



Technologia i rozwiązania

Kali Linux

Audyt bezpieczeństwa sieci Wi-Fi dla każdego

Wydanie II

Odkryj słabe punkty infrastruktury sieciowej!



Vivek Ramachandran
Cameron Buchanan

[PACKT] open source*
PUBLISHING community experience distilled

Tytuł oryginału: Kali Linux Wireless Penetration Testing: Beginner's Guide, Second Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-283-1611-9

Copyright © Packt Publishing 2015. First published in the English language under the title „Kali Linux Wireless Penetration Testing: Beginner's Guide (Second Edition)” – (9781783280414).

Polish edition copyright © 2015 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/kaliau>

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 autorach	7
O recenzencie	9
Klauzula wyłączenia odpowiedzialności	10
Wprowadzenie	11
Co znajdziesz w tej książce	12
Co będzie potrzebne do pracy z książką	14
Dla kogo przeznaczona jest ta książka	14
Konwencje użyte w tej książce	15
Errata	15
Nielegalne kopiowanie	16
Rozdział 1. Tworzymy laboratorium sieci bezprzewodowych	17
Wymagania sprzętowe	18
Niezbędne oprogramowanie	19
Instalowanie systemu Kali Linux	19
Czas na działanie — instalujemy system Kali Linux	19
Instalacja i konfiguracja bezprzewodowego punktu dostępowego	21
Czas na działanie — konfiguracja bezprzewodowego punktu dostępowego	22
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	29
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	39

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	45
Czas na działanie — eksperymentujemy z bezprzewodową kartą sieciową	46
Rola organów regulacyjnych w sieciach bezprzewodowych	48
Czas na działanie — eksperymentujemy z bezprzewodową kartą sieciową	48
Podsumowanie	52
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 w sieciach 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	72
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	77
Szyfrowanie WPA/WPA2	88
Czas na działanie — łamanie słabych haseł w sieciach z szyfrowaniem WPA-PSK	90
Przyspieszanie procesu łamania szyfrowania WPA/WPA2 PSK	96
Czas na działanie — przyspieszanie procesu łamania kluczy	97
Odszyfrowywanie pakietów WEP i WPA	99
Czas na działanie — deszyfrowanie pakietów WEP i WPA	100
Podłączanie się do sieci WEP i WPA	102
Czas na działanie — podłączanie się do sieci wykorzystującej szyfrowanie WEP	102
Czas na działanie — podłączanie się do sieci wykorzystującej szyfrowanie WPA	103
Podsumowanie	105
Rozdział 5. Ataki na infrastrukturę sieci WLAN	107
Domyślne konta i hasła punktów dostępowych	108
Czas na działanie — łamanie domyślnych, fabrycznych haseł punktów dostępowych	108
Ataki typu odmowa usługi (DoS)	110
Czas na działanie — atak DoS typu anulowanie uwierzytelnienia	110
Złośliwy bliźniak i fałszowanie adresów MAC	114
Czas na działanie — złośliwy bliźniak ze sfalszowanym adresem MAC	115
Nieautoryzowany punkt dostępowy	120
Czas na działanie — nieautoryzowany punkt dostępowy	120
Podsumowanie	127
Rozdział 6. Ataki na klienta sieci WLAN	129
Ataki typu Honeypot i Misassociation	130
Czas na działanie — przeprowadzanie ataków typu Misassociation	131
Atak typu Caffè Latte	135

Czas na działanie — przeprowadzanie ataku typu Caffè Latte	136
Ataki typu Deauthentication i Disassociation	138
Czas na działanie — anulowanie uwierzytelnienia klienta	139
Atak typu Hirte	141
Czas na działanie — łamanie klucza WEP poprzez atak typu Hirte	141
Łamanie klucza WPA PSK bez obecności punktu dostępowego	143
Czas na działanie — łamanie klucza WPA bez obecności punktu dostępowego	144
Podsumowanie	146
Rozdział 7. Zaawansowane ataki na sieci WLAN	147
Ataki typu Man-in-the-Middle	148
Czas na działanie — atak typu Man-in-the-Middle	148
Podśluchiwanie ruchu sieciowego na bazie ataków Man-in-the-Middle	152
Czas na działanie — podśluchiwanie ruchu w sieci bezprzewodowej	152
Przechwytywanie sesji w sieciach bezprzewodowych	157
Czas na działanie — przechwytywanie sesji w sieciach bezprzewodowych	157
Odkrywanie konfiguracji zabezpieczeń klienta	161
Czas na działanie — odkrywanie profili zabezpieczeń klientów bezprzewodowych	161
Podsumowanie	165
Rozdział 8. Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami Radius	167
Konfiguracja serwera FreeRadius WPE	168
Czas na działanie — konfigurowanie punktu dostępowego wykorzystującego serwer FreeRadius WPE	169
Ataki na protokół PEAP	171
Czas na działanie — łamanie zabezpieczeń protokołu PEAP	172
Ataki na protokół EAP-TTLS	175
Dobre praktyki zabezpieczania korporacyjnych sieci bezprzewodowych	176
Podsumowanie	177
Rozdział 9. Metodologia testów penetracyjnych sieci bezprzewodowych	179
Testy penetracyjne sieci bezprzewodowych	179
Planowanie	180
Rozpoznanie	181
Atak	182
Tworzenie raportów	183
Podsumowanie	184
Rozdział 10. Szyfrowanie WPS i sondowanie sieci	185
Ataki na szyfrowanie WPS	185
Nasłuchiwanie prób sondowania sieci	189
Podsumowanie	194
Dodatek A. Szybki quiz — odpowiedzi na pytania	195
Skorowidz	198

Metodologia testów penetracyjnych sieci bezprzewodowych

„Nie mów hop, póki nie przeskoczysz”.

Popularne przysłowie

W tym rozdziale postaramy się połączyć zagadnienia i techniki omawiane w poprzednich rozdziałach i wykorzystać je podczas przeprowadzania prawdziwego testu penetracyjnego sieci bezprzewodowej.

Testy penetracyjne sieci bezprzewodowych

Aby skutecznie przeprowadzić test penetracyjny sieci bezprzewodowych, powinieneś zawsze postępować zgodnie z ogólnie przyjętą i sprawdzoną metodologią. Proste uruchomienie programów takich jak airbase czy airodump z pewnością nie przyniesie oczekiwanych rezultatów. Jako pentester, powinieneś zawsze upewnić się, że działasz zgodnie ze standardami organizacji, dla której pracujesz, a jeżeli nie zostały one formalnie wyznaczone, powinieneś zawsze starać się przeprowadzać testy penetracyjne w sposób jak najbardziej profesjonalny.

Ogólnie rzecz biorąc, proces przeprowadzania testów penetracyjnych sieci bezprzewodowej można podzielić na cztery główne etapy:

- Faza planowania.
- Faza rozpoznania.
- Faza ataku.
- Faza raportowania.

W kolejnych podrozdziałach omówimy oddzielnie każdy z tych etapów.

Planowanie

W tej fazie należy zająć się następującymi zagadnieniami:

- **Zakres planowanego testu** — klient zatrudniający specjalistę do przeprowadzenia testów penetracyjnych powinien z góry zdefiniować zakres testu, jaki należy przeprowadzić. Zazwyczaj obejmuje to takie informacje, jak:
 - Lokalizacja sieci, która będzie testowana.
 - Całkowity obszar pokryty zasięgiem sieci na terenie firmy i terenach przyległych.
 - Przybliżona liczba zainstalowanych punktów dostępowych oraz autoryzowanych klientów bezprzewodowych.
 - Lista identyfikatorów sieci bezprzewodowych, które mają być poddane testowi.
 - Oświadczenie klienta, czy zezwala na eksploatację wykrytych podczas testu podatności i luk w zabezpieczeniach.
 - Oświadczenie klienta, czy zezwala na przeprowadzanie ataków na użytkowników testowanej sieci bezprzewodowej.
 - Oświadczenie klienta, czy zezwala na przeprowadzanie ataków typu DoS na badane sieci i ich użytkowników.
- **Oszacowanie czasu i zasobów niezbędnych do przeprowadzenia testów** — po ustaleniu zakresu testów, jakie mają zostać przeprowadzone, powinieneś przystąpić do oszacowania czasu i zasobów niezbędnych do ich zrealizowania. Pamiętaj, że często zakres przeprowadzanego testu może ulec zmianie na życzenie klienta.
- **Dokumenty prawne** — przeprowadzanie testów penetracyjnych to bardzo poważne zadanie i zawsze istnieje możliwość, że może się wydarzyć coś nieprzewidzianego, co doprowadzi do mniejszych bądź większych perturbacji w funkcjonowaniu testowanej sieci. Z tego powodu zawsze powinieneś mieć pod ręką odpowiednią, podpisaną z klientem umowę o zwolnieniu z odpowiedzialności, zapewniającą, że ani osoba przeprowadzająca testy penetracyjne, ani firma czy organizacja, którą reprezentuje, nie będą pociągnięte do odpowiedzialności za żadne szkody mogące

powstać w wyniku przeprowadzania testów penetracyjnych. Bardzo często zdarza się również, że klient żąda podpisania umowy o zachowaniu poufności (ang. *NDA* — *Non Disclosure Agreement*), która zapewnia, że dane zebrane podczas testów penetracyjnych nie będą udostępniane podmiotom trzecim, niebędącym stronami umowy.

Po pomyślnym zakończeniu fazy planowania i przygotowań możemy rozpocząć działania operacyjne.

Rozpoznanie

W tej fazie celem naszych działań będzie skanowanie ruchu w sieci bezprzewodowej w celu odszukania i zidentyfikowania punktów dostępowych oraz klientów bezprzewodowych znajdujących się w środowisku celu.

Wszystkie techniki niezbędne do przeprowadzenia tej fazy zostały szczegółowo omówione w poprzednich rozdziałach naszej książki, ale dla przypomnienia poniżej zamieszczamy krótkie zestawienie najważniejszych celów, które powinieneś osiągnąć w fazie rozpoznania:

- Identyfikacja wszystkich widocznych i niewidocznych sieci bezprzewodowych znajdujących się w obszarze środowiska celu.
- Identyfikacja wszystkich urządzeń bezprzewodowych działających w obszarze środowiska celu oraz wyodrębnienie tych, które są podłączone do sieci będących celem naszego testu penetracyjnego.
- Mapowanie obszarów fizycznej dostępności poszczególnych sieci bezprzewodowych oraz identyfikacja lokalizacji, z których potencjalny napastnik mógłby w ukryciu przeprowadzać ataki na badane sieci (na przykład pobliska kawiarnia znajdująca się w zasięgu badanej sieci).

Wszystkie pozyskane w tej fazie informacje powinny zostać skrupulatnie zanotowane. Jeżeli uzgodniony zakres testu penetracyjnego sprowadzał się wyłącznie do fazy rozpoznania, działania operacyjne zostaną zakończone na tym etapie i pentesterowi pozostanie już tylko napisanie odpowiedniego raportu, zawierającego między innymi wnioski i rekomendacje oparte na pozyskanych danych. W raporcie mogą się znaleźć między innymi takie informacje, bardzo cenne dla klienta:

- Liczba wykrytych urządzeń, które były powiązane zarówno z sieciami otwartymi, jak i siecią klienta.
- Liczba wykrytych urządzeń powiązanych z sieciami, które mogą być zlokalizowane za pomocą takich usług jak WiGLE.
- Informacje o wykrytych urządzeniach wykorzystujących słabe algorytmy szyfrowania.
- Wszelkie inne informacje, które mogą być przydatne dla klienta.

Atak

Po zakończeniu fazy rozpoznania możesz rozpocząć fazę ataku, której celem będzie dokonanie próby wykorzystania wykrytych wcześniej podatności i luk w zabezpieczeniach. Rodzaj i natężenie przeprowadzanych ataków zależą w dużej mierze od uzgodnionego z klientem zakresu przeprowadzanego testu penetracyjnego.

W fazie ataku możesz wykonywać następujące zadania:

- Ataki i łamanie kluczy szyfrowania sieci.
- Ataki na infrastrukturę sieci bezprzewodowych w środowisku celu.
- Przełamywanie zabezpieczeń klientów.
- Identyfikacja klientów podatnych na ataki.
- Wykrywanie nieautoryzowanych klientów sieci bezprzewodowych.

Łamanie klucza szyfrowania sieci

Pierwszym i najważniejszym elementem ataku będzie zazwyczaj próba pozyskania klucza szyfrowania wykorzystywanego w atakowanej sieci. Jeżeli dana sieć bezprzewodowa wykorzystuje szyfrowanie WEP, powinieneś dokonać próby ataku na klucz szyfrowania z wykorzystaniem metod opisywanych w rozdziale 4., „Słabe strony protokołów szyfrowania w sieciach WLAN”. Jeżeli sieci w środowisku celu używają szyfrowania WPA2, masz do wyboru dwie możliwości. Jeśli przeprowadzasz „ukryty” test penetracyjny, powinieneś pojawić się w zasięgu sieci w czasie, kiedy pracownicy firmy lub organizacji będą się logować do sieci i z niej wylogowywać. Zazwyczaj największe natężenie takich zdarzeń ma miejsce w następujących porach:

- Rozpoczęcie dnia pracy.
- Okolice lunchu.
- Zakończenie dnia pracy.

W takich porach możesz dokonać próby przeprowadzenia ataku na klucz WPA, tak jak to pokazywaliśmy w rozdziale 4., „Słabe strony protokołów szyfrowania w sieciach WLAN”. W razie potrzeby możesz również wymusić ponowne logowanie się użytkowników do sieci, przeprowadzając atak wymuszający anulowanie uwierzytelnienia użytkowników podłączonych do punktu dostępowego badanej sieci bezprzewodowej. Przykłady takich ataków opisywaliśmy w rozdziale 6., „Ataki na klienta sieci WLAN”.

Z oczywistych względów przeprowadzanie takich ataków generuje znacznie więcej „hałasu” w sieci, co zdecydowanie zwiększa szansę na to, że odpowiednie służby informatyczne atakowanego klienta będą w stanie wykryć taki atak.

Jeżeli badana sieć wykorzystuje szyfrowanie WPA-Enterprise, pamiętaj, że będziesz musiał użyć informacji zebranych w fazie rozpoznania do utworzenia i skonfigurowania odpowiedniego podstawionego środowiska sieciowego, tak jak to opisywaliśmy w rozdziale 8., „Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami Radius”, w sekcji „Ataki na protokół PEAP”.

Oczywiście, zawsze możesz dokonać próby złamania dowolnego hasła czy klucza szyfrowania, ale jednocześnie musisz się pogodzić z tym, że niektórych z nich nie da się po prostu złamać w rozsądnym czasie i przy użyciu rozsądnych zasobów. W każdym przypadku po zakończeniu testu penetracyjnego powinieneś skontaktować się z administratorem sieci bezprzewodowej i omówić z nim zagrożnienia związane z bezpieczeństwem używanych haseł.

Ataki na infrastrukturę sieci bezprzewodowych

Jeżeli udało Ci się złamać klucz szyfrowania i uzyskać dostęp do atakowanej sieci, możesz rozpocząć przeprowadzanie pozostałej części testu penetracyjnego (o ile oczywiście przeprowadzenie takiego testu wchodzi w zakres umowy uzgodnionej z klientem). Zazwyczaj podczas tej fazy testu penetracyjnego przeprowadzane są co najmniej następujące operacje:

- Skanowanie portów.
- Wykrywanie oraz identyfikacja usług sieciowych działających w środowisku celu.
- Wykrywanie oraz identyfikacja otwartych usług sieciowych, umożliwiających dostęp bez konieczności przeprowadzania uwierzytelniania, takich jak FTP, SMTP czy HTTP.
- Wykorzystywanie wykrytych podatności i luk w zabezpieczeniach do przełamywania zabezpieczeń atakowanych systemów.

Atakowanie klientów sieci bezprzewodowych

Po zakończeniu wykrywania oraz identyfikacji bezprzewodowych hostów sieciowych działających w środowisku celu możesz rozpocząć przeprowadzanie różnego rodzaju ataków.

Na przykład, jeżeli to konieczne, po wykryciu hostów podatnych na ataki typu Karma możesz utworzyć Honeypot i spróbować zmusić je do podłączenia się do niego, tak jak to opisywaliśmy w rozdziale 8., „Ataki na sieci WLAN z szyfrowaniem WPA-Enterprise i serwerami Radius”, w sekcji „Ataki na protokół PEAP”. Za pomocą takiej metody możesz zebrać ogromną ilość bardzo użytecznych informacji, choć zawsze powinieneś się upewnić, że gromadzone informacje są pozyskiwane, przesyłane i przetwarzane w etyczny i bezpieczny sposób oraz że zostaną wykorzystane wyłącznie na potrzeby uzgodnionego z klientem testu penetracyjnego.

Tworzenie raportów

Po zakończeniu fazy ataku wiesz już, jakie są słabe strony testowanej sieci, a zatem musisz przystąpić do utworzenia raportu, który przedstawiś zleceniodawcy. Ze względu na fakt, że klient będzie widział rezultaty przeprowadzonego testu penetracyjnego przez pryzmat przedstawionego przez Ciebie raportu, do jego tworzenia powinieneś zawsze podchodzić z takim samym zaangażowaniem jak do samego testu. Poniżej przedstawiamy krótkie zestawienie elementów, które powinien zawierać raport końcowy z przeprowadzonych testów penetracyjnych:

1. Podsumowanie dla zarządu.
2. Podsumowanie techniczne.
3. Zestawienie ważnych elementów odkrytych podczas testu:
 - Opis wykrytych podatności i luk w zabezpieczeniach.
 - Kategorie zagrożeń.
 - Lista urządzeń podatnych na ataki.
 - Rodzaje wykrytych podatności i luk w zabezpieczeniach — podatności programowe/sprzętowe/konfiguracyjne.
 - Opis rekomendowanych sposobów szybkiego naprawienia wykrytych podatności.
4. Dodatki.

Podsumowanie dla zarządu powinno zostać napisane prosto i przejrzyste, tak aby kadra zarządzająca — niemająca zbyt dużego doświadczenia technicznego — była w stanie zrozumieć wyniki przeprowadzonego testu i ewentualną konieczność wprowadzenia takich czy innych programów naprawczych. Pisząc podsumowanie dla zarządu, powinieneś zdecydowanie unikać używania skomplikowanego języka technicznego i omawiania złożonych detali oraz zawsze umieścić ogólny opis wyników testu i rekomendowanych rozwiązań.

Podsumowanie techniczne powinno być etapem pośrednim pomiędzy podsumowaniem dla zarządu a zestawieniem elementów odkrytych podczas testu. Ta część raportu jest zazwyczaj przeznaczona dla kierownika działu rozwoju bądź innego działu technicznego IT, dlatego powinna się koncentrować na rekomendowanych rozwiązaniach i sposobach ich ewentualnego wdrażania w badanym środowisku.

Zestawienie elementów powinno zawierać szczegółowe, precyzyjne opisy poszczególnych podatności i luk w zabezpieczeniach odkrytych podczas przeprowadzanego testu penetracyjnego oraz opis sposobu wykrycia i wykorzystania poszczególnych podatności.

Dodatki do raportu mogą zawierać dowolne dodatkowe informacje przydatne dla klienta, które z takich czy innych powodów nie powinny się znajdować w głównej części raportu. Przykładami takich elementów mogą być różnego rodzaju zrzuty ekranów, kody wykorzystanych exploitów czy skryptów PoC (ang. *proof-of-concept*) lub szczegółowe zestawienia danych, do jakich udało się dotrzeć pentesterowi podczas przeprowadzania testu.

Podsumowanie

W tym rozdziale pokazaliśmy, w jaki sposób możesz przeprowadzać testy penetracyjne sieci bezprzewodowych przy użyciu narzędzi i technik opisywanych w poprzednich rozdziałach naszej książki. Omawialiśmy również zagadnienia związane z prezentowaniem wyników przeprowadzanych testów penetracyjnych, zwłaszcza dla osób z kadry menedżerskiej, nieposiadającej odpowiedniego przygotowania technicznego. W ostatnim rozdziale naszej książki omówimy nowe techniki, jakie pojawiły się na rynku od czasu ukazania się pierwszego wydania tej książki, takie jak WPS czy monitorowanie prób sondowania sieci.

Skorowidz

A

adres MAC
 filtrowanie, 55, 61
 karty sieciowej, 25, 27
 punktu dostępowego, *Patrz:*
 punkt dostępowy adres
 MAC
algorytm
 AES-CCMP, 88
 RC4, 76
 TKIP, 88
atak
 anulowanie uwierzytelnienia,
 58, 60, 110, 112, 114, 129,
 135, 138, 140, 141
 anulowanie skojarzenia, 110
 CTS-RTS, 110
 kryptograficzny, 75, 76
 MITM, *Patrz:* atak typu Man-
 in-the-Middle
 na infrastrukturę sieci
 bezwzrostowej, 107
 słownikowy, 88, 89, 96, 108,
 175
 testowy, 182
 tylne wejście, 120
 typu
 brute-force, 109, 186
 Caffe Latte, 129, 135, 136,
 138
 Deauthentication, *Patrz:* atak
 anulowanie
 uwierzytelnienia
 Disassociation, 129, 138,
 140, 141
 evil twins, *Patrz:* atak typu
 złośliwy bliźniak

Hirte, 129, 141
Honeypot, 129, 130, 135
Man-in-the-Middle, 114,
 147, 148, 152
Misassociation, 129, 130, 131
odmowa usługi, 107, 110
złośliwy bliźniak, 107, 114,
 119

Authenticator Nonce, *Patrz:*
 wartość losowa ANonce

B

backdoor entry, *Patrz:* atak tylne
 wejście
bezpieczeństwo, 176
bridge-utils, 120
broadcast deauthentication
 packet, *Patrz:* pakiet
 rozgłoszeniowy anulowania
 uwierzytelnienia

C

channel hopping mode, *Patrz:*
 tryb skakania po kanałach
Clear-to-Send/Ready-to-Send,
 Patrz: atak CTS-RTS
Cowpatty, 96, 97

D

deauthentication attack, *Patrz:*
 atak anulowanie
 uwierzytelnienia
default regulatory settings,
 Patrz: karta sieciowa
 domyślne ustawienia
 wymogów prawnych

Denial of Service, *Patrz:* atak
 typu odmowa usługi
disassociation attacks, *Patrz:*
 atak anulowanie skojarzenia
Dnsspoof, 158, 160
DoS, *Patrz:* atak typu odmowa
 usługi
dziennik połączeń, 27

E

evil twin, *Patrz:* atak typu
 złośliwy bliźniak

F

firewall, *Patrz:* zaporą sieciową
four-way handshake, *Patrz:*
 uwierzytelnianie negocjacja
 czteroetapowa
frame control, *Patrz:* ramka pole
 sterujące
FreeRadius WPE, 168, 169, 171

I

identyfikator
 BSSID, 116, 118
 ESSID, 116, 130
 SSID, 55, 89, 148
 ujawnianie, 58, 59
 ukrywanie, 56, 57
initialization vector, *Patrz:*
 wektor inicjalizujący
interfejs
 sieciowy, 33, 36
 TAP, 148

intrusion prevention system,
Patrz: system wykrywania
 włamań
 IV, *Patrz:* wektor inicjalizujący

K

Kali Linux, 19
 instalowanie, 19
 na dysku USB, 21
 w maszynie wirtualnej, 21
 karta
 Alfa AWUS036H, 18
 Edimax EW-7711UAN, 18
 sieciowa
 adres MAC, 25, 27
 domyślne ustawienia
 wymogów prawnych,
 48, 51
 interfejs sieciowy, 25
 konfigurowanie, 24, 26
 keystream, *Patrz:* klucz strumień
 klient bezprzewodowy, 129
 klucz
 łamanie, 182
 PMK, 97
 PSK, 89, 97
 PTK, 89
 sesji, 89
 strumień, 66, 68
 WEP, 65, 135, 138
 podłączanie do sieci, 102
 WPA
 atak, 182
 łamanie, 129, 143, 144, 145
 podłączanie do sieci, 103
 współdzielony, 65, 66, 89
 kod MIC, 89
 komenda
 airbase-ng, 118, 137
 aircrack-ng, 61, 86, 88, 94, 95,
 97
 airdecap-ng, 101
 aireplay-ng, 45, 58, 68, 71, 82,
 83, 110
 airmon-ng, 34, 35
 airmon-ng start wlan0, 78
 airodump-ng, 47, 62, 63, 66,
 78, 83, 110, 118, 131, 133,
 136, 190

airodump-ng --bssid, 42
 airolib-ng, 99
 brctl addbr, 149
 brctl addif, 149
 dnsspoof, 158
 genpmk, 97
 ifconfig mon0, 35
 iwconfig mon0 channel, 43
 ifconfig wlan0
 netmask, 27
 up, 78
 ifconfig wlan1, 34
 iw reg set, 48
 iwconfig, 33, 102
 iwconfig mon0, 43, 46
 iwconfig wlan0
 essid, 65
 iwlist wlan0
 essid, 27
 scanning, 26
 macchanger, 63
 Pyrit, 99
 radiusd, 170
 reaver, 188
 tshark, 190
 Wireshark &, 36

L

laboratorium sieci
 bezprzewodowych, 17
 budowa, 18
 lista preferowanych sieci, 130

M

maszyna wirtualna
 VirtualBox, 21
 mechanizm
 nasłuchiwania pakietów, 18,
 24, 31, 43
 wstrzykiwania pakietów, 18,
 24, 31, 45
 Message Integrity Check,
 Patrz: kod MIC
 metoda bit-flipping, 138
 most sieciowy, 120, 123, 148, 149
 adres IP, 149

O

Open Authentication, *Patrz:* sieć
 z otwartym dostępem

P

packet injection, *Patrz:*
 mechanizm wstrzykiwania
 pakietów
 packet sniffing, *Patrz:*
 mechanizm nasłuchiwania
 pakietów
 Pairwise Transient Key, *Patrz:*
 klucz PTK
 pakiet
 aircrack-ng, 61
 ARP, 44, 138
 nasłuchiwanie, *Patrz:*
 mechanizm nasłuchiwania
 pakietów
 Probe Request, 59, 60
 Probe Response, 59, 60
 przechwytywanie, 36, 37, 42,
 Patrz: mechanizm
 nasłuchiwania pakietów
 filtowanie, 38, 39, 41, 42
 rozgłoszeniowy
 anulowania
 uwierzytelnienia, 112,
 114
 sondowania, 131, 161, 164,
 190, 193
 Wireshark, *Patrz:* Wireshark
 wstrzykiwanie, *Patrz:*
 mechanizm wstrzykiwania
 pakietów
 PNL, *Patrz:* lista preferowanych
 sieci
 podsłuchiwanie ruchu sieciowego,
 152
 polecenie, *Patrz:* komenda
 Preferred Network List, *Patrz:*
 lista preferowanych sieci
 Pre-Shared Key, *Patrz:* klucz PSK
 Probe Request, *Patrz:* pakiet
 sondowania
 program, *Patrz też:* komenda
 Wireshark, *Patrz:* Wireshark

promiscuous mode, *Patrz:* tryb nasłuchiwania
 protokół, *Patrz też:* szyfrowanie 802.11, 14
 EAP, 88, 171
 EAP-TLS, 176
 EAP-TTLS, 175, 177
 MSCHAP v2, 175
 PEAP, 171, 176
 konfigurowanie, 175
 łamanie zabezpieczeń, 172
 PEAPv0, 171
 PEAPv1, 171
 PSK, 88
 WEP, 66, 75, 76, 135
 przelamywanie
 zabezpieczeń, 77, 85, 88
 WPA, 75, 76, 88
 WPA2, 76
 WPA-Enterprise, 167, 177, 182
 przechwytywanie sesji, 157, 160
 modyfikacja danych, 161
 punkt dostępowy, 18, 21
 adres IP, 22
 adres MAC, 27, 89, 144
 fałszowanie, 107, 114, 115, 116
 dziennik połączeń, *Patrz:* dziennik połączeń
 fałszywy, 133, 137, 148
 FreeRadius WPE, 169
 konfiguracja zabezpieczeń, 161, 164
 konfigurowanie, 22, 24
 łamanie hasła, 109
 nieautoryzowany, 107, 120, 123
 tablica połączeń, 72
 tryb otwartego dostępu, *Patrz:* tryb otwartego dostępu
 Python, 190, 191, 193, 194

R

ramka
 danych, 33, 39
 podtyp, 32, 33, 40
 pole sterujące, 32
 rozgłoszeniowa, 56
 sterująca, 33, 39

zarządzająca, 32, 39
 Reaver, 188
 Remote Authentication Dial In User Service, *Patrz:* serwer Radius
 rogue access point, *Patrz:* punkt dostępowy nieautoryzowany
 router TP-LINK TL-WR841N Wireless, 18, 21, 108

S

serwer Radius, 88, 168
 Shared Key Authentication, *Patrz:* uwierzytelnienie
 klucz współdzielony
 sieć
 bezprzewodowa
 częstotliwość, 45, 46, 48
 infrastruktura, 107, 183
 kanał, 46
 laboratorium, *Patrz:* laboratorium sieci
 bezprzewodowych
 ramka, *Patrz:* ramka
 rozpoznanie, 181
 sondowanie, 59, 130, 135, 161, 164, 189, 193
 WLAN, 32
 z otwartym dostępem, 55
 uwierzytelnienie, *Patrz:* uwierzytelnienie
 z otwartym dostępem, 64
 preferowana, 130
 strumień klucza, *Patrz:* klucz strumień
 Supplicant Nonce, *Patrz:* wartość losowa SNonce
 system wykrywania włamań, 120
 szyfrowanie, 76
 algorytm, *Patrz:* algorytm
 WEP, 24, 28, 76, 77, 85, 88, 119, 140
 podłączanie do sieci, 102
 WPA, 24, 76, 88, 119, 140
 podłączanie do sieci, 103
 WPA2, 76
 WPS, 185
 atak, 186
 wady, 186

T

Temporal Key Integrity Protocol, *Patrz:* algorytm TKIP
test
 penetracyjny, 17, 18, 102, 147
 atak, 182
 metodologia, 179
 planowanie, 180
 raport, 183
 wstrzykiwania pakietów, 45
tryb
 monitora, 33, 36
 nasłuchiwania, 33
 otwartego dostępu, 24
 skakania po kanałach, 46, 47
 szyfrowany, *Patrz:* szyfrowanie

U

uwierzytelnianie
 fałszowanie, 88
 klucz współdzielony, 65, 66
 negocjacja czteroetapowa, 88, 89, 92, 97

W, Z

wartość losowa
 ANonce, 89, 144
 SNonce, 89, 144
 wektor inicjalizujący, 76
WiFi Pineapple, 185
 WiFishing, 164
 Wired Equivalent Privacy, *Patrz:* klucz WEP
 Wired Equivalent Protocol, *Patrz:* protokół WEP
 Wireless Eavesdropping, *Patrz:* podsłuchiwanie ruchu sieciowego
 Wireless Protected Setup, *Patrz:* szyfrowanie WPS
 Wireshark, 36, 101, 131, 138
 filtr, 38, 39, 41, 42, 43, 44, 59
 Follow a stream, 44
 Wright Joshua, 168
 wyszukiwarka Google, 157
 zapor sieciowa, 120

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**

Kali Linux

Audyt bezpieczeństwa sieci Wi-Fi dla każdego

Wydanie II

Sieci Wi-Fi obecnie można znaleźć wszędzie — coraz trudniej o miejsce, w którym nie będziemy w zasięgu przynajmniej jednej z nich. Taka sytuacja ma jedną wadę: brak możliwości fizycznej kontroli dostępu do sygnału. Zastanawiasz się, czy Twoja sieć jest bezpieczna i czy żadna postronna osoba nie ma możliwości podłączenia się do wewnętrznych zasobów? To są kluczowe pytania, na które musisz poznać odpowiedź, od tego zależy bezpieczeństwo użytkowników i przetwarzanych danych.

Jak się przekonać, czy Twoja sieć jest całkowicie bezpieczna? Spróbuj się do niej włamać! Testy penetracyjne to najsukursniejsza technika weryfikacji bezpieczeństwa systemów informatycznych. Kali Linux to popularna i zaawansowana dystrybucja systemu Linux, zawierająca zestaw niezbędnych narzędzi każdego pentestera. Jeżeli chcesz wykorzystać jej potencjał, w tej książce znajdziesz szczegółowe omówienie dostępnych narzędzi oraz sposobów prowadzenia ataków. Szyfrowania WEP, WPA/WPA2 mają swoje słabe strony, które może wykorzystać potencjalny intruz, a ataki typu Honeypot, Misassociation, Caffee Latte to tylko niektóre z opisanych tu technik. Dzięki lekturze kolejnych rozdziałów będziesz w stanie sprawdzić podatność na zaawansowane ataki Man-in-the-Middle oraz poznasz metodologię prowadzenia testów penetracyjnych. Sięgnij po tę książkę i zbuduj własne laboratorium do testowania bezpieczeństwa sieci Wi-Fi.

Zainwestuj w bezpieczeństwo Twojej sieci bezprzewodowej!



Sięgnij po tę książkę i:

- poznaj metody zabezpieczania sieci bezprzewodowych
- przeanalizuj typowe ataki na sieci Wi-Fi
- wykryj ukryte sieci
- przechwyć dane przesyłane przez sieć bezprzewodową
- uzyskaj klucze szyfrujące transmisję

Vivek Ramachandran — związany z bezpieczeństwem sieci Wi-Fi od ponad 12 lat. Pomysłodawca ataku znanego pod nazwą Caffee Latte. Złamał sposób szyfrowania WEP. W środowisku znany jako założyciel serwisu SecurityTube.net. Występuje jako prelegent na wielu konferencjach poświęconych bezpieczeństwu.

Cameron Buchanan — pentester, autor książek. W swojej karierze przeprowadził audyty bezpieczeństwa dla wielu organizacji.

[PACKT] open source
PUBLISHING community experience distilled

Helion

37699 numer katalogowy

księgarnia internetowa

<http://helion.pl>

zamówienia telefoniczne

0 801 339900

0 601 339900

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

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

Informatyka w najlepszym wydaniu

sięgnij po WIĘCEJ



KOD KORZYŚCI

ISBN 978-83-283-1611-9



9 788328 316119

cena: 49,00 zł