Az **Aircrack-ng** egy nyílt forráskódú, parancssoros vezeték nélküli hálózatbiztonsági programcsomag, amellyel WEP, WPA és WPA2 hálózatok tesztelhetők és törhetők fel. A folyamat alapja a hálózati adatforgalom figyelése, a kliensek lecsatlakoztatása a WPA "handshake" (kézfogás) megszerzéséhez, majd a jelszó visszafejtése egy szótárfájl (wordlist) segítségével.

Szükséges eszközök

- **Monitor mód kompatibilis Wi-Fi kártya**: Olyan hálózati kártya, amely támogatja a csomagbefecskendezést (packet injection) és a monitor módot.
- **Kali Linux vagy Aircrack-ng csomag**: Telepíthető a `sudo apt install aircrack-ng` paranccsal.
- **Szótárfájl (Wordlist)**: Egy `.txt` fájl, amely a lehetséges jelszavakat tartalmazza (pl. a beépített `rockyou.txt`).

A Wi-Fi feltörés lépései (WPA/WPA2)

1. Monitor mód bekapcsolása

Első lépésként a Wi-Fi kártyát megfigyelő (monitor) módba kell állítani, hogy lássa az összes környező adatforgalmat.

bash

```
sudo airmon-ng start wlan0
```

Körültekintően használja a kódot.

(Megjegyzés: A parancs létrehoz egy új interfészt, általában `wlan0mon` néven).

2. Környező hálózatok pásztázása

Keressük meg a célpont hálózatot és annak adatait (BSSID/MAC cím, Csatorna).

bash

```
sudo airodump-ng wlan0mon
```

Körültekintően használja a kódot.

A listából jegyezzük fel a célpont **BSSID**-jét (pl. `00:11:22:33:44:55`) és a csatorna számát (**CH**, pl. `6`). A futást a `Ctrl+C` gombokkal tudjuk leállítani.

3. Célzott adatgyűjtés és Handshake elfogása

Indítsunk el egy célzott rögzítést a kiválasztott csatornán, hogy elkapjuk a hálózathoz csatlakozó eszközök közötti 4-utas kézfogást (4-way handshake).

```bash
sudo airodump-ng -c 6 --bssid 00:11:22:33:44:55 -w hack_adatok wlan0mon
```

Körültekintően használja a kódot.

A terminált hagyjuk futni. A jobb felső sarokban kell majd megjelennie a `WPA handshake: ...` feliratnak.

4. Kliens lecsatlakoztatása (Dehitelesítés)

Ha nincs aktív csatlakozás, nem tudjuk elkapni a kézfogást. Egy új terminálablakban küldjünk dehitelesítő (deauth) csomagokat a hálózatnak, ami ideiglenesen ledob egy klienst. Amikor az eszköz automatikusan visszacsatlakozik, az előző ablakban futó `airodump-ng` rögzíti a kézfogást.

```bash
sudo aireplay-ng -0 5 -a 00:11:22:33:44:55 wlan0mon
```

Körültekintően használja a kódot.

(A `-0 5` paraméter 5 darab lecsatlakoztatási kísérletet jelent).

5. A jelszó visszafejtése (Cracking)

Miután az `airodump-ng` ablakában megjelent a sikeres handshake üzenet, leállíthatjuk a rögzítést. A jelszó feltörését a kimentett `.cap` kiterjesztésű fájllal és a saját szótárfájlunkkal indíthatjuk el:

```bash
aircrack-ng -w szotar.txt -b 00:11:22:33:44:55 hack_adatok-01.cap
```

Körültekintően használja a kódot.

Ha a jelszó szerepel a `szotar.txt` fájlban, az Aircrack-ng sikeresen kiírja azt a képernyőre.

Jognyilatkozat és Figyelmeztetés

Idegen vagy engedély nélküli vezeték nélküli hálózatok tesztelése, megfigyelése vagy feltörése **illegális és bűncselekménynek minősül**. Ez a leírás kizárólag saját tulajdonú hálózatok biztonsági ellenőrzésére (penetration testing), illetve oktatási célból használható.