Spis treści

O autorze **9**

O recenzentach **9**

Wstęp **11**

CZĘŚĆ 1. Wprowadzenie i konfiguracja

ROZDZIAŁ 1

Przechowywanie haseł — matematyka, prawdopodobieństwo i złożoność **15**

Czym jest łamanie haseł? 15
Ataki słownikowe 16
Ataki kombinowane 16
Ataki siłowe 17
Ataki hybrydowe 17
Ataki oparte na częściowej wiedzy, zwane też atakami z maską 18
Jak hasła są używane i przechowywane? 18
Skróty 19
Szyfrowanie 19
Dlaczego niektóre hasła są łatwiejsze do złamania od innych? 20
Długość hasła 20
Złożoność hasła 22
Pora na wykonanie skrótu lub zaszyfrowanie hasła 23
Trochę na temat „etycznego" łamania haseł 24
Podsumowanie 24

ROZDZIAŁ 2

Po co łamać hasła, jeśli wystarczy OSINT? **25**

Jak OSINT pomaga w łamaniu haseł? 25
Wykorzystanie OSINT do dostępu do ujawnionych haseł 26
Wykorzystanie OSINT do uzyskania kandydatów na hasła 31
Podsumowanie 33

ROZDZIAŁ 3

Budowa własnego środowiska łamania haseł 34

Wymagania techniczne 35
Instalacja i wprowadzenie do narzędzia John the Ripper 35
Podstawowe funkcje Johna 39
Instalacja hashcata 40
Podstawowe funkcje hashcata 45
Podsumowanie 45

ROZDZIAŁ 4

Reguły aplikacji John i hashcat 46

Analizowanie reguł złożoności haseł 46
Wybieranie i używanie reguł Johna 48
Wybieranie i używanie reguł hashcata 52
Podsumowanie 56

CZĘŚĆ 2. Zbieranie i łamanie

ROZDZIAŁ 5

Łamanie haseł w systemach Windows i macOS 59

Zbieranie skrótów haseł systemu Windows 60
Kerberos 62
Łamanie skrótów systemu Windows 64
Zbieranie skrótów haseł macOS 65
Formatowanie lub przekształcanie skrótów do oczekiwanych formatów 66
Łamanie skrótów 68
Podsumowanie 69

ROZDZIAŁ 6

Łamanie haseł w systemie Linux 70

Zbieranie skrótów haseł systemu Linux 71
Formatowanie lub przekształcanie skrótów do oczekiwanych formatów 78
Łamanie skrótów 80
Podsumowanie 81

ROZDZIAŁ 7

Łamanie haseł w bezprzewodowych sieciach WPA/WPA2 82

Uwaga dotycząca WEP 82
Architektura WPA/WPA2 85

Uzyskiwanie informacji WPA/WPA2 w celu złamania zabezpieczeń 87
Metody łamania haseł WPA/WPA2 89
Podsumowanie 91

ROZDZIAŁ 8
Łamanie haseł aplikacji WordPress, Drupal i Webmin 92
Zbieranie i formatowanie skrótów WordPressa 92
Łamanie skrótów WordPressa 94
Zbieranie i formatowanie skrótów Drupala 96
Łamanie skrótów Drupala 98
Zbieranie i formatowanie skrótów Webmina 100
Łamanie skrótów Webmina 102
Podsumowanie 104

ROZDZIAŁ 9
Łamanie haseł do sejfów 105
Zbieranie skrótów haseł KeePassa 106
Łamanie skrótów haseł KeePassa 107
Zbieranie skrótów haseł LastPassa 110
Łamanie haseł LastPassa 114
Zbieranie skrótów haseł 1Passworda 115
Łamanie skrótów haseł 1Passworda 117
Podsumowanie 118

ROZDZIAŁ 10
Łamanie haseł do portfeli kryptowalut 119
Objaśnienie kryptowalut i łańcucha bloków 119
Zbieranie i formatowanie skrótów portfela bitcoina/litecoina 120
Łamanie skrótów portfeli bitcoina/litecoina 123
Zbieranie i formatowanie skrótów portfela Ethereum 125
Łamanie skrótów portfela Ethereum 128
Podsumowanie 131

CZĘŚĆ 3. Wnioski

ROZDZIAŁ 11
Ochrona przed atakami polegającymi na łamaniu haseł 135
Jak wybrać hasło bardziej odporne na próby złamania? 135
Dodatkowe zabezpieczenia przed próbami złamania 139
Podsumowanie 140