VAJA: WiFi napadi

Namen

Namen te naloge je raziskati različne metode napadov na WiFi omrežja, njihove posebnosti in tehnične zahteve

Uvod

WiFi-ji so pogosta tarča napadov in napade na njih lahko umestimo v kategorijo L2 napadov vendar imajo svoje specifike. Najbolj pogost napad na WiFi je Eviltwin kjer naredimo kopijo legitimnega SSID-ija na katerega se povezujejo tarče. Tak napada je zelo učinkovit vendar je ratal bolj kompleksen saj se naprave privzeto ne povezujejo na SSID-je brez gesla. Bodo pa te napadi postali zelo aktualni v WiFi 6e kjer je možno uporabljati šifrirano povezavo brez gesla. Napade lahko tudi razdelim v naslednji dve kategoriji.

- Napadi na WiFi omrežja z »domačo« zaščito (PSK)
- Napadi na poslovna WiFi omrežja (Radius auth)

Naloge:

1. Razbijanje WPA/WPA2 gesel

Pri tem napadu je ključ pridobivanje gesla iz »handshaka«, ki poteka med dostopovno točko ter napravo. Napad je zelo učinkovit če več naprav uporablja enako dostopovno točko, vendar pa zavisi od uporabe slovnice proti kateri primerjamo gesla (večina slovnic je angleških). Orodje za napad se imenuje aircrack-ng.

V prvem koraku z ukazom airmon-ng preverimo vse adapterje, ki obstajajo na naši Kali napravi. Nato sledimo naslednjim korakom.

- Vmesnik postavimo v »monitor« način z ukazom `airmon-ng start <vmesnik>`
- Vse vidne dostopne točke pregledamo z ukazom `airodump-ng <vmesnik>`
- Začnemo z zajemom prometa `airodump-ng -c <kanal> --bssid <bss> -w <pot za pcap datoteke>`

Ko začnemo spremljati promet se moramo odločiti za tip deauth napada. Deauth sporočila lahko pošiljamo neposredno na dostopovno točko ali pa na napravo, ki uporablja dostopovno točko.

```
aireplay-ng –deauth 0 – a <bssid> <vmesnik>
```

Prvi korak napada bo uspešen, ko bomo prestregli EAPOL sporočilo, ki vsebuje handshke. Nato moramo le še pridobiti geslo v plaintext obliki.

```
aircrack-ng -w <pot do slovice> <pot do pcap datoteke>
```

2. Wifi Pineapple Eviltwin

Wifi Pineapple je hak5 naprava, ki jo lahko vsaka oseba kupi. Naprava podpira več funkcionalnosti in dodatne razširitve vendar je v osnovni dostopovna točka, ki omogoča kloniranje SSID-jov.

- Ko se naprava prižge, lahko do nje dostopamo preko GUI-ja
- Omrežje preskeniramo, da odkrijemo vse dostopovne točke v območju
- Kloniramo PSK dostopovno točko ali pa Radius dostopovno točko
- Spremljamo promet
- Naprave lahko tudi deavtenticiramo.