C9:42:36] - Scanning chan 09
Dying...
[09:42:36] TO-OWN [] OWNED []
```

```
madsen@MadsenPc:~$ sudo airmon-ng stop wlx049226868a88

PHY     Interface       Driver          Chipset

phy0    wlx049226868a88 rtl88x2bu       ASUSTek Computer, Inc. 802.11ac NIC

You already have a wlx049226868a88 device but it is NOT in station mode.
Whatever you did, don't do it again.
Please run "iw wlx049226868a88 del" before attempting to continue
```

```
madsen@MadsenPc:~$ sudo airmon-ng start wlx049226868a88


PHY     Interface       Driver          Chipset

phy0    wlx049226868a88 rtl88x2bu       ASUSTek Computer, Inc. 802.11ac NIC
Interface wlx049226868a88mon is too long for linux so it will be renamed to the old style (wlan#) name.


  ERROR adding monitor mode interface: command failed: Operation not supported (-95)
```