

Obsah

Předmluva	15
Příložené CD	15
Hlavní autorka.....	15
Odborný korektor a spoluautor.....	16
Spoluautoři.....	16
Konvence použité v knize.....	17
Poznámka redakce českého vydání	18
Kapitola 1	
Úvod do analýzy sítě	19
Úvod	20
Co je analýza sítě a sniffing?	20
Kdo používá analýzu sítě?	22
Jak sniffery používají útočníci?	23
Jak vypadají zachycená data?	24
Obvyklé síťové analyzátory.....	24
Jak funguje analýza sítě?	26
Vysvětlení Ethernetu	26
Porozumění modelu OSI (Open Systems Interconnection).....	27
Vrstva první: Fyzická.....	28
Vrstva druhá: Spojová.....	29
Vrstva třetí: Síťová	30
Vrstva čtvrtá: Transportní.....	31
Vrstva pátá: Relační	32
Vrstva šestá: Prezentační	33
Vrstva sedmá: Aplikační.....	33
CSMA/CD	35
Hlavní protokoly: IP, TCP, UDP a ICMP	35
Protokol IP.....	35
Internet Control Message Protocol.....	36
TCP.....	36
Protokol UDP.....	37
Hardware: Kabelové odbočky, rozbočovače a přepínače.....	37

Zrcadlení portů.....	39
Vítězíme nad přepínači.....	40
Odhaltování snifferů.....	42
Zachytávání dat v bezdrátových sítích	44
Hardwarové požadavky.....	44
Programové vybavení.....	45
Rozbor protokolů.....	46
DNS.....	46
NTP.....	47
HTTP.....	48
SMTP.....	49
Ochrana proti snifferům.....	51
Síťová analýza a firemní směrnice	52
Shrnutí	53
Rychlá řešení.....	54
Časté dotazy.....	56

Kapitola 2

Představujeme Wireshark:

analýzátor síťových protokolů..... 57

Úvod	58
Co je Wireshark?	58
Historie Wiresharku.....	59
Kompatibilita.....	60
Podporované protokoly.....	61
Uživatelské rozhraní programu Wireshark	63
Filtry.....	64
Doporučené zdroje.....	68
Podpůrné programy	69
Tshark.....	69
Editcap.....	71
Mergecap.....	71
Text2pcap.....	72
Používání Wiresharku ve vaší síťové architektuře.....	73
Používání Wiresharku pro řešení problémů se sítí	77
Používání Wiresharku pro administraci systému	79
Kontrola síťové konektivity.....	80
Kontrola dostupnosti síťových aplikací.....	80

Scénář 1: Zpráva SYN bez zprávy SYN+ACK.....	80
Scénář 2: Zpráva SYN s okamžitou odezvou RST	81
Scénář 3: SYN SYN+ACK ACK.....	81
Spojení ukončeno.....	81
Používání Wiresharku pro administraci zabezpečení.....	81
Odhalení aktivity IRC (Internet Relay Chat).....	81
Wireshark jako síťový systém pro detekci průniku (NIDS).....	82
Wireshark jako detektor přenosu firemních informací.....	82
Zabezpečení Wiresharku.....	82
Optimalizace Wiresharku	83
Rychlost síťového připojení.....	83
Minimalizace příslušenství Wiresharku.....	83
Procesor.....	83
Paměť.....	84
Pokročilé techniky zachytávání dat.....	84
Dsniff	84
Ettercap	86
Útoky MITM.....	86
Cracking	87
Triky s přepínačem.....	87
Falšování zpráv protokolu ARP (ARP Spoofing)	87
Zahlcování tabulky s adresami MAC (MAC Flooding).....	87
Hrajeme si se směrováním.....	88
Ochrana sítě proti zachytávání dat	88
Použití šifrování	88
SSH.....	88
SSL.....	89
Pretty Good Privacy a Secure/Multipurpose Internet Mail Extensions.....	89
Přepínání.....	89
Nasazení detekčních metod	89
Místní detekce	90
Síťová detekce	90
Dotazy DNS	90
Latence.....	91
Chyby v ovladači.....	91
NetMon.....	91
Shrnutí	92
Rychlá řešení.....	92
Časté dotazy	94

Kapitola 3

Jak získat a nainstalovat Wireshark..... 97

Úvod	98
Jak získat Wireshark	98
Platformy a požadavky na systém.....	99
Ovladače pro zachytávání paketů	100
Instalace knihovny libpcap	101
Instalace knihovny libpcap pomocí balíčků RPM.....	101
Instalace knihovny libpcap ze zdrojových kódů	103
Instalace knihovny WinPcap.....	104
Instalace Wiresharku na operačním systému Windows	105
Instalace Wiresharku na operačním systému Linux.....	106
Instalace Wiresharku pomocí balíčků RPM.....	106
Instalace Wiresharku na operačním systému Mac OS X.....	108
Instalace Wiresharku na operační systém Mac OS X ze zdrojového kódu	108
Instalace Wiresharku na Mac OS X s použitím DarwinPorts.....	111
Instalace Wiresharku na operační systém Mac OS X s použitím aplikace Fink.....	112
Instalace Wiresharku ze zdrojového kódu.....	113
Zapínání a vypínání vlastností prostřednictvím skriptu configure.....	115
Shrnutí	117
Rychlá řešení.....	117
Časté dotazy	118

Kapitola 4

Používáme Wireshark 121

Úvod	122
Začínáme s Wiresharkem	122
Seznamujeme se s Hlavním oknem.....	123
Souhrnné okno.....	124
Okno stromu protokolů	125
Okno pro zobrazení dat	127
Další části okna	128
Panel filtrů	128
Informační pole	130
Pole pro zobrazování informací	130
Seznamujeme se s nabídkami	131
Nabídka File	131

Open (Otevřít)	132
Save As (Uložit jako)	133
Print (Tisk)	135
Nabídka Edit (Editace)	138
Find Packet (Najdi paket)	140
Set Time Reference (toggle) – Nastavit časový odkaz (přepínač)	141
Preferences (Nastavení)	142
Nabídka View (Zobrazení)	143
Informace Time Display (Zobrazení času)	144
Auto Scroll in Live Capture (Automatický posun při zachytávání)	145
Apply Color Filters (Použití barevných filtrů)	145
Show Packets in New Window (Zobrazit pakety v novém okně)	147
Nabídka Go (Přejdi na)	148
Go To Packet (Přejdi na paket)	149
Nabídka Capture (Zachytávání)	150
Capture Interfaces (Rozhraní pro zachytávání)	151
Capture Options (Možnosti zachytávání)	152
Edit Capture Filter List (Editace seznamu filtrů pro zachytávání)	158
Nabídka Analyze (Analýza)	159
Edit Display Filter List (Editace seznamu filtrů pro zobrazení)	160
Apply as Filter (Použít jako filtr) a Prepare a Filter (Připravit filtr)	164
Enabled Protocols (Povolené protokoly)	165
Decode As (Dekódovat jako)	165
Decode As: Show (Dekódovat jako: Zobrazit)	167
Follow TCP Stream (Sledovat datový proud protokolu TCP) a Follow SSL Stream (Sledovat datový proud protokolu SSL)	167
Expert Info (Expertní informace) a Expert Info Composite (Složené expertní informace)	169
Nabídka Statistics (Statistiky)	169
Summary (Souhrn)	171
Protocol Hierarchy (Hierarchie protokolů)	172
Podnabídka TCP Stream Graph (Graf datového proudu protokolu TCP)	172
Nabídka Help (Nápověda)	182
Contents (Obsah)	183
Supported Protocols (Podporované protokoly)	184
Podnabídka Manual Pages (Stránky manuálu)	185
Podnabídka Wireshark Online	186
About Wireshark (O Wiresharku)	187
Místní nabídky	187
Místní nabídky Souhrnného okna	187
Místní nabídky Okna stromu protokolů	189
Místní nabídky Okna pro zobrazení dat	190

Používání voleb v příkazovém řádku.....	191
Volby pro zachytávání a práci se soubory.....	191
Možnosti filtru.....	192
Další volby.....	192
Shrnutí.....	193
Rychlá řešení.....	193
Časté dotazy.....	194

Kapitola 5

Filtry.....	197
Úvod.....	198
Tvorba zachytávacích filtrů.....	198
Vysvětlení syntaxe tcpdump.....	199
Názvy a adresy hostitelů.....	199
Hardwarové adresy.....	200
Porty.....	200
Logické operace.....	201
Protokoly.....	202
Pole protokolů.....	203
Bitové operátory.....	206
Velikost paketu.....	208
Příklady.....	209
Používání filtrů pro zachytávání.....	209
Tvorba zobrazovacích filtrů.....	211
Tvorba výrazů.....	212
Integerové hodnoty.....	214
Boolean.....	216
Čísla s pohyblivou desetinnou čárkou.....	217
Řetězce.....	217
Sekvence bajtů.....	220
Adresy.....	221
Časová pole.....	223
Další typy polí.....	223
Rozsahy.....	224
Logické operátory.....	226
Funkce.....	226
Vícenásobné výskyty v polích.....	227
Skrutá pole.....	229
Shrnutí.....	230

Rychlá řešení.....	230
Časté dotazy	231

Kapitola 6

Sniffování bezdrátových sítí pomocí Wiresharku.....233

Úvod	234
Výzvy sniffování bezdrátových sítí	234
Výběr statického kanálu.....	234
Použití channel hoppingu	235
Dosah bezdrátových sítí.....	236
Interference a kolize	236
Doporučení pro zachytávání dat v bezdrátových sítích.....	236
Operační módy bezdrátových síťových karet	237
Nastavení podpory monitorovacího módu v operačním systému Linux ..	238
Ovladače kompatibilní s rozhraním Linux Wireless Extensions.....	239
Konfigurace ovladačů MADWIFI 0.9.1	240
Zachytávání bezdrátového provozu v operačním systému Linux.....	242
Zahájení zachytávání paketů – Linux.....	243
Nastavení podpory monitorovacího módu v operačním systému Windows.....	244
Představujeme AirPcap	244
Určení kanálu pro zachytávání	245
Zachytávání bezdrátového provozu v operačním systému Windows	246
Analýza bezdrátového provozu.....	247
Navigace v okně Packet Details.....	247
Statistiky rámců	247
Hlavička IEEE 802.11.....	249
Potenciál zobrazovacích filtrů.....	251
Provoz pro určitý Basic Service Set.....	252
Provoz pro specifický Extended Service Set	255
Pouze datový provoz	260
Pouze nešifrovaný datový provoz.....	261
Identifikace skrytých SSID.....	262
Zkoumáme výměny EAP	264
Identifikace bezdrátových šifrovacích mechanismů.....	269
Potenciál barevného odlišení zobrazených paketů.....	273
Označování From DS a To DS.....	273
Označování rušeného provozu	275
Označování opakovaných pokusů.....	276

Přidávání informačních sloupců	277
Dešifrování provozu.....	278
Zachytávání bezdrátového provozu v praxi	281
Identifikace kanálu stanice.....	282
Úvod.....	282
Ovlivněné systémy.....	282
Analýza.....	282
Selhání bezdrátového připojení.....	283
Úvod.....	283
Ovlivněné systémy.....	283
Analýza.....	284
Průzkum bezdrátových sítí.....	290
Úvod.....	290
Ovlivněné systémy.....	291
Analýza.....	291
Sdílení účtů pro ověřování pomocí protokolu EAP	293
Úvod.....	293
Ovlivněné systémy.....	293
Analýza.....	294
Útoky typu odepření služby na protokol IEEE 802.11	295
Úvod.....	295
Ovlivněné systémy.....	295
Analýza.....	295
Útoky typu spoofing v sítích IEEE 802.11	298
Úvod.....	298
Ovlivněné systémy.....	298
Analýza.....	298
Analýza poškozeného datového provozu.....	306
Úvod.....	306
Ovlivněné systémy.....	307
Analýza.....	307
Shrnutí	313
Rychlá řešení.....	313
Časté dotazy	315

Kapitola 7

Zachytávání paketů v praxi317

Úvod	318
Skenování	318
Sken typu „TCP Connect“.....	318
Sken typu „SYN“	320

Sken typu „XMAS“	320
Sken typu „NULL“	321
Trojany pro vzdálený přístup.....	322
SubSeven Legend.....	322
Net Bus	324
RST.b.....	325
Rozbor červů	326
Červ SQL Slammer.....	327
Červ Code Red	328
Podrobnosti o červu Code Red	329
Přehled dat zachycených od červa Code Red	329
Podrobný rozbor zachycených dat CodeRed_Stage1	331
Podrobný rozbor zachycených dat CodeRed_Stage2	335
Červ Ramen	336
Aktivní odezva	339
Shrnutí	342
Rychlá řešení.....	343
Časté dotazy	344

Kapitola 8

Vývoj Wiresharku.....345

Úvod	346
Podmínky pro vývoj Wiresharku	346
Dovednosti.....	347
Nástroje / Knihovny	348
Další vývojářské prostředky	352
Wiki Wiresharku.....	353
„Wish List“ Wiresharku	353
E-mailová konference Wiresharku.....	353
Návrh Wiresharku.....	353
svn	354
aclocal-fallback a autom4te.cache	354
Složka ASN1	354
Složka Debian	354
Složka Diameter	354
Složka doc	354
DocBook.....	355
Definice dtids	355
Složka epan.....	356

Složka gtk	356
Složka gtk2.tmp	356
Složka Help	356
Složka IDL	356
Složka Image	356
Složka Packaging	357
Zásuvné moduly	358
Složka Radius	358
Složka Test	358
Složka Tools.....	358
Složka Wiretap	359
Vývoj disektoru.....	359
Krok 1 – zkopírujte šablonu.....	359
Krok 2 – definujte začleněné soubory	360
Krok 3 – vytvořte funkci pro registraci.....	362
Krok 4 – informujte Wireshark	364
Krok 5 – vytvořte disektor	364
Krok 6 – předání dat	370
Spouštění disektoru	371
Proces rozboru.....	372
Pokročilá témata	373
Nad čím se při tvorbě disektoru zamyslet.....	373
Vytváření podstromů.....	374
Bitová pole.....	375
Řetězce Unicode.....	376
Konverzace	377
Opakovaný přenos paketů	378
Předávání dat mezi disektory	378
Ukládání nastavení preferencí.....	379
Fragmentace paketů.....	380
Řetězce hodnot.....	380
Expertní TAP	381
Ladění vašeho disektoru	383
Grafické uživatelské rozhraní Wiresharku (GUI).....	383
Item Factory	384
Používání GTK.....	385
TAP	387
Zásuvné moduly.....	393
Shrnutí	393
Rychlá řešení.....	394
Časté dotazy	396

Kapitola 9

Další programy dodávané s Wiresharkem.....399

Úvod	400
TShark	400
Statistiky TSharku	406
Statistiky hierarchie protokolů.....	407
Statistiky protokolů podle intervalu	407
Statistiky konverzací.....	409
Rozdělení délky paketů.....	410
Strom cílů	411
Sloupce souhrnu paketů	411
Statistiky SIP	412
Čítače protokolu H.225	412
H.225 Service Response Time (Doba odezvy služby)	413
Media Gateway Control Protocol Round Trip Delay.....	413
SMB Round Trip Data.....	413
Zjišťování názvů identifikátorů zabezpečení protokolu SMB.....	414
Statistiky protokolu BOOTP	414
Statistiky protokolu HTTP	415
Statistiky stromu protokolu HTTP.....	415
Statistiky žádostí protokolu HTTP.....	416
Editcap	419
Merg pcap.....	424
Text2pcap	426
Capinfos.....	429
Dumpcap	430
Shrnutí	431
Rychlá řešení.....	432
Časté dotazy	433

Rejstřík.....435

Předmluva

Přiložené CD

Většina nástrojů použitých v této knize patří do kategorie Open Source, a tudíž se neustále vyvíjí. Pokud se rozhodnete nasadit libovolný z těchto nástrojů na své síti, prosím ujistěte se, že jste stáhli nejaktuálnější dostupnou verzi.



Kdekoliv to bylo možné, uvedli jsme informace o webových stránkách, na kterých jsou nástroje dostupné ke stažení. Vždy proto hledejte ikonu CD umístěnou na okraji stránky, která značí přítomnost právě probíraného nástroje nebo souboru na přiloženém CD.

Pro vaše pohodlí a také proto, abychom zajistili konzistenci použitých příkladů, jsme přiložili Wireshark ve verzi 0.99.4; v době vzniku této knihy se jednalo o poslední dostupnou stabilní verzi.

Složka „Windows Installer“ obsahuje soubor wireshark-setup-0.99.4.exe pro instalaci na operačních systémech platformy Win32. Tento soubor Nullsoft Scriptable Install System se vás zeptá na několik málo informací v průběhu instalace Wiresharku a WinPcapu. Po instalaci bude program dostupný v nabídce Start → Programy.

Složka Source Files obsahuje soubor wireshark-0.99.4.tar.gz pro instalaci na jiných operačních systémech než Microsoft Windows.

Na CD také najdete složky obsahující filtry probírané v této knize a složku obsahující zachycená data použitá ve cvičeních v kapitolách 4, 6 a 7.



Poznámka: Toto CD obsahuje zachycené pakety aktivity viru Code Red a obsahuje řetězce, které mohou být vaší antivirovou aplikací detekovány jako hrozba. Abyste mohli pokračovat v použití těchto souborů, budete muset zakázat ochranu v reálném čase. Tyto soubory neobsahují skutečné viry, pouze neškodná data generovaná aktivitou viru.

Wireshark podléhá regulaci exportu ve Spojených státech. V případě pochybností se poraďte s právníkem.

Hlavní autorka

Angela Orebaugh je uznávanou expertkou na bezpečnostní technologie, vizionářkou a vědeckou pracovnící s více než dvanáctiletou praxí v oboru. V současnosti pracuje jako přední bezpečnostní konzultantka a věnuje se výzkumu a vývoji elitních systémů pro zabezpečení informací. Angela se momentálně podílí na několika bezpečnostních iniciativách pro National Institute of Standards and Technology (NSIT). Je přední vědeckou pracovnící pro National Vulnerability Database a autorkou několika publikací o bezpečnostních technologiích NIST. Časově Angelino působení a zkušenosti přesahují jednu dekádu práce s informačními technologiemi se zaměřením na obranu perimet-

rů, design zabezpečených sítí, objevování zranitelností, penetrační testování a systémy pro detekci průniku. Je držitelkou univerzitního titulu Master in Computer Science a momentálně pracuje na získání titulu Ph.D se zaměřením na informační bezpečnost na George Mason University. Angela je autorkou bestselleru *Ethereal Packet Sniffing* a podílela se na knihách *Snort Cookbook* a *Intrusion Prevention and Active Response: Deploying Network and Host IPS*. Angela je výzkumnice, spisovatelka a mluvčí institutu SANS a fakulty The Institute for Applied Network Security a George Mason University. Má bohaté znalosti z branže, univerzitního působení a spolupráce s vládou a také z práce jako konzultantka společností Fortune 500, Ministerstva obrany USA, dot-com startupů a univerzit. Je často zvaným přednášejícím na různých konferencích o bezpečnosti.

Její současné centrum zájmu zahrnuje detekci průniku, prevenci průniku, dolování dat, profilování útočníků, analýzu chování uživatelů a vyšetřování bezpečnostních incidentů.

Odborný korektor a spoluautor

Gilbert Ramirez – poté co byl *Ethereal* představen veřejnosti, stal se Gilbert prvním přispěvatelem a je znám jako autor pravidelných aktualizací tohoto produktu. Přispíval také tvorbou disketorů protokolů a návrhem základní logiky *Ethereal*. Je technickým vedoucím u Cisco Systems, kde pracuje na tvorbě různých systémů a nástrojů. Gilbert by se dal charakterizovat jako rodinný typ, lingvista, rádoby kuchař a student taekwon-do. Také je autorem publikace *Ethereal Packet Sniffing*.

Spoluautoři

Josh Burke (CISSP) je nezávislý konzultant v oboru informační bezpečnosti v Seattlu, stát Washington. Po dobu 7 let pracoval na pozicích souvisejících se sítěmi, systémy a zabezpečením na poli technologií, financí a médií. Promoval na obchodní škole University of Washington. Josh se zaměřuje na hledání optimální rovnováhy mezi technickými a obchodními potřebami společností v mnoha oblastech informační bezpečnosti. Také podporuje všeobecně pozitivní bezpečnostní filozofii společností, které povzbuzují diskusi o zásadních otázkách bezpečnosti a zásadách zabezpečení, místo aby vyučoval pouze různé formy omezení a zákazů.

Josh je expertem na open-source aplikace jako Snort, *Ethereal* a Nessus. Jeho výzkumné zájmy zahrnují zlepšování bezpečnosti a odolnosti systému DNS a NTP. Také se věnuje četbě knih s matematickou tematikou nebo tematikou historie kryptografie, ale stejně se nemůže zbavit pocitu, že po každém takovém čtení ví o dané oblasti ještě méně, než když s četbou začal.

Larry Pesce (CCNA, GCFA Silver, GAWN Silver) je manažerem společnosti Information Services Security at Care New England, středně velké společnosti zaměřené na poskytování zdravotní péče v Nové Anglii. Za posledních 13 let strávených v IT-branži se Larry stal doslova všeumělem; zabýval se opravami PC, síťovým inženýrstvím, návrhem webu, nelineární audio a video produkcí a počítačovou bezpečností. Larry je také za výhodných podmínek zaměstnán jako penetrační tester a etický hacker u společnosti Defensive Intuition na Rhode Islandu. Po promoci na Roger Williams University v oboru počítačových informačních systémů Roger přemýšlí o dalším vzdělávání.

Kromě působení v oboru je Larry také Security Evangelist týdenních podcastů PaulDotCom Security Weekly na adrese www.pauldotcom.com. Larry momentálně dokončuje svou práci s kolegou z PaulDotCom Security Weekly Paulem Asadoorianem o hackování Linksys WRT54G. Další Larryho práce, návody a články najdete na jeho blogu na adrese www.haxorthematrix.com.

Greg Morris (5-CNA, 5-CNE, 3-MCNE, Linux+, LPIC-1) je Senior Resolution Engineer ve společnosti Novell Technical Services v Provo, stát Utah. Greg je původem z Oklahomy a strávil přes 25 let práci v počítačové branži. I když Greg promoval v oboru managementu, jeho vášní je kreativita. A přesně tu Gregovi poskytuje proces vývoje softwaru. Jeho nespočetné zkušenosti zahrnují znalost řešení problémů hardwaru a softwaru na mainframech a PC různých kategorií. Gregovy rané kořeny ve vývoji softwaru spočívají v databázových technologiích, koketování s programováním v C a assembleru, avšak nejvíce pracoval s jazykem zvaným Clipper od Nantucketu. Gregova práce na Etherealu začala v listopadu roku 2000. Od té doby přispěl k tomuto projektu významným množstvím práce, včetně nových disektorů (NCP, NDS, NDPS) a nových funkcí (rozšířené vyhledávání). Greg také upravil mnoho dalších disektorů a momentálně vyvíjí dekodéry pro Novell Modular Authentication Services (NMAS), Novell SecretStore Services (SSS), Novell International Cryptographic Infrastructure (NICI) a další dekodéry specifické pro Novell. Greg aktivně vyvíjel tréninkové programy pro zákazníky i interní zaměstnance pro množství různých produktů Novell. Jeden z jeho nejunikátnějších programů byl vyvinut pro výuku interních uživatelů, aby ovládli schopnosti nutné pro analýzu zachycených paketů. Greg začal pracovat se sledováním paketů před mnoha lety pomocí novellový LANalyzeru. Odtud Greg migroval k produktu Network Associates Sniffer. Avšak od té doby, co začal pracovat s Etherealem a přidal kompletní podporu paketů Novell NCP/NDS, by Greg už nepoužíval žádný jiný produkt. Momentálně pracuje s Windows 2000 a Microsoft Visual C++, ale plánuje přechod na SuSE Linux a kompilátor GNU pro další vývoj Wiresharku.

Joshua Wright pracuje jako senior bezpečnostní výzkumník pro společnost Aruba Network, světovou jedničku v oblasti řešení pro zabezpečení mobilních bezdrátových komunikací. Joshua je autorem několika dokumentů o bezdrátové bezpečnosti a analýze průniků. Také napsal několik open-source nástrojů navržených pro zvýraznění slabín v bezdrátových sítích. Joshua je také senior instruktorem v SANS Institute a pravidelným přednášejícím na konferencích o informační bezpečnosti. Když se právě nezabývá prolamováním bezdrátových sítí, rád se věnuje práci na svém domě, kde většinou rozbíjí věci zcela jiného charakteru.

Konvence použité v knize

Text doplňuje řada speciálních odstavců a částí:



Tip: Zajímavý tip pro práci a rozšiřující informace.



Důležité: Informace, které byste si měli zapamatovat.



Poznámka: Další informace k tématu.

Další informace

Tyto části textu poskytují podrobnější informace.



Takto je označen text, který se vztahuje k obsahu CD.

Poznámka redakce českého vydání

I nakladatelství Computer Press, které pro vás tuto knihu přeložilo, stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

Computer Press
redakce počítačové literatury
Holandská 8
639 00 Brno
nebo

knihy@cpress.cz.

Další informace a případné opravy českého vydání knihy najdete na internetové adrese <http://knihy.cpress.cz/1599>. Prostřednictvím uvedené adresy můžete též naší redakci zaslat komentář nebo dotaz týkající se knihy. Na vaše reakce se srdečně těšíme.