

SZKOŁA HAKERÓW

Raport Specjalny

Ataki na sieci bezprzewodowe.
Teoria i praktyka.



Tytuł: Ataki na sieci bezprzewodowe. Teoria i praktyka.

ISBN: 978-83-923745-2-7

Copyright © 2010 by Wydawnictwo CSH.

All Rights Reserved.

Autorami poszczególnych rozdziałów są: Mariusz Gliwiński (rozdziały 1–5),
Robert Dylewski (rozdziały 6–7).

Korekta merytoryczna: Jakub Kałużny, Roger Zacharczyk

Skład: Aдекватna

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.

Autorzy oraz wydawnictwo CSH 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. Autorzy oraz wydawnictwo CSH nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wydawnictwo CSH

82-500 Kwidzyn

ul. Długa 27

e-mail: wydawnictwo@csh.pl


Najnowsze informacje związane z projektem Szkoły Hakerów, znajdziecie Państwo pod adresem <http://www.SzkolaHakerow.pl>. Serdecznie zapraszamy!

Printed in Poland.



Spis treści

Wskazówki prawne	9
Art. 267.	9
Art. 268.	10
Art. 268a.	11
Art. 269.	11
Art. 269a.	12
Art. 269b.	12
Rozdział 1. Wprowadzenie do sieci bezprzewodowych	15
Wstęp	15
Standardy przesyłu danych	17
Rodzaje sieci bezprzewodowych 802.11	20
Standardy szyfrowania i uwierzytelniania	22
Obsługa kart bezprzewodowych w systemie Linux	25
Rozdział 2. Omówienie półśrodków traktowanych jako zabezpieczenie sieci	27
Ochrona poprzez filtrowanie adresów MAC	27
Wyłączenie rozgłaszania ESSID	32
Ograniczenie zasięgu sieci	34



Rozdział 3. Ataki niezależne od standardu szyfrowania	35
Wstęp	35
DoS – RF jamming	37
DoS – CSMA/CA jamming	39
DoS – deauthentication attack	40
MITM w sieciach bezprzewodowych	42
Rozdział 4. Ataki na WEP	45
Szyfrowanie informacji w WEP	46
Chop-Chop	50
Keystream reuse	54
Narzędzie packetforge-ng	54
Narzędzie easside-ng	62
FMS, ataki KoreK'a, PTW	67
Interactive packet replay	73
ARP request attack	75
Caffe Latte Attack	77
Rozdział 5. Ataki na WPA	79
Wstęp	79
WPA	81
WPA2	86
Rainbow Tables	91
Atak przy użyciu aplikacji cowpatty	93
DoS – wykorzystanie blokady błędnej MIC	95
Rozdział 6. Ataki z wykorzystaniem technologii CUDA	97
Czym jest CUDA?	97
Karta graficzna nie tylko do gier?	98
Sterowniki i konfiguracja środowiska	100
Sterowniki Nvidia	100
Instalacja CUDA-Toolkit oraz SDK	104
Cowpatty	106
Pyrit	107
Aircrack-ng	114
Podkręcanie GPU w Linux-ie	118
CUDA w akcji – ataki na sieci bezprzewodowe	123

Platforma testowa	123
Pliki testowe	123
Przygotowania do przeprowadzenia ataku	124
Pyrit – tryby generowania haszy	128
Analiza wyników	138
Słowniki	140
Dodatek A: Łamanie haszy MD4/MD5 z technologią CUDA	145
Czym jest MD5?	145
CUDA-Multiforcer	145
GPU MD5 Crack	150
Dodatek B: Badanie sieci bezprzewodowych	156
Platforma sprzętowa	156
Metodologia badania	156
Wyniki	157
Podsumowanie	158

Rozdział 7. Najnowsze, zaawansowane metody ataku

na WPA	159
Atak na WPA TKIP	159
Powstawanie pakietu	161
Licznik sekwencji TSC	163
Message Integrity Code (MIC)	163
QoS – Quality of Service , WiFi MultiMedia – WMM	164
Atak na TKIP	164
Wymagania	165
Etapy ataku:	165
Obrona	168
WPA TKIP złamany kompletnie	169
Kolejne udoskonalenie ataku Beck'a i Tews'a	172
Atak Michael Reset	176
Podsumowanie	178

Rozdział 8. Podsumowanie

179

Rozdział 9. Bibliografia

181