

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

Wi-Foo. Sekrety bezprzewodowych sieci komputerowych

Autorzy: Andrew Vladimirov, Konstantin
V. Gavrilenko, Andrei A. Mikhailovsky
Tłumaczenie: Rafał Szpoton, Witold Ziolo
ISBN: 83-7361-921-6

Tytuł oryginału: [Wi-Foo: The Secrets of Wireless Hacking](#)

Format: B5, stron: 520



Sieci bezprzewodowe stają się coraz popularniejsze. Wszędzie tam, gdzie instalowanie okablowania jest nieoptyczne, niemożliwe lub po prostu niewygodne, możemy zastosować technologie bezprzewodowe. Na rynku dostępnych jest wiele urządzeń umożliwiających szybkie i proste stworzenie sieci bezprzewodowej. Jednak sieć bezprzewodowa jest bardziej niż tradycyjna sieć „przewodowa” narażona na ataki hakerów. Oczywiście istnieją mechanizmy zabezpieczania takich sieci, lecz wykorzystanie ich wymaga poznania nie tylko ich możliwości, ale także technik stosowanych przez osoby włamujące się do sieci.

„Wi-Foo. Sekrety bezprzewodowych sieci komputerowych” to książka opisująca wszystkie zagadnienia związane z bezpieczeństwem sieci bezprzewodowych. Czytając ją, dowiesz się, jakich sposobów używają hakerzy włamując się do sieci, i nauczysz się zapobiegać ich atakom. Zbadasz słabe punkty sieci bezprzewodowej, wykorzystując do tego celu zestaw opisanych w książce narzędzi, i zaimplementujesz mechanizmy obrony sieci. Poznasz też sposoby wykrywania włamań do sieci bezprzewodowej i systemy, jakie możesz wykorzystać do „namierzenia” hakerów.

- Osprzęt sieciowy i konfiguracja sieci
- Wykrywanie sieci bezprzewodowych
- Narzędzia do łamania haseł
- Techniki włamań do sieci
- Założenia polityki bezpieczeństwa w sieciach bezprzewodowych
- Kryptografia i szyfrowanie informacji
- Metody uwierzytelniania użytkowników sieci
- Bezprzewodowe sieci VPN
- Systemy wykrywania intruzów w sieciach bezprzewodowych

Poznaj sposoby działania hakerów i zbuduj mechanizmy, dzięki którym Twoja sieć bezprzewodowa będzie bezpieczna.



Spis treści

O Autorach	11
Wstęp	13
Rozdział 1. Bezpieczeństwo sieci bezprzewodowych w praktyce	21
Dlaczego skupiamy się na bezpieczeństwie sieci 802.11?	22
Smutna rzeczywistość: szeroko otwarte sieci 802.11 wokół nas	25
Przyszłość bezpieczeństwa sieci 802.11 — czy aby na pewno taka jasna?	26
Podsumowanie	28
Rozdział 2. W stanie obłączenia	29
Dlaczego ktoś czyha na Twoją bezprzewodową sieć?	29
Kim są bezprzewodowi krakerzy?	32
Potencjalne cele: korporacje, małe firmy, sieci domowe	34
Sam sobie celem: testy penetracyjne jako pierwsza linia obrony	37
Podsumowanie	39
Rozdział 3. Przygotowanie sprzętu. Urządzenia sieci 802.11	41
Palmtopy a laptopy	41
Karty bezprzewodowe PCMCIA i CF	43
Wybór lub ocena chipsetu karty sieciowej klienta	43
Anteny	52
Wzmacniacze antenowe	55
Kable i złącza antenowe	55
Podsumowanie	56
Rozdział 4. Uruchomienie sprzętu. Sterowniki i narzędzia sieci 802.11	57
Systemy operacyjne, oprogramowanie otwarte i oprogramowanie zamknięte	57
Chipsety, sterowniki i polecenia	58
Uruchomienie karty sieciowej w systemach Linux i BSD	59
Poprawna konfiguracja kart bezprzewodowych	67
Narzędzia Linux Wireless Extensions	67
Narzędzia linux-wlan-ng	74
Konfigurowanie kart Cisco Aironet	76
Konfigurowanie kart bezprzewodowych w systemach BSD	79
Podsumowanie	80
Rozdział 5. Polowanie na sieci oraz prowadzenie rekonesansu	81
Wykrywanie sieci bezprzewodowych za pomocą skanowania aktywnego	82
Narzędzia wykrywania sieci oraz analizy ruchu działające w trybie monitorowania	85
Kismet	85
Wellenreiter	94

Airtraf	94
Gtkskan	97
Airfart	97
Mognet	98
WifiScanner	99
Inne programy i skrypty wiersza poleceń	101
Narzędzia wykrywania sieci oraz rejestrowania ruchu dla systemów BSD	106
Narzędzia korzystające z programu iwlist z opcją scan	109
Narzędzia mierzące natężenie sygnału radiowego	111
Podsumowanie	113
Rozdział 6. Budowanie arsenału. Narzędzia specjalistyczne	115
Narzędzia służące do łamania szyfrów	116
Narzędzia łamiące zabezpieczenie WEP	117
Narzędzia wykradające klucze WEP przechowywane w komputerach	123
Narzędzia wprowadzające do sieci ruch umożliwiające szybsze złamanie zabezpieczenia WEP	124
Narzędzia atakujące systemy uwierzytelniania 802.1x	125
Narzędzia służące do generowania ramek sieci bezprzewodowych	127
AirJack	128
File2air	130
Libwlan	131
FakeAP	133
Void11	134
Wnet	135
Wprowadzanie do sieci zaszyfrowanego ruchu za pomocą programu Wepwedgie	137
Narzędzia do zarządzania punktami dostępowymi	141
Podsumowanie	144
Rozdział 7. Planowanie ataku	145
Zestaw urządzeń i narzędzi	145
Szukanie śladów sieci	147
Rodzaje i planowanie rekonesansu	149
Planowanie czasu ataku i oszczędzanie baterii	152
Ukrywanie się podczas prowadzenia testów penetracyjnych	153
Czynności wykonywane podczas ataku	154
Podsumowanie	155
Rozdział 8. Włamanie	157
Najłatwiejszy sposób włamania	157
Niski płot do przeskoczenia: odkrycie identyfikatora ESSID oraz ominięcie filtrów adresów MAC i filtrów protokołów	159
Zerwanie słabej kłódki: różne sposoby łamania zabezpieczenia WEP	162
Siłowe ataki na WEP	163
Atak FMS	164
Udoskonalony atak FMS	165
Zerwanie słabej kłódki w mniej trywialny sposób: przyspieszanie łamania WEP przez wprowadzanie ruchu do sieci	169
Kilka spostrzeżeń związanych z łamaniem zabezpieczenia WEP	169
Nowe zagrożenie: łamanie zabezpieczenia TKIP	170
Podstępne ramki: ataki man in the middle oraz fałszywe punkty dostępowe	172
Zrób to sam. Wykorzystanie fałszywych punktów dostępowych w testach penetracyjnych	173
Niewielka skuteczność — ataki man in the middle na warstwę fizyczną	178
Bezprzewodowy phishing: połączone ataki man in the middle	179

Włamanie do zabezpieczonego sejfu	180
Wyważenie drzwi: ataki na systemy uwierzytelniania	181
Wejście w tunel: ataki na sieci VPN	185
Ostatnia deska ratunku: bezprzewodowe ataki DoS	191
Ataki na warstwę fizyczną, czyli zagłuszanie	191
Zasypanywanie sieci ramkami zrywającymi skojarzenie i uwierzytelnienie	192
Atak za pomocą sfałszowanych i zmodyfikowanych ramek żądania uwierzytelnienia	193
Wypełnienie buforów punktu dostępowego	193
Usuwanie ramek	194
Ataki DoS wykorzystujące podstawowe mechanizmy sieci bezprzewodowych	194
Ataki na implementacje 802.11i	195
Podsumowanie	195
Rozdział 9. Łupienie i plądrowanie. Nieprzyjaciel wewnątrz	197
Krok 1. Analiza ruchu sieciowego	198
Ramki 802.11	198
Transmisje otwartym tekstem oraz protokoły uwierzytelniające	198
Protokoły sieciowe o znanych lukach w bezpieczeństwie	201
Protokoły DHCP, routingu oraz protokoły zapewniające odporność bram na awarie	201
Dane protokołów Syslog oraz NTP	202
Protokoły, których w ogóle nie powinno być w sieci	203
Krok 2. Połączenie się z siecią WLAN i wykrycie snifferów	203
Krok 3. Pasywna identyfikacja komputerów i systemów operacyjnych	205
Krok 4. Wykrycie i wykorzystanie luk w komputerach sieci bezprzewodowych	207
Krok 5. Atak na sieć kablową	209
Krok 6. Badanie filtrowania na wyjściu z sieci bezprzewodowej do kablowej	214
Podsumowanie	216
Rozdział 10. Budowanie twierdzy. Wprowadzenie	
do obrony sieci bezprzewodowych	217
Polityka bezpieczeństwa sieci bezprzewodowych. Fundamentalne założenia	217
Dopuszczanie, rejestracja, aktualizacja oraz monitorowanie urządzeń	218
Szkolenie oraz odpowiedzialność użytkowników	218
Bezpieczeństwo fizyczne	219
Bezpieczeństwo warstwy fizycznej	219
Budowa i konfiguracja sieci	219
Środki profilaktyczne	219
Monitorowanie sieci oraz reakcja na incydent	220
Audyty bezpieczeństwa sieci	220
Podstawy bezpieczeństwa sieci bezprzewodowych w warstwie pierwszej	221
Stosowanie zabezpieczenia WEP, zamkniętych ESSID, filtrowania MAC oraz przekazywania SSH	224
Bezpieczne miejsce dla sieci bezprzewodowej a sieci wirtualne	226
Zwiększenie bezpieczeństwa sieci bezprzewodowych za pomocą przełączników Catalyst oraz punktów dostępowych Aironet firmy Cisco	227
Wzmocniona brama bezprzewodowa oparta na systemie Linux	230
Firmowe rozszerzenia mechanizmu WEP	236
Nowa nadzieja: standardy 802.11i oraz WPA	238
Wystawienie straży. Protokół 802.1x	239
Załatanie dziury. Mechanizmy TKIP i CCMP	241
Podsumowanie	243

Rozdział 11. Podstawy kryptografii. Szyfry symetryczne	245
Podstawy kryptografii oraz steganografii	246
Tryby działania oraz struktury nowoczesnych szyfrów	252
Klasyczny przykład: analiza algorytmu DES	252
Reguła Kerckhoffa oraz tajność szyfru	255
Elementarz 802.11i: szyfr wspomagający inny szyfr	257
Podstawy trybów działania szyfrów	260
Bit po bicie: szyfry strumieniowe oraz bezpieczeństwo sieci bezprzewodowych	263
Dążenie do AES	265
AES (Rijndael)	268
MARS	271
RC6	272
Twofish	274
Serpent	277
Pomiędzy DES a AES. Popularne szyfry okresu przejściowego	280
3DES	280
Blowfish	280
IDEA	282
Wybór szyfru symetrycznego odpowiedniego dla potrzeb sieci komputerowej lub programu	285
Podsumowanie	289
Rozdział 12. Ochrona spójności danych kryptograficznych, wymiana kluczy oraz mechanizmy uwierzytelniania użytkowników	291
Kryptograficzne funkcje mieszające	292
Szczegółowa analiza przykładu standardowej jednokierunkowej funkcji mieszającej	293
Funkcje mieszające, ich osiągi i HMAC-i	296
MIC — słabszy, ale szybszy	297
Kryptografia asymetryczna — prawdziwa bestia	300
Przykłady szyfrów asymetrycznych: ElGamal, RSA oraz krzywe eliptyczne (ang. Elliptic Curves)	301
Praktyczne wykorzystanie kryptografii asymetrycznej: dystrybucja klucza, uwierzytelnianie i podpisy cyfrowe	304
Podsumowanie	307
Rozdział 13. Bramy fortecy. Uwierzytelnianie użytkownika a bezpieczeństwo sieci bezprzewodowych	309
Protokół RADIUS	309
Podstawy modelu AAA	310
Podstawy protokołu RADIUS	311
Właściwości protokołu RADIUS	311
Formaty pakietów	312
Rodzaje pakietów	313
Instalacja programu FreeRADIUS	313
Konfiguracja	315
Rozliczanie użytkowników	319
Luki w protokole RADIUS	320
Atak z wykorzystaniem ciągu uwierzytelniającego z odpowiedzi	320
Atak na współdzielony sekret w oparciu o atrybut hasła	321
Atak w oparciu o hasło użytkownika	321
Ataki w oparciu o ciąg uwierzytelniający żądania	321
Powtórzenie odpowiedzi serwera	321
Problemy ze współdzielonym sekretem	322

Inne narzędzia współpracujące z protokołem RADIUS	322
802.1x: brama do bezprzewodowej fortecy	323
Podstawy protokołu EAP-TLS	324
Integracja z serwerem FreeRADIUS	327
Klienci	329
Przykład konfiguracji punktu dostępowego: Orinoco AP-2000	334
LDAP	335
Podstawy	335
Instalacja OpenLDAP	338
Konfiguracja OpenLDAP	340
Testowanie LDAP	343
Wypełnianie bazy danych LDAP	345
Centralizowanie uwierzytelniania za pomocą LDAP	347
Użytkownicy mobilni a LDAP	352
Narzędzia związane z LDAP	353
NoCat — alternatywna metoda bezprzewodowego uwierzytelniania użytkowników	356
Instalacja i konfiguracja bramki NoCat	357
Instalacja i konfiguracja serwera uwierzytelniania	358
Podsumowanie	359

Rozdział 14. Ochrona fal radiowych. Tworzenie bezprzewodowych sieci VPN 361

Co skłania do instalacji VPN?	363
Przegląd topologii VPN z perspektywy rozwiązań bezprzewodowych	364
Połączenie sieci z siecią	364
Połączenie serwera z siecią	365
Połączenie serwera z serwerem	366
Gwiazda	367
Krata	368
Popularne protokoły VPN oraz protokoły tunelujące	369
IPSec	369
PPTP	369
GRE	370
L2TP	370
Alternatywne implementacje VPN	371
cIpe	371
OpenVPN	371
VTun	372
Protokoły IPSec — przegląd trybów oraz podstawy działania	372
Skojarzenia zabezpieczeń	373
AH	373
ESP	375
Kompresja IP	376
Protokół zarządzania oraz wymiany kluczy IPSec	376
IKE	376
Doskonałe utajnienie przekazywania	379
Wykrywanie martwych partnerów	379
Utrudnienia w stosowaniu IPSec	379
Szyfrowanie oportunistyczne	379
Tworzenie osiągalnych rozwiązań VPN IPSec przy użyciu FreeS/WAN	380
Kompilacja FreeS/WAN	380
Konfiguracja FreeS/WAN	385
Ustawienia dla topologii VPN połączenia sieci z siecią	389
Ustawienia dla topologii VPN połączenia serwera z siecią	391

Konfiguracja klienta w systemie Windows 2000	393
Konfiguracja klienta IPSec w systemie Windows 2000	397
Podsumowanie	405
Rozdział 15. Kontrywiad — bezprzewodowe systemy IDS	407
Klasyfikacja podejrzanych zdarzeń w sieci WLAN	409
1. Zdarzenia w fizycznej warstwie RF	409
2. Zdarzenia dotyczące ramek zarządzających i kontrolnych	409
3. Zdarzenia dotyczące ramek 802.1x/EAP	410
4. Zdarzenia związane z WEP	411
5. Zdarzenia dotyczące ogólnego strumienia połączeń i ruchu	411
6. Inne zdarzenia	411
Przykłady i analiza popularnych sygnatur ataków bezprzewodowych	412
Uruchomić radary! Wdrażanie rozwiązań bezprzewodowych systemów IDS	
w sieci WLAN	417
Komercyjne bezprzewodowe systemy IDS	418
Ustawianie i konfiguracja bezprzewodowych systemów IDS typu open source	419
Kilka uwag dotyczących konstruowania sensorów DIY	
bezprzewodowych systemów IDS	422
Podsumowanie	426
Posłowie	426
Dodatek A Tabela konwersji decybel – wat	427
Dodatek B Urządzenia bezprzewodowe zgodne ze standardem 802.11	431
Dodatek C Charakterystyka promieniowania anten	437
Anteny dookólne	437
Anteny półkierunkowe	438
Anteny kierunkowe	440
Dodatek D Dokumentacja narzędzi dla sieci bezprzewodowych	443
1. Iwconfig	443
Parametry	444
Wyświetlane informacje	449
2. Iwpriv	450
Parametry	450
Wyświetlane informacje	451
3. Iwlist	451
Parametry	452
4. Wicontrol	453
Parametry	454
5. Ancontrol	458
Parametry	459
Dodatek E Zanik sygnału w zależności od typu przeszkody	467
Dodatek F Znaki naznaczonego dostępu	469
Znaki oryginalne	469
Proponowane nowe znaki	470
Dodatek G Szablon czynności testowych do kontroli	
 penetracji sieci bezprzewodowej	471
Szablon czynności testowych do kontroli bezpieczeństwa oraz stabilności	
sieci bezprzewodowej opracowany przez firmę Arhont	471
1. Cel przeprowadzenia kontroli	471
2. Wywiad wstępny	472

3. Przegląd instalacji sieci bezprzewodowej	472
4. Istniejące zabezpieczenia sieci	475
5. Wykryte problemy (anomalie) w badanej sieci	478
6. Procedura testowa penetracji sieci bezprzewodowej	482
7. Ostateczne zalecenia	486
Dodatek H Domyślne identyfikatory SSID dla niektórych popularnych produktów 802.11	487
Słownik	491
Skorowidz	503

Rozdział 7.

Planowanie ataku

Planując inteligentnie, można pokrzyżować komuś wszystkie zamiary.

Wang Xi

Większość książek o bezpieczeństwie systemów informatycznych po zaprezentowaniu listy dostępnych narzędzi i poleceń nagle się urywa. To tak jakby wypić rano dobrą kawę i nic więcej już tego dnia nie zrobić. Nie wystarczy bowiem sama znajomość podstaw działania sieci bezprzewodowych oraz użycia narzędzi służących do odkrywania punktów dostępowych, rejestrowania ruchu sieciowego, łamania kluczy WEP i tym podobnych. Co więcej, taka wiedza lokuje jej posiadacza na poziomie „skryptowych dzieciaków”, a przecież specjalista bezpieczeństwa sieci bezprzewodowych powinien znajdować się na o wiele wyższym poziomie i powinien wiedzieć, **jak** działają wykorzystywane protokoły oraz **jak** przeprowadza się znane ataki (co powoli odkrywamy przed Tobą w tej książce). Poza tym specjalista bezpieczeństwa musi dysponować drobiazgowo przygotowanym planem testów penetracyjnych, uwzględniającym wszystkie cechy interesującej go sieci.

Zestaw urządzeń i narzędzi

Do tego momentu powinieneś już zdążyć przygotować cały zestaw urządzeń i narzędzi oraz przetestować go w swojej laboratoryjnej sieci WLAN po to, żeby zgodnie z potężnymi prawami Murphy’ego nie zostać niczym zaskoczony podczas pracy u klienta (a mogą Cię zaskoczyć nieobsługiwane symbole ujawniające się podczas ładowania modułów, niezgodność wersji usług kart sieciowych, uszkodzone pigtaile i tym podobne przykrości).

Jeżeli podchodzisz poważnie do swojej pracy, w skład Twojego zestawu wchodzi następujące urządzenia i narzędzia:

1. Laptop z podwójnym gniazdem kart PCMCIA i z zainstalowanym oraz poprawnie skonfigurowanym systemem Linux lub BSD (lub z oboma tymi systemami).
2. Kilka kart bezprzewodowych PCMCIA o różnych chipsetach wyposażonych w złącza anten zewnętrznych, a wśród nich:
 - ◆ Karta Cisco Aironet służąca do wykrywania sieci bezprzewodowych oraz do rejestrowania i analizowania ruchu wielu kanałów radiowych jednocześnie.
 - ◆ Karta z układem Prism służąca do łamania zabezpieczenia WEP (w tym do przyśpieszania tej czynności przez wprowadzenie do sieci dodatkowego ruchu), prowadzenia ataków DoS za pomocą programów *FakeAP*, *Wnet* lub *AirJack*, prowadzenia za pomocą sterowników *HostAP* i drugiej karty z układem Prism ataków *man in the middle* w warstwie pierwszej, prowadzenia za pomocą programu *AirJack* i karty z układem Hermes ataków *man in the middle* w warstwie drugiej lub prowadzenia za pomocą programu *Wnet* i drugiej karty z układem Prism ataków *man in the middle* w warstwie drugiej na platformie OpenBSD.
 - ◆ Karta z układem Hermes przeznaczona do łamania zabezpieczenia WEP (z wyjątkiem metod wymagających wprowadzania do sieci zaszyfowanego ruchu) oraz do prowadzenia za pomocą programu *AirJack* i karty z układem Prism ataków *man in the middle* w warstwie drugiej.
 - ◆ Karta z układem Atheros przeznaczona do badania bezpieczeństwa sieci 802.11a.
3. Co najmniej dwie anteny zewnętrzne (dookólna i kierunkowa o dużym zysku) wraz z odpowiednimi złączami i być może stojakiem do ich mocowania.
4. Wybrane narzędzia bezpieczeństwa sieci bezprzewodowych, za pomocą których można wykonać następujące zadania:
 - ◆ Wykrywanie sieci oraz rejestrowanie ruchu w trybie RFMON.
 - ◆ Dekodowanie i analiza ruchu bezprzewodowego.
 - ◆ Łamanie zabezpieczenia WEP i jeżeli trzeba, siłowe łamanie zabezpieczenia 802.1x.
 - ◆ Generowanie i wprowadzanie do sieci ramek warstwy drugiej.
 - ◆ Skonfigurowanie co najmniej jednej karty sieciowej jako fałszywego punktu dostępowego.
5. Wybrane narzędzia bezpieczeństwa sieci niezwiązane wyłącznie z sieciami bezprzewodowymi (powiemy o nich więcej w rozdziale 9.).

Poza tym w zestawie mogą znaleźć się dodatkowo:

- ◆ Odbiornik GPS podłączony do portu szeregowego laptopa.
- ◆ Palmtop z uruchomionym programem *Kismet* lub *Wellenreiter* oraz z jakimś programem mierzącym natężenie sygnału.
- ◆ Dodatkowe anteny, szczególnie anteny kierunkowe.

- ♦ Zapasowe baterie.
- ♦ Jeden lub więcej wzmacniaczy.
- ♦ Nierzucające się w oczy urządzenie bezprzewodowe służące do testowania mechanizmów wykrywania sieci bezprzewodowych oraz do testowania bezpieczeństwa fizycznego. Najlepiej nadaje się do tego celu interfejs sieci 802.11 w postaci urządzenia USB, które można szybko i dyskretnie podłączyć do jednego z serwerów lub komputerów audytowanej firmy.
- ♦ Mapy terenu (elektroniczne lub papierowe).
- ♦ Lornetka (do wykrywania anten na dachach i tym podobnych).
- ♦ Środek transportu (samochód, rower, łódka, samolot, zeppelin lub balon na ogrzane powietrze).

Przed wyruszeniem w teren sprawdź w warunkach laboratoryjnych, czy możesz przechwytywać ruch, dekodować ramki, łamać zabezpieczenie WEP oraz wprowadzać do sieci własne ramki (przechwyć je, aby się przekonać). Zwróć szczególną uwagę na złącza anten i na to, co się z nimi dzieje podczas zmiany położenia anten. Jeżeli jesteś pewien, że wszystko działa tak jak powinno i tak również będzie działać w terenie, możesz przejść do następnej fazy. Faza ta nie obejmuje jeszcze jeżdżenia, chodzenia, zeglowania ani latania wokół testowanego obiektu z wystającymi antenami, wymaga natomiast myślenia i dostępu do serwisu Google.

Szukanie śladów sieci

Zacznij od gruntownych poszukiwań w internecie informacji na temat interesującego Cię obszaru lub firmy. Nigdy nie lekceważ siły serwisu Google. Być może obszar z interesującymi Cię sieciami WLAN został już zbadany przez kogoś wcześniej, a wyniki tych badań znalazły się na jakiejś stronie WWW, na liście dyskusyjnej lub w blogu. Istnieje mnóstwo społeczności sieci bezprzewodowych, które publikują w internecie informacje na temat publicznych i domowych sieci bezprzewodowych znajdujących się w najbliższej okolicy. Przykładem tego rodzaju publikacji może być strona <http://www.consume.net>. Na rysunku 7.1 przedstawiliśmy zacytowaną z tej strony mapę sieci WLAN w centrum Londynu (zapewniamy Cię, że w tym rejonie działa znacznie więcej sieci bezprzewodowych, niż to pokazano na rysunku). Interesującym miejscem poświęconym sieciom bezprzewodowym w Stanach Zjednoczonych, zawierającym informacje o wielu społecznościach, jest strona <http://www.cybergeography.org/atlas/wireless.html>. Jednak największe i najbardziej szczegółowe listy społeczności sieci bezprzewodowych z całego świata można znaleźć w serwisie WiGLE (<http://www.wigle.net>) zawierającym informacje o ponad milionie sieci WLAN na całym świecie oraz na stronie <http://www.personaltelco.net/index.cgi/WirelessCommunities>. Przeglądając te listy, na pewno znajdziesz jakąś sieć działającą w interesującym Cię rejonie. Poza informacjami na temat sieci bezprzewodowych możesz znaleźć w internecie również informacje o występujących na danym obszarze zakłóceniach radiowych, na przykład powodowanych przez działające w pobliżu nadajniki mikrofalowe, wielkie kompleksy przemysłowe i tym podobne.

Rodzaje i planowanie rekonesansu

Kiedy faza gromadzenia informacji jest już zakończona, pora wybrać sposób przeprowadzenia rekonesansu w terenie. Istnieje kilka możliwości prowadzenia rekonesansu:

- ♦ *Warwalking* — czyli rekonesans prowadzony na piechotę,
- ♦ *Warcycling* — czyli rekonesans prowadzony na rowerze,
- ♦ *Wardriving* — czyli rekonesans prowadzony z samochodu,
- ♦ *Warclimbing* — czyli rekonesans prowadzony na dużej wysokości.

Każda z wymienionych taktyk rekonesansu ma swoje wady i zalety. Prowadząc rekonesans na piechotę, nie obejmiesz zbyt wielkiego obszaru, ale za to zgromadzisz wiele danych. By sprawdzić natężenie sygnału, możesz zatrzymać się w dowolnym miejscu, możesz analizować ruch sieciowy na bieżąco, możesz próbować łączyć się z siecią, prowadzić atak DoS lub atak *man in the middle* i tym podobne. Poza tym masz możliwość wypatrzenia:

- ♦ lokalizacji i rodzajów anten,
- ♦ zewnętrznych punktów dostępowych,
- ♦ informacji „Zakaz korzystania z urządzeń Bluetooth” oraz „Zakaz korzystania z telefonów bezprzewodowych”,
- ♦ symboli sieci (znaków *warchalking*).

Obecność oznaczeń „Zakaz korzystania z urządzeń Bluetooth” i temu podobnych jest czytelnym sygnałem, że administrator sieci rozumie problem zakłóceń i próbuje mu zapobiec. Symbole sieci nanoszone są na chodnikach lub murach i ścianach i służą do identyfikowania najbliższych punktów dostępowych. Znajomość symboli sieci jest nieodzowna, a zapoznać się z nimi można na stronie <http://www.warchalking.org>. Pewną liczbę symboli sieci umieściliśmy w dodatku F. W różnych rejonach to samo znaczenie mogą mieć różne symbole. Istnieje nawet symbol oznaczający sieci FHSS. Nie możesz zatem zakładać, że korzystając z sieci niezgodnych z 802.11 DSSS, takich jak 802.11 FHSS czy HomeRF, pozbędziesz się problemu włamywaczy. Skoro sieci te mają własne symbole, oznacza to, że ktoś ich poszukuje. Nie zdziwimy się, gdy na ulicach pojawią się wkrótce nowe symbole, takie jak „Sieć Bluetooth”, „Łącze punkt-punkt nie 802.11” albo też „WLAN WEPPlus”, „802.1x w użyciu, wykorzystywany EAP to...”, „Sieć z protokołem 802.11i”, „TKIP”, „TurboCell” i tym podobne.

Warwalking ma oczywiście wady — musisz nieść cały sprzęt (szczególny problem stanowią anteny), jesteś ograniczony czasem pracy baterii laptopa lub palmtopa oraz liczbą zapasowych baterii, które możesz zabrać. Mało prawdopodobne jest, byś podczas tego rekonesansu mógł skorzystać z anteny kierunkowej albo ze wzmacniacza. Ważne jest również narażenie sprzętu. Laptopy nie lubią deszczu, podobnie jak złącza anten, które po zamknięciu wykazują większe tłumienie utrzymujące się również po wyschnięciu, a powodem jest pojawiająca się korozja.

Rekonesans prowadzony z samochodu nie naraża tak sprzętu na czynniki zewnętrzne, a poza tym można korzystać z dodatkowego źródła zasilania w postaci akumulatora samochodowego czy prądnicy. Poruszając się samochodem, można odkryć wszystkie sieci występujące na interesującym terenie i nie ma przy tym znaczenia prędkość, z jaką się poruszasz, gdyż ramki Beacon wysyłane są co 10 milisekund i nie sposób mijając sieć WLAN, przegapić którąś z nich. Oczywiście jeżeli nie jedziesz bardzo wolno, nie uda Ci się zgromadzić zbyt wiele ruchu, a obserwowanie i analizowanie pakietów oraz przeprowadzanie ataków jest utrudnione, chyba że zdołasz zaparkować w odpowiednim miejscu, co może się nie udać w centrum dużego miasta czy na terenach prywatnych. Również w przypadku rekonesansu prowadzonego za pomocą samochodu stajemy przed problemem z anteną. Aby wyeliminować duże tłumienie sygnału powodowane przez karoserię samochodu, antena powinna być wystawiona na zewnątrz. Pamiętaj, że już zwykła szyba samochodowa wnosi tłumienie o wartości 2 dB. Oczywiście umieszczenie anteny na zewnątrz samochodu oznacza konieczność użycia kabla antenowego z dodatkowymi złączami. W typowym zestawie wykorzystywanym do tego rekonesansu musi znaleźć się montowana na podstawie magnetycznej antena dookólna na płaszczyźnie masy o zysku około 5 dBi oraz cienki kabel, taki jaki stosowany jest w pigtailach, który może wnosić większe tłumienie, niż wynosi zysk anteny dookólnej zamocowanej na dachu samochodu. Zastosowanie na dachu jakiegoś lepszego uchwyty jest już nie lada wyzwaniem technicznym, a i tak nie będziesz mógł skorzystać z anteny kierunkowej, chyba że podróżując kabrioletem. Z tych powodów rekonesans terenu będzie musiał być prowadzony częściowo z samochodu, a częściowo na piechotę.

Rekonesans prowadzony na rowerze jest czymś pośrednim między obiema zaprezentowanymi metodami. W jego przypadku jesteś ograniczony pojemnością baterii, warunkami atmosferycznymi i niewielką prędkością, ale za to uda Ci się zebrać całkiem sporo ruchu sieciowego, nie siedzisz w metalowej klatce, możesz zatrzymać się gdziekolwiek i nikt nie zabroni Ci podwiesić sobie do ramienia anteny dookólnej o dużym zysku. Użycie anteny kierunkowej podczas jazdy na rowerze nie ma żadnego sensu, bo i bez tego ręce masz zbyt zajęte. Nie możesz również wpisywać żadnych poleceń. Najlepszym rozwiązaniem w przypadku rekonesansu prowadzonego na rowerze jest monitorowanie ruchu i natężenia sygnału za pomocą palmtopa umocowanego do kierownicy.

Terminem *warclimbing* określamy w firmie Arhont odkrywanie, analizowanie i penetrowanie sieci bezprzewodowych z punktu znajdującego się na dużej wysokości. Po co wspinać się i szukać sieci wysoko, skoro podchodzą one pod same drzewa? Latem 2002 roku z wierzchołka wieży Cabot Tower w Bristolu (zobacz rysunek 7.2) odkryliśmy za pomocą anteny o zysku 19 dBi 32 sieci, a za pomocą anteny Yagi o zysku 15 dBi połowę tej liczby. Niektóre z tych sieci działały w Bath, a nawet wzdłuż granicy z Walią, co jest naprawdę dużą odległością! Nawet za pomocą anteny dookólnej 12 dBi mogliśmy odkryć około tuzina sieci działających w tamtym rejonie. Jesteśmy pewni, że od tamtego czasu liczba tych sieci jeszcze wzrosła.

Tego rodzaju rekonesans można prowadzić z dachu wysokiego budynku, wierzchołka wzgórza czy z pokoju na najwyższym piętrze dogodnie usytuowanego hotelu, z którego zdeteminowany napastnik może przez dzień lub dwa prowadzić atak na sieć bezprzewodową wybranej firmy. Zalety tej metody prowadzenia rekonesansu to stabilna pozycja, duży zasięg oraz dobra jakość łącza uzyskiwanego w przypadku czystej ścieżki

Rysunek 7.2.

*Wieża Cabot Tower
w Bristolu w Wielkiej
Brytanii*



za pomocą silnie kierunkowej anteny. Oczywiście żeby skorzystać z tej metody, w pobliżu interesującej nas sieci muszą znajdować się odpowiednio wysoko położone miejsca, a najlepszym z nich będzie to, w którym sygnał interesującej nas sieci będzie jak największy. Wcześniejsze odnalezienie wszystkich takich miejsc w sprawdzanym obszarze stanowi duże ułatwienie, na przykład w przypadku potrzeby zlokalizowania za pomocą metody triangulacji położenia napastnika wyposażonego w antenę o dużym zysku, przekonanego o swojej nieuchwytności, coś jak Borys z filmu *Golden Eye*.

Nie będziemy się tu zajmować innymi, bardziej egzotycznymi metodami wykrywania sieci bezprzewodowych, takimi jak choćby *warflying*, czyli rekonesans prowadzony z powietrza, gdyż jak słusznie zauważył ktoś w serwisie Slashdot, „jak z wysokości 4 tysięcy metrów oznaczyć istnienie sieci kredą na murze?”. Z pewnością z takiej wysokości można wykrywać sieci, ale przechwycenie choćby jednego pakietu danych można nazwać szczęściem. Mimo to planujemy podróż balonem na rozgrzane powietrze z dobrą anteną kierunkową, będzie to coś między *warclimbingiem* a *warcyclingiem*.

Planując rekonesans w terenie oraz w dalszej perspektywie testy penetracyjne, powinienś uwzględnić informacje, które być może uzyskałeś już w fazie zbierania danych, na przykład informacje o otoczeniu interesującego Cię miejsca czy o położeniu sieci:

- ♦ Na których piętrach budynku znajdują się punkty dostępowe lub anteny?
- ♦ Gdzie znajdują się anteny zainstalowane na masztach?
- ♦ Jakie są największe przeszkody terenowe?
- ♦ Z jakiego materiału wykonane są ściany budynku?
- ♦ Jak grube są ściany? (Ich tłumienie wyznaczysz, korzystając z dodatku E).
- ♦ Czy wykorzystywane są anteny kierunkowe przenikające przeszkody?
- ♦ Czy teren chroniony jest fizycznie? Gdzie znajdują się strażnicy i kamery telewizyjnej przemysłowej?

Planowanie czasu ataku i oszczędzanie baterii

Inną bardzo ważną częścią planowania testów penetracyjnych jest zaplanowanie czasu ich przeprowadzenia oraz czasu ich trwania. Czas prowadzenia testów powinien zostać uzgodniony z klientem choćby po to, by przeprowadzane testy zakłócające (takie jak na przykład badanie odporności sieci na atak DoS) nie zakłóciły normalnej pracy firmy. Jednak niektóre testy bezpieczeństwa, takie jak na przykład rekonesans czy łamanie zabezpieczenia WEP, należy przeprowadzić w czasie największego wykorzystania sieci WLAN. W tym celu należy ustalić wcześniej, o której godzinie użytkownicy zaczynają korzystać z badanej sieci i kiedy przypada szczyt jej wykorzystania. Informacja ta pomoże nie tylko w złamaniu zabezpieczenia WEP (pamiętaj, że im więcej uda Ci się zgromadzić danych, tym lepiej), ale również w atakach prowadzonych po rozszyfrowaniu klucza WEP, polegających na zbieraniu danych uwierzytelniających użytkowników. Tego rodzaju ataki są niezbędne do udowodnienia kierownictwu firmy potencjalnych konsekwencji naruszenia bezpieczeństwa sieci bezprzewodowej oraz konieczności zabezpieczania sieci WLAN w sposób podobny do zabezpieczania połączeń WAN realizowanych za pośrednictwem sieci publicznych.

Zagadnieniem ściśle związanym z planowaniem czasu przeprowadzania testów penetracyjnych jest problem użycia baterii oraz oszacowania pozostałego czasu pracy baterii. W tym celu należy odpowiedzieć na dwa pytania: ile czasu będą trwały zaplanowane testy oraz czy wykorzystywana bateria wystarczy na ten czas? Jednym z najbardziej czasochłonnych procesów testów penetracyjnych jest łamanie zabezpieczenia WEP, a kiedy chce się je przyśpieszyć wywołując w sieci dodatkowy ruch, wysyłanie go pociąga za sobą większe zużycie energii z baterii. Dlatego w sytuacji rzeczywistego włamywania się do sieci wprowadzanie do niej dodatkowego ruchu jest narzędziem obosiecznym, przynajmniej wówczas, gdy kraker nie dysponuje dodatkowym źródłem zasilania, na przykład możliwością skorzystania z akumulatora samochodu. Prowadząc testy penetracyjne, zazwyczaj będziesz mógł skorzystać z gniazdka elektrycznego, choć nie należy przyjmować tego za pewnik. Najlepszy test penetracyjny to taki, który jest przeprowadzany w identycznych warunkach, w jakich kraker przeprowadza atak, a żadna firma nie zezwoli (a przynajmniej nie powinna zezwolić) włączyć krakerowi laptopa do swojego gniazdka (nic nie stoi jednak na przeszkodzie, by kraker podłączył się do gniazdka w pubie czy restauracji po drugiej stronie ulicy).

Aby skutecznie oszczędzać baterię w terenie, wystarczy przedsięwziąć kilka prostych środków. Należy zacząć od zatrzymania wszystkich niepotrzebnych usług (my pozostawiamy jedynie serwer syslog). Nie korzystaj z systemu X Windows ani innego graficznego systemu użytkownika, który dosłownie pożera energię baterii! Złóż laptop, co spowoduje wyłączenie ekranu. Jeżeli to możliwe, zmniejsz moc nadawania karty sieciowej do minimum (można to zrobić w przypadku kart Cisco Aironet i kilku innych kart PCMCIA). Przekonaliśmy się, że gdy normalnie laptop pracował na bateriach niecałe dwie godziny, to po zastosowaniu tych zaleceń czas pracy na bateriach z uruchomionym programem *Kismet* i *tcpdump* wydłużył się do ponad dwóch i pół godziny. Zastanów się, czy nie można przenieść wszystkich danych do pamięci RAM i tak skonfigurować dysku, by wyłączał się automatycznie po kilku chwilach nieaktywności.

Większość nowoczesnych laptopów wyposażona jest w dużą ilość pamięci RAM, która starcza do przechowania przechwyconych pakietów. Nie zapomnij jednak przy tym, że pamięć ta jest ulotna, więc oszczędź trochę energii na zapisanie danych z pamięci na dysk po skończeniu pracy lub na chwilę przed wyczerpaniem się baterii. Wszystkie czynności wykonuj za pomocą wiersza poleceń — oszczędzisz czas, baterię, a poza tym nauczysz się szybciej pisać. Zwiększ swoją wydajność, przygotowując sobie wcześniej odpowiednie skrypty lub zrób sobie listę wykorzystywanych poleceń, z której będziesz je mógł kopiować i wklejać w wierszu poleceń, jeżeli trzeba zmieniając tylko wartości adresów IP, MAC czy kanałów DSSS. Jak już informowaliśmy wcześniej, nie stosuj skanowania aktywnego, gdy nie jest ono niezbędne (na przykład do testowania sygnatur systemu IDS). Zalety wynikające z przestrzegania wymienionych tu zaleceń to kolejne argumenty za użyciem do testowania bezpieczeństwa sieci bezprzewodowych któregoś z systemów uniksowych.

Ukrywanie się podczas prowadzenia testów penetracyjnych

Ostatnim zagadnieniem, które należy wziąć pod uwagę, planując prowadzenie testów penetracyjnych sieci bezprzewodowych, jest pozostawanie w ukryciu. W niektórych sytuacjach, na przykład podczas testowania jakości wykorzystywanego systemu IDS, należy zadbać o wysoki poziom ukrycia. Ukrycie testów sieci bezprzewodowych można osiągnąć na kilka sposobów:

- ♦ przez unikanie skanowania aktywnego,
- ♦ przez użycie anten o silnej kierunkowości,
- ♦ przez zmniejszenie podczas przechwytywania ruchu mocy nadawania,
- ♦ przez inteligentne fałszowanie adresu MAC,
- ♦ przez usunięcie z kodu narzędzia wykorzystywanego do prowadzenia ataku charakterystycznych dla niego sygnatur (patrz rozdział 15.),
- ♦ przez prowadzenie ataków DoS, których zadaniem jest uniemożliwienie działania sensorom IDS (patrz rozdział 8.).

Oczywiście w przypadku prowadzenia ataków na sieć już po skojarzeniu się z nią należy również zastosować środki ochrony przed wykryciem przez systemy IDS naszych działań w warstwach trzeciej i wyższych (powiemy o tym w rozdziale 9.).

Panuj nad sondami! Karty Cisco Aironet mogą wysyłać ramki Probe Request, działając w trybie RFMON. Chociaż problem ten został rozwiązany w modułach *Aironet* dostarczanych z jądrami systemu Linux, począwszy od wersji 2.4.22, może on pozostać nierozwiązany w innych systemach operacyjnych. Poza tym może okazać się, że wciąż korzystasz ze starszej wersji jądra.

Czynności wykonywane podczas ataku

Z naszych doświadczeń wynika, że dobrze przemyślany profesjonalny atak na sieć bezprzewodową powinien przebiegać według następującego schematu:

1. Zdobycie informacji o sieci oraz jej zasięgu poprzez poszukiwania w internecie, przez kontakty osobiste oraz za pomocą socjotechniki. Nigdy nie należy lekceważyć takich źródeł informacji jak serwis Google i zawsze należy pamiętać, że najsłabszym ogniwem są i zawsze będą ludzie.
2. Zaplanowanie metodologii rekonesansu oraz testów, jakim należy poddać sieć.
3. Zgromadzenie, przygotowanie, skonfigurowanie i sprawdzenie urządzeń i narzędzi niezbędnych do wykonania zadań zaplanowanych w punkcie 2.
4. Przeprowadzenie rekonesansu w celu określenia zasięgu sieci oraz pomierzenia natężenia sygnału (w tym celu najpierw należy się posłużyć anteną dookólną, następnie anteną kierunkową i na koniec antenami o wysokiej kierunkowości). Znalezienie odpowiednich miejsc, z których można przeprowadzić atak w pozycji stacjonarnej. Czynniki, jakie należy brać pod uwagę przy wyborze takiego miejsca, są: bezpośrednia widoczność celu ataku, wartość natężenia sygnału oraz wartość SNR, możliwość fizycznego ukrycia się (widoczność miejsca z atakowanego obiektu, dostęp do tego miejsca służb ochrony atakowanego obiektu, znalezienie się w zasięgu kamer telewizji przemysłowej), wygoda napastnika rozumiana jako możliwość dogodnego umiejscowienia komputera i zainstalowania anteny oraz bezpieczeństwo fizyczne (unikanie miejsc, w których można być narażonym na utratę drogiego sprzętu).
5. Analiza dostępnego ruchu w celu uzyskania odpowiedzi na kilka pytań. Czy ruch jest szyfrowany? Jak mocno obciążona jest sieć? Które ramki zarządzania i kontrolowania sieci są dostępne i ile z nich można uzyskać informacji? Czy widoczne są oczywiste problemy sieci, takie jak duży poziom zakłóceń, nakładanie się kanałów, częsta utrata połączeń objawiająca się wysyłaniem przez komputery dużej liczby ramek Probe Request?
6. Próba uniknięcia wykrytych środków bezpieczeństwa. Obejmuje to omijanie filtrowania adresów MAC oraz filtrowania pakietów, odkrycie identyfikatorów ESSID w sieciach zamkniętych, złamanie zabezpieczenia WEP, a także uniknięcie środków bezpieczeństwa działających w wyższych warstwach sieciowych, takich jak filtrowanie ruchu w bramie bezprzewodowej, uwierzytelnianie wykorzystujące serwer RADIUS czy też stosowanie połączeń VPN.
7. Połączenie się z siecią bezprzewodową, a następnie wykrycie bramy prowadzącej do internetu albo wykrycie routera brzegowego, wykrycie tradycyjnych i bezprzewodowych sensorów IDS, komputera lub komputerów prowadzących centralny rejestr zdarzeń oraz innych komputerów w sieciach bezprzewodowej i kablowej.
8. Pasywne gromadzenie informacji o odkrytych komputerach oraz przeanalizowanie bezpieczeństwa protokołów wykorzystywanych w sieci bezprzewodowej oraz połączonej z nią sieci kablowej.

9. Aktywne badanie interesujących komputerów, a następnie przeprowadzanie na nie ataków mających na celu uzyskanie uprawnień administracyjnych (root, administrator, tryb *enable*).
10. Połączenie się z internetem lub z innymi sieciami równorzędnymi za pośrednictwem wykrytej bramy, a następnie wykonanie próby pobierania i umieszczania tam plików.

Przetestuj tę procedurę, a być może zauważysz, że skuteczność Twoich testów penetracyjnych sieci bezprzewodowych bardzo się poprawiła, choć może nie użyłeś żadnych innych narzędzi ponad te, które już stosujesz.

Na zakończenie proponujemy Ci zapoznanie się ze znajdującą się w dodatku G uszczuploną wersją szablonu audytu bezpieczeństwa i stanu sieci bezprzewodowej, który wykorzystujemy w firmie Arhont w swojej codziennej działalności. W dodatku znajdź część szablonu poświęconą testom penetracyjnym i przeczytaj, na co należy zwracać uwagę podczas rekonesansu. Uzyskasz w ten sposób dodatkowe informacje przydatne Ci podczas planowania prawidłowego audytu sieci bezprzewodowych. Niektóre punkty tego szablonu mogą nie być dla Ciebie jeszcze zrozumiałe, ale zostaną wyjaśnione w dalszej części książki. Jeżeli wcześniej sam przygotowałeś podobny szablon, jesteśmy otwarci na wszystkie propozycje, które mogłyby udoskonalić nasz.

Podsumowanie

Planowanie i dokumentowanie ataku jest tak samo ważne jak zgromadzenie niezbędnych urządzeń i narzędzi. Skuteczne planowanie oszczędza czas oraz wysiłek, odkrywa ważne informacje jeszcze przed rozpoczęciem właściwego audytu oraz zmniejsza prawdopodobieństwo wydarzenia się podczas audytu przykrych niespodzianek (na przykład wyczerpania się baterii podczas skanowania sieci). „Bitwę powinno się wygrać jeszcze przed jej rozpoczęciem” — Sun Tzu.