

Pochvalná vyjádření k prvnímu vydání Hacking – umění exploitace

„Nejkompletnější výuka hackerských technik. Konečně kniha, která jen nepředvádí, jak využívat exploity, ale také ukazuje, jak je vyvíjet.“

– PHRACK

„Ze všech knih, co jsem doposud četl, tuto považuji za vynikající hackerskou příručku.“

– SECURITY FORUMS

„Tuto knihu doporučuji už jen kvůli její programovací sekci.“

– UNIX REVIEW

„Vřele tuto knihu doporučuji. Napsal ji člověk, který ví, co čem mluví, navíc s použitelným kódem, nástroji a příklady.“

– IEEE CIPHER

„Ericksonova kniha, hutný a seriózní průvodce pro začínající hackery, je naplněna až po okraj nejenom kódem a hackerskými technikami ze skutečného světa, ale také vysvětleními, jak fungují.“

– COMPUTER POWER USER (CPU) MAGAZINE

„Tohle je vynikající kniha. Ti, kdo se právě chystají přejít na další úroveň, měli by si ji opatřit a pečlivě pročíst.“

– ABOUT.COM INTERNET/NETWORK SECURITY

Hacking

umění exploitace

Druhé, upravené a doplněné vydání

Jon Erickson



HACKING: THE ART OF EXPLOITATION, 2ND EDITION

Jon Erickson

Copyright © 2008 by Jon Erickson. Title of English-language original: Hacking: The Art of Exploitation, 2nd Edition, ISBN 978-1-59327-144-2 published by No Starch Press. Czech-language edition copyright © 2009 by ZONER software s.r.o. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from No Starch Press.

Copyright © 2008 Jon Erickson. Název originálního anglického vydání: Hacking: The Art of Exploitation, 2nd Edition, ISBN 978-1-59327-144-2, vydal No Starch Press. České vydání copyright © 2009 ZONER software s.r.o. Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována nebo předávána žádnou formou nebo způsobem, elektronicky ani mechanicky, včetně fotokopíí, natáčení ani žádnými jinými systémy pro ukládání bez výslovného svolení No Starch Press.

Hacking – umění exploitace

Autor: Jon Erickson

Copyright © ZONER software, s.r.o. Druhé, upravené a doplněné vydání v roce 2009. Všechna práva vyhrazena.

Zoner Press

Katalogové číslo: **ZR803**

ZONER software, s.r.o.

Nové sady 18, 602 00 Brno

Překlad: RNDr. Jan Pokorný

Odpovědný redaktor: Miroslav Kučera

Odborná korektura: Miroslav Kučera

Šéfredaktor: Ing. Pavel Kristián

DTP: Miroslav Kučera

Obraz bootovatelného LiveCD ke stažení:

<http://zonerpress.cz/download/hacking.zip> (750 MB)

Informace, které jsou v této knize zveřejněny, mohou být chráněny jako patent. Jména produktů byla uvedena bez záruky jejich volného použití. Při tvorbě textů a vyobrazení bylo sice postupováno s maximální péčí, ale přesto nelze zcela vyloučit možnost výskytu chyb. Vydavatelé a autoři nepřebírají právní odpovědnost ani žádnou jinou záruku za použití chybných údajů a z toho vyplývajících důsledků. Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována ani distribuována žádným způsobem ani prostředkem, ani reprodukována v databázi či na jiném záznamovém prostředku či v jiném systému bez výslovného svolení vydavatele, s výjimkou zveřejnění krátkých částí textu pro potřeby recenzí.

Veškeré dotazy týkající se distribuce směřujte na:

Zoner Press

ZONER software, s.r.o.

Nové sady 18, 602 00 Brno

tel.: **532 190 883**, fax: **543 257 245**

e-mail: **knihy@zoner.cz**

<http://www.zonerpress.cz>

ISBN 978-80-7413-022-9

Obsah

Předmluva	11
Poděkování	11

Kapitola 0x100	Úvod	13
-----------------------	-------------	-----------

0x110	Obráz LiveCD ke stažení	16
-------	-------------------------	----

Kapitola 0x200	Programování	17
-----------------------	---------------------	-----------

0x210	Co je programování?	18
0x220	Pseudokód	19
0x230	Řídící struktury	19
0x231	If-Then-Else	19
0x232	Cykly While/Until	21
0x233	Cykly For	22
0x240	Další základní programovací pojmy	23
0x241	Proměnné	23
0x242	Aritmetické operátory	24
0x243	Porovnávací operátory	26
0x244	Funkce	28
0x250	Nejvyšší čas zkusit něco prakticky	31
0x251	Bliž k celkovému obrazu	32
0x252	Procesory architektury x86	36
0x253	Assembler	37
0x260	Zpět k základům	51
0x261	Řetězce	51
0x262	Signed, unsigned, long a short	55
0x263	Ukazatele	57
0x264	Formátovací řetězce	62
0x265	Přetypování	65
0x266	Argumenty příkazového řádku	73
0x267	Obor proměnných	77
0x270	Segmentace paměti	85
0x271	Paměťové segmenty v C	93
0x272	Jak se pracuje s haldou	95
0x273	Funkce malloc() s kontrolou, zdali se alokace podařila	98

0x280	Stavění na solidních základech	100
0x281	Přístup k souboru	100
0x282	Souborová oprávnění	106
0x283	Uživatelská ID	108
0x284	Struktury	117
0x285	Ukazatele funkce	121
0x286	Pseudonáhodná čísla	122
0x287	Sada hazardních her	124

Kapitola 0x300	Exploitate	141
-----------------------	-------------------	------------

0x310	Všeobecné exploitační techniky	144
0x320	Přetečení paměti	144
	0x321 Zranitelnosti způsobené přetečením bufferu založeného na zásobníku	148
0x330	Experimenty s BASH	161
	0x331 Používání proměnných prostředí	172
0x340	Přetečení v jiných segmentech	181
	0x341 Základní přetečení založené na haldě	181
	0x342 Přetečení ukazatelů na funkce	187
0x350	Formátovací řetězce	201
	0x351 Formátovací parametry	202
	0x352 Zranitelnost spojená s formátovacím řetězcem	204
	0x353 Čtení z libovolné adresy paměti	207
	0x354 Zápis na libovolnou adresu paměti	208
	0x355 Přímý přístup k parametru	216
	0x356 Zápisy dvoubajtových slov	218
	0x357 Odbočka s .dtors	220
	0x358 Další zranitelnost programu notesearch	226
	0x359 Přepisování tabulky globálních offsetů	228

Kapitola 0x400	Sítě	233
-----------------------	-------------	------------

0x410	Model OSI	233
0x420	Sockety 235	
	0x421 Socketové funkce	236
	0x422 Socketové adresy	238
	0x423 Síťové pořadí bajtů	240
	0x424 Konverze internetové adresy	240

0x425	Ukázka jednoduchého serveru	241
0x426	Ukázka webového klienta	245
0x427	Maličký webový server	251
0x430	Loupání slupek nižších vrstev	256
0x431	Spojová vrstva	257
0x432	Síťová vrstva	258
0x433	Transportní vrstva	261
0x440	Odposlouchávání provozu na síti (network sniffing)	264
0x441	Odposlouchávání nezpracovaných socketů	266
0x442	Odposlouchávací knihovna libpcap	268
0x443	Dekódování vrstev	270
0x444	Aktivní odposlouchávání	281
0x450	Odmítnutí služby	295
0x451	Zahlcení podvrženými SYN pakety	296
0x452	Ping smrti	301
0x453	Slza	301
0x454	Zahlcení přes ping	301
0x455	Zesilující se útoky	302
0x456	Útok DDoS	302
0x460	Únos TCP/IP	303
0x461	Únos RST	304
0x462	Pokračování únosu	309
0x470	Skenování portů	310
0x471	Tajné skenování SYN	310
0x472	Skenování FIN, X-mas a Null	310
0x473	Podvržené návnady	311
0x474	Nečinné skenování	311
0x475	Aktivnější obrana	313
0x480	K lidu blíž – někoho hackneme	320
0x481	Analýza s GDB	321
0x482	Téměř vždy počítejte s ručními granáty	323
0x483	Shellkód, který se navazuje na port	326

Kapitola 0x500 Shellkód

331

0x510	Assembler versus C	331
0x511	Linuxová systémová volání v assembleru	334

0x520	Cesta k shellkódu	337
0x521	Assemblerové instrukce používající zásobník	337
0x522	Vyšetřování s GDB	340
0x523	Odstranění bajtů null	341
0x530	Shellkód, který zplodí shell	347
0x531	Otázka oprávnění	351
0x532	Ještě menší shellkód	354
0x540	Shellkód, který se navazuje na port	356
0x541	Duplikace standardních souborových deskriptorů	361
0x542	Řídící struktury pro větvení	363
0x550	Shellkód připojující se zpět	368

Kapitola 0x600 Protiopatření 375

0x610	Detekující protiopatření	376
0x620	Systémoví démoni	376
0x621	Signály letem-světlem	378
0x622	Démon tinyweb	381
0x630	Nástroje našeho řemesla	386
0x631	Nástroj pro exploitaci tinywebd	386
0x640	Protokolovací soubory	392
0x641	Jak splynout s davem	392
0x650	Přehlížení očividného	394
0x651	Krok za krokem	395
0x652	A dejme zase všechno dohromady	400
0x653	Dceřiní nádeníci	406
0x660	Pokročilá kamufláž	408
0x661	Podvržení přihlášené IP adresy	409
0x662	Nezaprotokolovaná exploitate	414
0x670	Kompletní infrastruktura	417
0x671	Opětovné použití socketu	417
0x680	Propašování nálože	422
0x681	Zašifrování řetězců	422
0x682	Jak skrýt sled	426
0x690	Restriktivní opatření na buffer	427
0x691	Polymorfní tisknutelný ASCII shellkód	430
0x6a0	Vylepšená protiopatření	442

0x6b0	Nespustitelný zásobník	442
0x6b1	ret2libc	442
0x6b2	Návrat do system()	443
0x6c0	Náhodné rozvržení paměti zásobníku	445
0x6c1	Výzkumy s BASH a GDB	447
0x6c2	Odsakování od linux-gate	451
0x6c3	Umění aplikovat získané znalosti v praxi	455
0x6c4	První pokus	456
0x6c5	Pohrajeme si s šancemi	458

Kapitola 0x700	Kryptologie	461
-----------------------	--------------------	------------

0x710	Teorie informace	462
0x711	Nepodmíněná bezpečnost	462
0x712	Jednorázové zašifrování	462
0x713	Distribuce kvantového klíče	463
0x714	Výpočetní bezpečnost	464
0x720	Doba běhu algoritmu	464
0x721	Asymptotická notace	465
0x730	Symetrické šifrování	466
0x731	Lov Groverův kvantový vyhledávací algoritmus	467
0x740	Asymetrické šifrování	468
0x741	RSA	468
0x742	Kvantový faktorizační algoritmus Petera Shora	472
0x750	Hybridní šifry	473
0x751	Útoky typu "Muž uprostřed"	473
0x752	Rozdíly v otiscích prstů hostitele protokolu SSH	478
0x753	Fuzzy otisky prstů	482
0x760	Prolamování hesel	487
0x761	Slovníkové útoky	489
0x762	Vyčerpávající útok hrubou silou	492
0x763	Vyhledávací tabulka hašů	493
0x764	Pravděpodobnostní matice hesla	494
0x770	Bezdrátové šifrování 802.11b	506
0x771	Šifrovací metoda WEP (Wired Equivalent Privacy)	506
0x772	Proudová šifra RC4	508
0x780	Útoky na WEP	508

0x781	Offline útoky hrubou silou	509
0x782	Opětovné použití stejného proudového klíče	509
0x783	Dešifrovací slovníkové tabulky založené na inicializačním vektoru	510
0x784	Přesměrování IP adresy	511
0x785	Útoky typu Fluhrer, Mantin a Shamir (FMS)	512

Kapitola 0x800	Shrnutí	523
-----------------------	----------------	------------

0x810	Seznam zdrojů	524
0x820	Užitečné nástroje	525

Rejstřík	527
-----------------	------------

Předmluva

Cílem této knihy je podělit se s vámi všemi o umění hackingu. Často není snadné pochopit techniky hackingu, protože k tomu potřebujete poměrně mnoho důkladně zvládnutých vědomostí. Mnohé texty o hackingu se vám mohou zdát jako nesrozumitelné a matoucí, protože bez jistých předběžných znalostí se nelze obejít a vy v tomto druhu vzdělání jednoduše máte několik mezer.

Druhé vydání knihy Hacking – umění exploitace by vám mělo zpřístupnit svět hackingu, protože o něm dostanete kompletní informace. Od programování přes strojový kód až k exploitaci. K tomuto vydání si navíc můžete stáhnout obraz bootovacího CD (z <http://zonerpress.cz/download/hacking.zip>), který v sobě obsahuje upravenou linuxovou distribuci Ubuntu. Jakmile tento obraz stáhnete, rozbalíte a vypálíte na CD/DVD médium, můžete ho použít na jakémkoliv počítači s procesorem x86 bez toho, aby došlo k poškození stávajícího operačního systému vašeho počítače. Obsahuje veškerý zdrojový kód z knihy a poskytuje jak vývojové, tak i exploitační prostředí, v němž můžete při četbě souběžně zkoušet všechny příklady uvedené v knize a provádět své vlastní experimenty.

Poděkování

Mé vřelé díky si zaslouží Bill Pollock a všichni ostatní ve vydavatelství No Starch Press, že konali tak, aby tato kniha mohla spatřit světlo světa, a že jsem mohl kreativně ovlivňovat všechny fáze procesu jejího vzniku. Dále bych rád poděkoval svým přátelům, Sethu Bensonovi a Aaronu Adamsovi, za korektury a úpravy, Jacku Mathesonnovi, že mi vypomohl s assemblerem, Dr. Seidelovi, že udržel můj zájem o počítačovou vědu, rodičům, že mi koupili první Commodore VIC-20, a komunitě hackerů, jejichž inovace a kreativita vytvořila techniky vysvětlované v této knize.

