

# Obsah

<b>PODĚKOVÁNÍ .....</b>	<b>11</b>
<b>ÚVOD .....</b>	<b>13</b>
Cíle knihy .....	13
Koncepce a přístup .....	13
Jak s knihou pracovat .....	15
Ukázkové zachycené soubory .....	15
Nadace Rural Technology Fund .....	16
Kontakt s autorem .....	16
Zpětná vazba od čtenářů .....	16
Errata .....	17
 <b>KAPITOLA 1</b>	
<b>ÚVOD DO ANALÝZY PAKETŮ A SÍTÍ .....</b>	<b>19</b>
Analýza paketů a nástroje pro sledování paketů .....	20
Hodnocení paketového snifferu .....	20
Principy paketových snifferů .....	21
Principy komunikace počítačů .....	22
Protokoly .....	22
Model OSI se sedmi vrstvami .....	22
Zapouzdření dat .....	25
Síťový hardware .....	28
Klasifikace provozu .....	33
Všesměrový provoz .....	33
Vícesměrový provoz .....	34

Jednosměrový provoz .....	34
Závěrečné poznámky .....	34

## KAPITOLA 2

<b>NAPÍCHNUTÍ LINKY .....</b>	<b>35</b>
Promiskuitní život .....	35
Sledování s rozbočovači .....	37
Sledování v přepínaném prostředí .....	38
Zrcadlení portu .....	39
Rozbočování .....	40
Použití odposlechu .....	42
Znehodnocení mezipaměti ARP .....	45
Sledování ve směrovaném prostředí .....	49
Umístění snifferu v praxi .....	50

## KAPITOLA 3

<b>ÚVOD DO PROGRAMU WIRESHARK .....</b>	<b>53</b>
Stručná historie programu Wireshark .....	53
Výhody programu Wireshark .....	54
Instalace programu Wireshark .....	55
Instalace v systémech Microsoft Windows .....	55
Instalace v systémech Linux .....	57
Instalace v systémech Mac OS X .....	59
Základy programu Wireshark .....	59
První zachycené pakety .....	59
Hlavní okno programu Wireshark .....	60
Předvolby programu Wireshark .....	62
Barevné kódování paketů .....	63

## KAPITOLA 4

<b>ZPRACOVÁNÍ ZACHYCENÝCH PAKETŮ .....</b>	<b>67</b>
Zpracování zachycených souborů .....	67
Ukládání a export zachycených souborů .....	67
Sloučení zachycených souborů .....	69
Zpracování paketů .....	70
Hledání paketů .....	70
Označování paketů .....	71
Tisk paketů .....	71

Nastavení formátu zobrazení času a referencí . . . . .	72
Formáty zobrazení času . . . . .	72
Referenční čas paketu . . . . .	73
Nastavení možností zachytávání . . . . .	74
Nastavení Capture . . . . .	74
Nastavení Capture File(s) . . . . .	75
Nastavení Stop Capture . . . . .	77
Nastavení Display Options . . . . .	77
Nastavení Name Resolution . . . . .	77
Použití filtrů . . . . .	77
Filtry zachytávání . . . . .	78
Filtry zobrazení . . . . .	84
Ukládání filtrů . . . . .	87

## KAPITOLA 5

### **POKROČILÉ FUNKCE PROGRAMU WIRESHARK . . . . .89**

Koncové body sítě a konverzace . . . . .	89
Zobrazení koncových bodů . . . . .	90
Zobrazení síťových konverzací . . . . .	91
Řešení potíží pomocí oken Endpoints a Conversations . . . . .	92
Okno Protocol Hierarchy Statistics . . . . .	94
Překlad názvů . . . . .	95
Povolení překladu názvů . . . . .	95
Potenciální nevýhody překladu názvů . . . . .	96
Rozbor protokolů . . . . .	96
Změna disektoru . . . . .	97
Zobrazení zdrojového kódu disektoru . . . . .	99
Sledování datových proudů TCP . . . . .	99
Okno Packet Lengths . . . . .	101
Vytváření grafů . . . . .	102
Zobrazení vstupně-výstupních grafů . . . . .	102
Grafy času obousměrného přenosu . . . . .	104
Grafy toku . . . . .	106
Expertní informace . . . . .	106

## KAPITOLA 6

### **BĚŽNÉ PROTOKOLY NIŽŠÍCH VRSTEV . . . . .109**

Protokol ARP (Address Resolution Protocol) . . . . .	109
Hlavička ARP . . . . .	111

Paket 1: požadavek ARP .....	112
Paket 2: odpověď ARP .....	113
Nevyžádané ARP .....	114
Protokol IP (Internet Protocol) .....	115
IP adresy .....	116
Hlavička IPv4 .....	117
Time to Live .....	118
Fragmentace IP .....	120
Protokol TCP (Transmission Control Protocol) .....	123
Hlavička TCP .....	123
Porty TCP .....	124
Trojcestné ověřování TCP typu handshake .....	127
Proces TCP teardown .....	130
Reset TCP .....	131
Protokol UDP (User Datagram Protocol) .....	132
Hlavička UDP .....	133
Protokol ICMP (Internet Control Message Protocol) .....	134
Hlavička ICMP .....	134
Typy a zprávy ICMP .....	134
Požadavky a odpovědi echo .....	135
Traceroute .....	138

## KAPITOLA 7

### **BĚŽNÉ PROTOKOLY VYŠŠÍ VRSTVY .....**

Protokol DHCP (Dynamic Host Configuration Protocol) .....	141
Struktura paketu DHCP .....	142
Proces obnovení DHCP .....	143
Obnovení během zápůjčky protokolu DHCP .....	148
Možnosti a typy zpráv protokolu DHCP .....	148
Systém DNS (Domain Name System) .....	149
Struktura paketu DNS .....	149
Jednoduchý dotaz DNS .....	151
Typy dotazů DNS .....	152
Rekurze DNS .....	153
Přenosy zóny DNS .....	156
Protokol HTTP (Hypertext Transfer Protocol) .....	159
Prohlížení webu pomocí HTTP .....	159
Odesílání dat protokolem HTTP .....	161
Závěrečné poznámky .....	162

**KAPITOLA 8**

<b>BĚŽNÉ SCÉNÁŘE Z PRAXE . . . . .</b>	<b>163</b>
Sociální sítě na úrovni paketů . . . . .	164
Zachytávání provozu služby Twitter . . . . .	164
Zachytávání provozu služby Facebook . . . . .	168
Porovnání metod Twitteru a Facebooku . . . . .	170
Zachytávání provozu služby ESPN.com . . . . .	170
Použití okna Conversations . . . . .	171
Použití okna Protocol Hierarchy Statistics . . . . .	171
Zobrazení provozu DNS . . . . .	172
Zobrazení požadavků HTTP . . . . .	173
Praktické problémy . . . . .	174
Nedostupný Internet: konfigurační problémy . . . . .	174
Nedostupný Internet: nežádoucí přesměrování . . . . .	177
Nedostupný Internet: problémy mimo lokální síť . . . . .	181
Nespolehlivá tiskárna . . . . .	183
Izolovaná pobočka . . . . .	187
Naštvaný vývojář . . . . .	190
Závěrečné poznámky . . . . .	195

**KAPITOLA 9**

<b>ZRYCHLENÍ POMALÉ SÍTĚ . . . . .</b>	<b>197</b>
Funkce opravy chyb protokolu TCP . . . . .	198
Opakované přenosy TCP . . . . .	198
Duplicitní potvrzení TCP a rychlé opakované přenosy . . . . .	201
Řízení toku TCP . . . . .	206
Úpravy hodnoty Window Size . . . . .	207
Zastavení toku dat pomocí oznámení nulové velikosti okna . . . . .	208
Posuvné okno protokolu TCP v praxi . . . . .	209
Poučení z paketů opravy chyb a řízení toku protokolu TCP . . . . .	213
Určení zdroje vysoké latence . . . . .	213
Normální komunikace . . . . .	214
Pomalá komunikace – latence linky . . . . .	214
Pomalá komunikace – latence klienta . . . . .	216
Pomalá komunikace – latence serveru . . . . .	216
Schéma určování zdroje latence . . . . .	217
Standardní hodnoty sítě . . . . .	218
Standardní hodnoty lokality . . . . .	218
Standardní hodnoty hostitele . . . . .	219

Standardní hodnoty aplikace .....	220
Další poznámky ke standardním hodnotám .....	221
Závěrečné poznámky .....	221

## KAPITOLA 10

### **ANALÝZA PAKETŮ A ZABEZPEČENÍ .....**

Průzkum .....	223
Skenování SYN .....	224
Zjišťování otisků operačního systému .....	229
Napadení systému .....	232
Operace Aurora .....	232
Znehodnocení mezipaměti ARP .....	238
Trojský kůň se vzdáleným přístupem .....	242
Závěrečné poznámky .....	250

## KAPITOLA 11

### **ANALÝZA**

### **BEZDRÁTOVÝCH PAKETŮ .....**

Fyzická hlediska .....	251
Postupné sledování jednotlivých kanálů .....	251
Interference bezdrátového signálu .....	253
Detekce a analýza interference signálu .....	253
Režimy bezdrátových karet .....	254
Bezdrátové sledování v systému Windows .....	256
Konfigurace karty AirPcap .....	256
Zachytávání provozu pomocí zařízení AirPcap .....	257
Bezdrátové sledování v systému Linux .....	259
Struktura paketu 802.11 .....	260
Doplnění sloupců specifických pro bezdrátové sítě do podokna Packet List .....	262
Filtry specifické pro bezdrátové sítě .....	263
Filtrování provozu podle konkrétní hodnoty BSS ID .....	263
Filtrování konkrétních typů bezdrátových paketů .....	264
Filtrování konkrétní frekvence .....	265
Zabezpečení bezdrátové sítě .....	266
Úspěšná autentizace WEP .....	266
Neúspěšná autentizace WEP .....	268
Úspěšná autentizace WPA .....	269

Neúspěšná autentizace WPA .....	270
Závěrečné poznámky .....	272

## PŘÍLOHA

### **DALŠÍ INFORMACE .....273**

Nástroje na analýzu paketů .....	273
tcpdump a Windump .....	273
Cain & Abel .....	274
Scapy .....	274
Netdude .....	274
Colasoft Packet Builder .....	275
CloudShark .....	275
pcapr .....	276
NetworkMiner .....	276
Tcpreplay .....	277
ngrep .....	277
libpcap .....	277
hping .....	277
Domain Dossier .....	277
Perl a Python .....	277
Informační zdroje týkající se analýzy paketů .....	278
Domovská stránka programu Wireshark .....	278
Podrobný bezpečnostní kurz detekce vniknutí pořádaný organizací SANS .....	278
Blog Chrise Sanderse .....	278
Blog Packetstan .....	279
Univerzita programu Wireshark .....	279
IANA .....	279

### **REJSTŘÍK .....281**