Słabe strony sieci WiFI

Dziś sieci bezprzewodowe stają się coraz bardziej popularniejsze. Do ich sukcesu przyczynia się przede wszystkim; stosunkowo niewielki koszt urządzeń, prosta rozbudowa (brak konieczności ciągnięcia wielu kabli, wykonywania przewiertów, itp.) oraz prosta konfiguracja. Należy jednak pamiętać, że z korzystaniem z sieci WiFi wiążą się niestety zagrożenia wykradania danych lub włamywania do sieci.

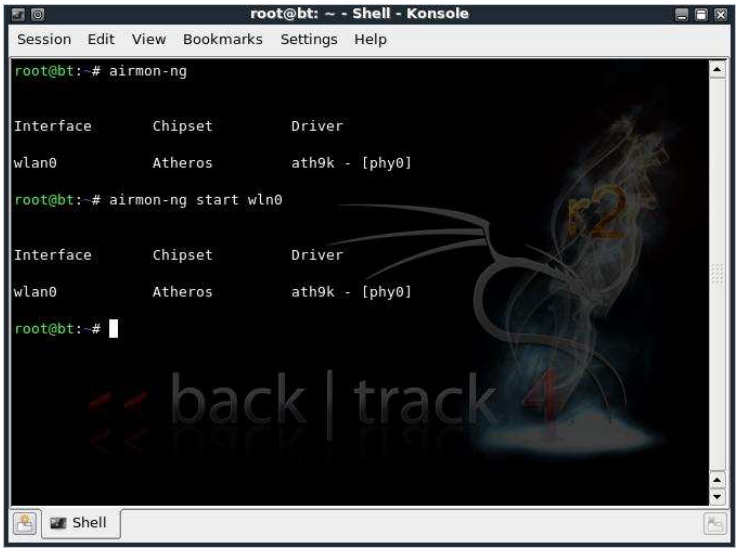
Najpopularniejszym, bo maso stosowanym rozwiązaniem w sieciach bezprzewodowych jest standard 802.11 b,g,n działający na zasadzie rozsyłania fal radiowych w częstotliwościach 2,4 MHZ do 2,48MHz. Sieć taka w zależności od zastosowanego standardu b,g,n może działać z prędkością od 11Mb/s do ponad 100MB/s. W związku z tym że sygnał rozsyłany jest w eterze w sposób dookólny istnieje bardzo duże prawdopodobieństwo, że jakaś niepowołana osoba będzie chciała przechwycić transmisje naszych danych i w ten sposób wykraść poufne informacje.

Dziś chciałbym przedstawić dwie sytuacje potencjalnie niebezpieczne: 1 wykradanie poufnych danych z sieci WIFi która nie została zabezpieczona i 2 włamanie do sieci WIFi która została zabezpieczona słabym kluczem szyfrującym WEP.

Do naszego eksperymentu potrzebujemy Router Bezprzewodowy, dzięki któremu stworzymy sieć WiFi, laptop kliencki np. z system XP ,który będzie łączył się z siecią pobierał jakieś dane, oraz laptop z kartą WiFi i system Linux (w naszym wypadku będzie to dystrybucja BackTrack4)

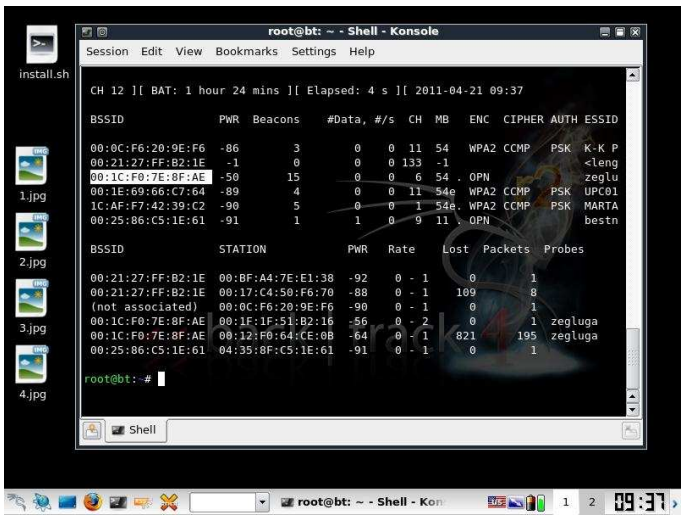
Wypływanie poufnych danych z sieci niezabezpieczonych

1. Na komputerze którego zadaniem ma być przechwytywanie danych uruchamiamy program **airmon-ng** , który przestawia kartę WiFi w tryb tzw. „Monitora”, dzięki czemu bez podłączania do konkretnej sieci jesteśmy w stanie monitorować ruch pakietów w eterze.

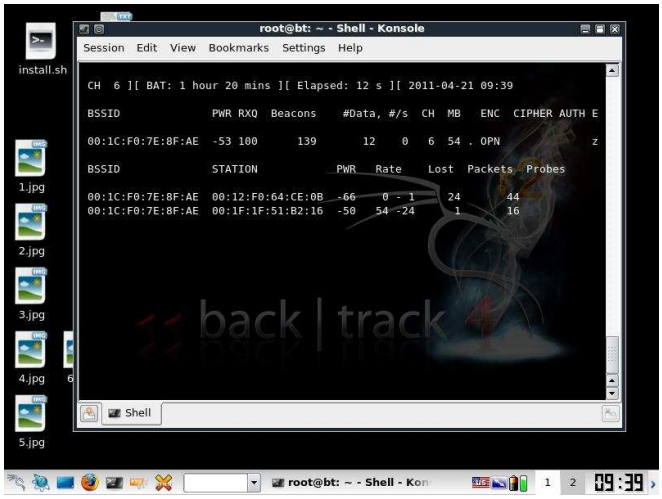


2. Poleceniem **airodump-ng** skanujemy dostępne kanały sieci bezprzewodowych otrzymując w rezultacie jakie sieci bezprzewodowe znajdują się w naszym zasięgu. Dodatkowo otrzymujemy informację o tzw BSSID sieci – czyli MAC adres punktu dostępu, CH kanał na którym działa sieć, SSID – nazwę sieci, ENC – rodzaj zastosowanego szyfrowania w sieci itd.

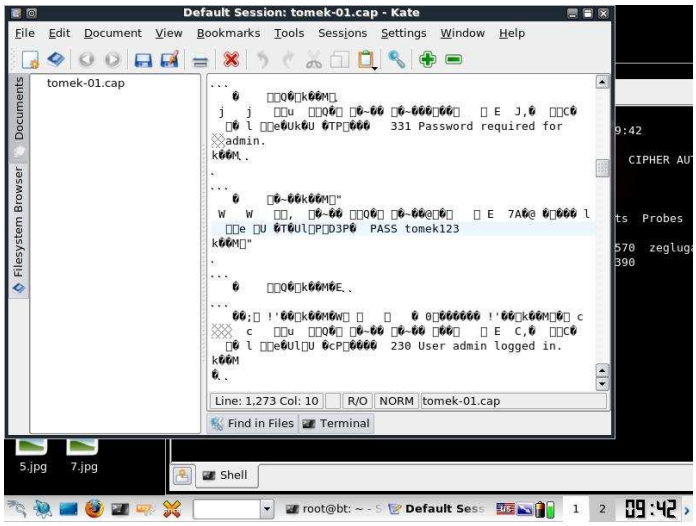
   Wybieramy sieć zegluga, która jest niezabezpieczona OPN (open) i kopiujemy BSSID tej sieci.



3. Poleceniem **airodump-ng –c 6 –w tomek --bssid 00:1C:F0:7E:8F:AE mon0** nakazujemy by nasza karta bezprzewodowa, która pracuje w trybie monitora przechwytywała pakiety wysyłane pomiędzy klientem pracującym na systemie XP, a dostępowym punktem bezprzewodowym. –c 6 – oznacza że nasłuchujemy na kanale 6, -w tomek – przechwycone dane zostaną zapisane do pliku o nazwie „tomek…”; **--bssid 00:1C:F0:7E:8F:AE –** oznacza że przechwytujemy wszystkie pakiety kierowane do sieci o tej nazwie (MAC adres karty sieciowej punktu dostępowego, która obsługuje cały ruch sieci bezprzewodowej), **mon0 –** podajemy nazwę karty sieciowej która pełni funkcje monitora i ma przechwytywać dane z eteru.



4. Teraz wystarczy jedynie przeanalizować plik „tomek…” i poszukać w nim wrażliwych danych np. haseł loginów itp. Inf, które zostały przesłane w sieci przez innych użytkowników w sposób niezaszyfrowany. **Uwaga!!!** należy wystrzegać się przesyłania danych wrażliwych w sposób niezaszyfrowany, ponieważ są one przesyłane w sieci w postaci jawnego tekstu. Należy unikać łączenia się z nieznanymi niezabezpieczonymi sieciami WiFi – niejednokrotnie może być to pułapka zastawiona przez hackerów celem wyłudzenia poufnych informacji. Z punktu widzenia prawa nielegalnym jest łączenie się z otwartymi sieciami bezprzewodowymi. W końcu fakt, że nie zamykamy drzwi na klucz nie stanowi zaproszenia do wejścia do naszego domu dla wszystkich – nawet najbardziej przypadkowych ludzi.



Testowanie bezpieczeństwa sieci zabezpieczonej kluczem WEP

Podstawowym środkiem bezpieczeństwa w standardzie 802.11 jest protokół warstwy łącza danych WEP (ang. Wired Equivalent Privacy), który - zgodnie z nazwą - zapewnić ma sieci bezprzewodowej bezpieczeństwo nie gorsze niż na poziomie standardowego bezpieczeństwa przewodowej sieci LAN. Standardowym poziomem bezpieczeństwa w sieciach przewodowych jest brak jakichkolwiek mechanizmów zabezpieczających, więc zadanie postawione przed protokołem WEP nie jest specjalnie wygórowane i pomimo że w 2001 roku opublikowano już sposób jego złamania to i tak jest on wykorzystywany w większości sieci.

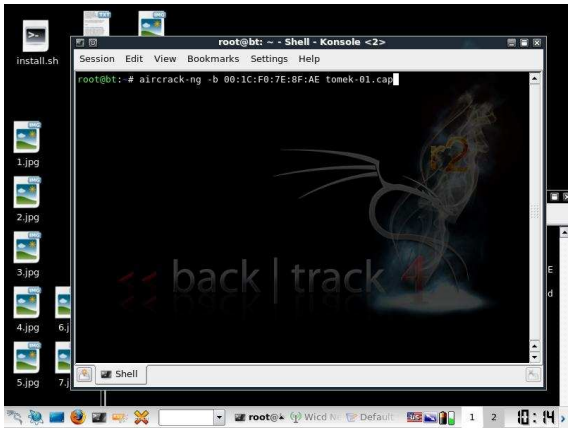
Zasada działania

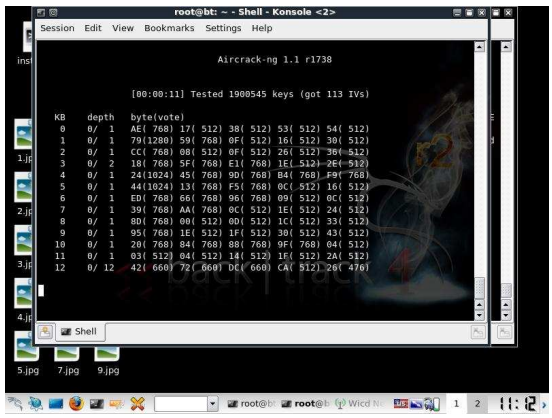
Szyfrowanie w mechanizmie WEP odbywa się w oparciu o szyfr strumieniowy RC4 znany też jako ARC4 lub ARCFOUR. Algorytm RC4 został opracowany przez Ronalda Rivesta w 1987 roku i pozostawał utrzymany w tajemnicy aż do roku 1994, kiedy to został opublikowany w Internecie na jednej z grup dyskusyjnych. Algorytm generuje strumień kluczy, który jest poddawany operacji XOR z zawartością tekstu wejściowego. Algorytm ten oprócz sieci bezprzewodowych stosowany jest w wielu innych produktach, takich jak Lotus, Oracle a także SSL i SSH. Algorytm RC4 dla szyfrowania WEP wybrany został z tego powodu, że jest stosunkowo prosty i szybki w działaniu i nie spowalnia działania sieci w taki sposób jak inne bardziej skomplikowane algorytmy.

Słabe strony WEP:

- brak zarządzania i dystrybucji kluczy,
- brak wzajemnego uwierzytelniania,
- długość i sposób generowania wektora IV (co pewien czas ramki szyfrowane są tym samym kluczem szyfrującym, co umożliwia osobom niepowołanym ustalenie klucza tajnego WEP i w konsekwencji dostęp do danych – pamiętamy, że wektor IV jest przesyłany jawnie);
- wraz ze wzrostem długości klucza zwiększa się liczba danych, które są przesyłane w celu zabezpieczenia transmisji, skutkuje to zmniejszeniem wydajności sieci,
- obecność „słabych kluczy" (ze względu na sposób tworzenia klucza szyfrującego, pojawiają się klucze dla których układ bitów w pierwszych 3 bajtach powoduje pojawienie się podobnych układów w pierwszych bajtach ciągu szyfrującego), umożliwia to szybsze łamanie klucza WEP (co staje sie jeszcze łatwiejsze przy wykorzystaniu narzędzi do wstrzykiwania pakietów i generowania sztucznego ruchu, pomocnego w szybszym zgromadzeniu pakietów).

1. By przetestować bezpieczeństwo sieci WiF gdzie zastosowano do szyfrowania klucz WEP należy wykonać dokładnie te same kroki które opisałem do pkt 4 powyżej. Gdy nasza karta sieciowa pracująca w trybie monitora przechwytuje dane zapisując je do pliku np.: „tomek…" należy w następnej kolejności użyć narzędzia (**aircrack-ng**), które przeanalizuje zgromadzone dane – a właściwie porówna klucze i vektory inicjujące (IV) szukając w nich słabych punktów mogących zdradzić hasło do zabezpieczonej sieci. By całe zadanie zakończyło się sukcesem należy zgromadzić dość spora ilość danych. Zasada jest prosta im większy jest ruch w sieci tym szybciej uda nam się odgadnąć hasło ☺. Powodzenia.





Materiał opracował:
Tomasz Marenin
tmarenin@wodip.opole.pl