

Spis treści

Podziękowania	15
Wprowadzenie	17

ROZDZIAŁ 1. PODSTAWY DZIAŁANIA SIECI I ANALIZY PAKIETÓW 23

Analiza pakietów i sniffery pakietów	24
Ocena aplikacji typu sniffer pakietów	24
Jak działa sniffer pakietów?	26
W jaki sposób komunikują się komputery?	26
Protokoły	26
Siedem warstw modelu OSI	27
Sprzęt sieciowy	33
Klasyfikacje ruchu sieciowego	38
Ruch typu broadcast	39
Ruch typu multicast	40
Ruch typu unicast	40
Podsumowanie	40

ROZDZIAŁ 2. DOBRANIE SIĘ DO SIECI 41

Tryb mieszany	42
Przechwytywanie pakietów z koncentratorów	43
Przechwytywanie pakietów w środowisku sieci opartej na przełączniku sieciowym	45
Kopiowanie ruchu na wskazany port	46

Technika hubbing out	48
Użycie rozgałęźnika	49
Zatrucie bufora ARP	52
Przechwytywanie pakietów w środowisku sieci opartej na routerze	58
Praktyczne wskazówki dotyczące umieszczania sniffera pakietów	59
ROZDZIAŁ 3. WPROWADZENIE DO NARZĘDZIA WIRESHARK	63
Krótką historią narzędzia Wireshark	63
Zalety narzędzia Wireshark	64
Instalowanie narzędzia Wireshark	65
Instalowanie Wireshark w systemie Windows	66
Instalowanie narzędzia Wireshark w systemie Linux	68
Instalowanie narzędzia Wireshark w systemie macOS	70
Podstawy używania narzędzia Wireshark	71
Twoje pierwsze przechwycone pakiety	71
Okno główne narzędzia Wireshark	72
Preferencje narzędzia Wireshark	73
Kolorowanie pakietów	75
Pliki konfiguracyjne	77
Profile konfiguracyjne	78
ROZDZIAŁ 4. PRACA Z PRZECHWYCONYMI PAKIETAMI	81
Praca z plikami zawierającymi przechwycone dane	81
Zapis i eksport plików zawierających przechwycone dane	82
Łączenie plików zawierających przechwycone dane	83
Praca z pakietami	84
Wyszukiwanie pakietów	84
Oznaczanie pakietów	85
Wydruk pakietów	86
Konfiguracja formatu wyświetlania czasu i odniesień	87
Format wyświetlania czasu	87
Odniesienie czasu do pakietu	88
Przesunięcie czasu	89
Konfiguracja opcji przechwytywania danych	89
Karta Input	90
Karta Output	90
Karta Options	92
Używanie filtrów	94
Filtry przechwytywania	94
Filtry wyświetlania	101
Zapis filtrów	104
Dodanie filtrów wyświetlania do paska narzędzi	105

ROZDZIAŁ 5. ZAAWANSOWANE FUNKCJE NARZĘDZIA WIRESHARK 107

Konwersacje i punkty końcowe sieci	107
Przeglądanie danych statystycznych punktów końcowych	108
Przeglądanie konwersacji sieciowych	110
Identyfikowanie za pomocą okien Endpoints i Conversations punktów kontrolnych generujących największą ilość ruchu sieciowego	111
Okno Protocol Hierarchy Statistics	113
Określanie nazw	115
Włączenie funkcji określania nazw	115
Potencjalne wady określania nazw	117
Użycie własnego pliku hosts	117
Ręczne zainicjowanie określania nazw	119
Szczegółowa analiza protokołu	119
Zmiana dekodera	119
Wyświetlanie kodu źródłowego dekodera	122
Funkcja Follow Stream	122
Funkcja Follow SSL Stream	124
Wielkość pakietu	125
Grafika	126
Wykres operacji wejścia-wyjścia	127
Wykres czasu podróży	130
Wykres przepływu danych	131
Informacje zaawansowane	132

ROZDZIAŁ 6. ANALIZA PAKIETÓW Z POZIOMU WIERSZA POLECEŃ 135

Instalowanie tshark	136
Instalowanie tcpdump	137
Przechwytywanie i zapisywanie pakietów	138
Manipulowanie danymi wyjściowymi	142
Określanie nazw	145
Stosowanie filtrów	146
Formaty wyświetlania daty i godziny w narzędziu tshark	148
Podsumowanie danych statystycznych w narzędziu tshark	149
Porównanie narzędzi tshark i tcpdump	153

ROZDZIAŁ 7. PROTOKOŁY WARSTWY SIECIOWEJ 155

Protokół ARP	156
Struktura pakietu ARP	157
Pakiet 1.: żądanie ARP	158
Pakiet 2.: odpowiedź ARP	159
Bezpłatny pakiet ARP	159
Protokół IP	161
Internet Protocol Version 4 (IPv4)	161
Internet Protocol Version 6 (IPv6)	169

Protokół ICMP	182
Struktura pakietu ICMP	182
Wiadomości i typy ICMP	182
Żądania echo i odpowiedzi na nie	183
Polecenie traceroute	185
Protokół ICMPv6	188

ROZDZIAŁ 8. PROTOKOŁY WARSTWY TRANSPORTOWEJ 191

Protokół TCP	191
Struktura pakietu TCP	192
Porty TCP	192
Trzyetapowy proces negocjacji TCP	195
Zakończenie komunikacji TCP	198
Zerowanie TCP	199
Protokół UDP	201
Struktura pakietu UDP	201

ROZDZIAŁ 9. NAJCZĘŚCIEJ UŻYWANE PROTOKOŁY WYŻSZYCH WARSTW 203

Protokół DHCP	203
Struktura pakietu DHCP	204
Proces odnowy DHCP	204
Proces odnowy dzierżawy DHCP	210
Opcje DHCP i typy wiadomości	211
DHCP Version 6 (DHCPv6)	211
Protokół DNS	213
Struktura pakietu DNS	214
Proste zapytanie DNS	215
Typy zapytań DNS	216
Rekurencja DNS	218
Transfer strefy DNS	221
Protokół HTTP	223
Przeglądanie zasobów za pomocą HTTP	224
Przekazywanie danych za pomocą HTTP	227
Protokół SMTP	227
Wysyłanie i odbieranie poczty elektronicznej	228
Śledzenie poczty elektronicznej	230
Wysyłanie załączników za pomocą SMTP	237
Podsumowanie	240

ROZDZIAŁ 10. NAJCZĘŚCIEJ SPOTYKANE SYTUACJE 241

Brakująca treść witryny internetowej	242
Dobranie się do sieci	242
Analiza	243
Wnioski	247

Oporna usługa prognozy pogody	247
Dobranie się do sieci	247
Analiza	249
Wnioski	252
Brak dostępu do internetu	253
Problem związany z konfiguracją	253
Niechciane przekierowanie	256
Problemy związane z przekazywaniem danych	260
Nieprawidłowo działająca drukarka	263
Dobranie się do sieci	263
Analiza	263
Wnioski	266
Uwięzieni w oddziale	266
Dobranie się do sieci	267
Analiza	267
Wnioski	270
Błąd programisty	270
Dobranie się do sieci	271
Analiza	271
Wnioski	273
Podsumowanie	274

ROZDZIAŁ I I. ZMAGANIA Z WOLNO DZIAŁAJĄCĄ SIECIĄ 275

Funkcje usuwania błędów protokołu TCP	276
Ponowna transmisja pakietu TCP	276
Duplikaty potwierdzeń TCP i szybka retransmisja	279
Kontrola przepływu danych TCP	284
Dostosowanie wielkości okna	286
Wstrzymanie przepływu danych i powiadomienie o zerowej wielkości okna odbiorcy	287
Mechanizm przesuwającego się okna TCP w praktyce	288
Wnioski płynące z usuwania błędów protokołu TCP i kontroli przepływu danych	291
Lokalizacja źródła opóźnień	292
Normalna komunikacja	293
Wolna komunikacja — opóźnienie z winy sieci	293
Wolna komunikacja — opóźnienie po stronie klienta	294
Wolna komunikacja — opóźnienie po stronie serwera	295
Struktury pozwalające na wyszukiwanie opóźnień	296
Punkt odniesienia dla sieci	296
Punkt odniesienia dla miejsca	297
Punkt odniesienia dla komputera	298
Punkt odniesienia dla aplikacji	300
Informacje dodatkowe dotyczące punktów odniesienia	300
Podsumowanie	301

ROZDZIAŁ 12. ANALIZA PAKIETÓW I ZAPEWNIANIE BEZPIECZEŃSTWA	303
Rozpoznanie systemu	304
Skanowanie TCP SYN	305
Wykrywanie systemu operacyjnego	309
Manipulacje ruchem sieciowym	313
Zatrucie bufora ARP	313
Przechwycenie sesji	317
Malware	321
Operacja Aurora	322
Koń trojański umożliwiający zdalny dostęp	328
Zestaw automatyzujący atak i Ransomware	336
Podsumowanie	343
ROZDZIAŁ 13. ANALIZA PAKIETÓW W SIECI BEZPRZEWODOWEJ	345
Względy fizyczne	346
Przechwytywanie danych tylko jednego kanału w danej chwili	346
Zakłócenia sygnału bezprzewodowego	347
Wykrywanie i analizowanie zakłóceń sygnału	347
Tryby działania kart sieci bezprzewodowych	349
Bezprzewodowe przechwytywanie pakietów w systemie Windows	351
Konfiguracja AirPcap	351
Przechwytywanie ruchu sieciowego za pomocą urządzenia AirPcap	353
Bezprzewodowe przechwytywanie pakietów w systemie Linux	354
Struktura pakietu 802.11	356
Dodanie do panelu Packet List kolumn charakterystycznych dla sieci bezprzewodowej ..	357
Filtry przeznaczone dla sieci bezprzewodowej	359
Filtrowanie ruchu sieciowego należącego do określonego BSS ID	359
Filtrowanie określonych typów pakietów sieci bezprzewodowej	359
Odfiltrowanie określonej częstotliwości	360
Zapis profilu sieci bezprzewodowej	361
Bezpieczeństwo w sieci bezprzewodowej	361
Zakończone powodzeniem uwierzytelnienie WEP	362
Nieudane uwierzytelnienie WEP	364
Zakończone powodzeniem uwierzytelnienie WPA	364
Nieudane uwierzytelnienie WPA	367
Podsumowanie	368
DODATEK A. CO DALEJ?	369
Narzędzia analizy pakietów	369
CloudShark	369
WireEdit	370
Cain & Abel	371
Scapy	371
TraceWrangler	371

Tcpreplay	371
NetworkMiner	371
CapTipper	372
ngrep	372
libpcap	373
npcap	373
hping	374
Python	374
Zasoby dotyczące analizy pakietów	374
Witryna domowa narzędzia Wireshark	374
Kurs internetowy praktycznej analizy pakietów	374
Kurs SANS Security Intrusion Detection In-Depth	375
Blog Chrisa Sandersa	375
Malware Traffic Analysis	375
Witryna internetowa IANA	375
Seria TCP/IP Illustrated napisana przez W. Richarda Stevensa	376
The TCP/IP Guide (No Starch Press)	376

DODATEK B. NAWIGACJA PO PAKIETACH 377

Reprezentacja pakietu	377
Użycie diagramów pakietów	380
Poruszanie się po tajemniczym pakiecie	382
Podsumowanie	385

Skorowidz	387
-----------------	-----