

Obsah

Předmluva	19
Úvod	21
Část první: Úvod do etického zveřejňování informací	23
1. Etický hacking	25
Odkazy	29
1.1 Jak tohle všechno souvisí s knihou o etickém hackingu?	30
1.1.1 Hledání slabých míst	30
1.1.2 Penetrační testování	31
1.1.3 Odkazy	32
1.2 Problémové knihy a přednášky o hackingu	32
1.2.1 Dvojitá povaha nástrojů	33
Rozdíly v použití nástrojů pro dobré a špatné účely	33
1.2.2 Odkazy	34
1.2.3 Jak poznat problémy	34
1.2.4 Simulované útoky	35
1.3 Co baví útočníky nejvíc	36
1.3.1 Bezpečnost a složitost se nemají rádi	36
1.3.2 Odkazy	37
1.4 Shmutí	37
1.4.1 Otázky	37
1.4.2 Odpovědi	39
2. Etický hacking a právní systém	41
Odkazy	42
2.1 Konkrétní zákony	42
2.1.1 Zákon o přístupových zařízeních	42
2.1.2 Odkazy	45
2.1.3 Zákon o počítačových podvodech (CFAA)	45
2.1.4 Víry a červi	47

2.1.5	Útoky červa Blaster.....	48
2.1.6	Nespokojení zaměstnanci.....	48
2.1.7	Odkazy.....	49
2.1.8	Státní zákony.....	49
2.1.9	Odkazy.....	50
2.1.10	Zákon o soukromé elektronické komunikaci (ECPA).....	51
2.1.11	Zajímavé způsoby použití ECPA.....	51
2.1.12	Důsledky rozšíření internetu.....	52
2.1.13	Odkazy.....	53
2.1.14	Digital Millenium Copyright Act (DMCA).....	53
2.1.15	Odkazy.....	54
2.1.16	Zákon o vylepšení počítačové bezpečnosti z roku 2002.....	54
2.2	Shmutí.....	54
2.2.1	Otázky.....	55
2.2.2	Odpovědi.....	57
3.	Etické ohlašování chyb.....	59
3.1	Různé týmy, různé pohledy.....	60
3.1.1	Trocha historie.....	61
3.2	Jak na to jde CERT.....	62
3.3	Politika typu full disclosure.....	63
3.4	Organizace pro internetovou bezpečnost (OIS).....	64
3.4.1	Hledání.....	65
3.4.2	Oznámení.....	66
3.4.3	Ověření.....	67
	Výšetřování.....	67
	Chyby ve sdíleném kódu.....	67
	Závěr.....	68
	Potvrzení chyby.....	68
	Popření chyby.....	68
	Neschopnost chybu potvrdit nebo vyvrátit.....	69
3.4.4	Řešení.....	69
	Časový plán.....	69
3.4.5	Zveřejnění.....	70
3.5	Přetrvávající konflikty.....	71
3.6	Případové studie.....	71
3.6.1	Výhody a nevýhody různých metod.....	71
	Pohled bezpečnostní komunity.....	71

Pohled výrobce softwaru.....	72
Správa znalostí.....	72
Publicita.....	73
Pouto, které váže.....	73
Týmový přístup.....	73
Komunikace.....	74
Rozdíly ve znalostech.....	74
Neúspěšné záplaty.....	74
Chyby po vydání záplat.....	74
3.6.2 Lepší řešení.....	74
3.7 Jak dál?.....	75
3.7.1 Defense.....	76
3.7.2 Odkazy.....	76
3.8 Shmutí.....	77
3.8.1 Otázky.....	77
3.8.2 Odpovědi.....	78
Část druhá: Penetrační testování a nástroje.....	81
4. Penetrační testování.....	83
4.1 Typy testů.....	84
4.1.1 Odkaz.....	85
4.2 Sestavení týmu.....	85
4.2.1 Technický vedoucí.....	85
4.2.2 Vedoucí týmu.....	85
4.2.3 Řadoví členové týmu.....	86
4.3 Vytvoření laboratoře.....	86
4.4 Smlouvy, aneb jak se nedostat za mříže.....	86
4.5 Proces testování.....	87
4.5.1 Plánování testů.....	87
4.5.2 Setkání se zákazníkem a odstartování testů.....	88
4.6 Penetrační testování.....	88
4.6.1 Průzkum.....	89
4.6.2 Hledání chyb.....	89
4.6.3 Zneužití nalezených chyb.....	90
4.6.4 Výhody a nevýhody penetračního testování.....	90
4.6.5 Odkazy.....	90
4.7 Red Teaming.....	90

4.7.1	Získání přístupu do sítě.....	91
4.7.2	Získání vyšších práv.....	92
4.7.3	Zkouška reakcí na bezpečnostní incident.....	92
4.7.4	Výhody a nevýhody red teamingu.....	92
4.8	Systémové testy.....	93
4.8.1	Ohledání povrchu.....	93
	Instalace.....	93
	Běžný provoz.....	94
	Odinstalování.....	95
4.8.2	Cílené hledání chyb.....	95
	Útok přes soubory.....	95
	Útok přes registr systému.....	96
	Útok přes pojmenované roury.....	96
	Útok přes slabá ACL.....	96
	Síťové útoky.....	97
4.8.3	Výhody a nevýhody systémových testů.....	97
4.8.4	Odkazy.....	97
4.9	Zpracování výsledků.....	98
4.10	Shrnutí.....	98
4.10.1	Otázky.....	99
4.10.2	Odpovědi.....	100
5.	Za hacking bez záhad – nástroje dnešního hackera.....	103
5.1	Skenování za „starých dobrých časů“.....	104
5.1.1	Paketto Keiretsu (scanrand, paratrace).....	104
	scanrand.....	105
	paratrace.....	111
5.1.2	Odkazy.....	116
5.2	Identifikace operačního systému a síťových služeb.....	116
5.2.1	xprobe2.....	117
5.2.2	Odkazy.....	121
5.2.3	pOf.....	122
5.2.4	Odkazy.....	125
5.2.5	amap.....	125
5.2.6	Odkazy.....	129
5.2.7	Winfingerprint.....	129
5.3	Odposlech sítě.....	131
5.3.1	libpcap a WinPcap.....	131

5.3.2	Odkazy.....	132
5.3.3	Aktivní a pasivní odposlech.....	132
	Triky sARP.....	134
	K čemu to všechno je útočníkovi.....	135
	Jak otrávit dav.....	137
5.3.4	Odkazy.....	137
	arpspoof.....	138
	ettercap.....	138
5.3.5	Odkazy.....	140
5.3.6	Obrana proti aktivnímu odposlechu.....	140
5.3.7	Odposlech autentizačních údajů.....	141
	dsniff.....	141
5.3.8	Odkazy.....	142
5.4	Autentizace systému LAN Manager.....	142
5.4.1	Co s výzvou a hesí (složitější varianta).....	145
5.4.2	Co s výzvou a hesí (jednodušší varianta).....	146
5.4.3	Odkazy.....	148
5.4.4	Odposlech a lámání hesel systému Kerberos.....	148
5.5	Shmutí.....	150
5.5.1	Otázky.....	152
5.5.2	Odpovědi.....	153
6.	Automatické penetrační testování.....	155
6.1	Základy Pythonu.....	156
6.1.1	Jak Python získat.....	156
6.1.2	Hello, world.....	156
6.1.3	Objekty v Pythonu.....	157
	Řetězce.....	157
	Čísla.....	159
	Seznamy.....	160
	Slovníky.....	161
	Soubory.....	162
	Sokety.....	163
6.1.4	Odkazy.....	164
6.2	Nástroje pro automatické penetrační testování.....	164
6.2.1	Core IMPACT.....	165
6.2.2	Odkaz.....	167
6.2.3	Immunity CANVAS.....	167
6.2.4	Odkazy.....	171

6.2.5 Metasploit.....	171
Instalace.....	171
Použití.....	172
Co dál?.....	179
6.2.6 Odkazy.....	179
6.3 Shmutí.....	179
6.3.1 Otázky.....	180
6.3.2 Odpovědi.....	181
Část třetí: Exploity.....	183
7. Základní programátorské dovednosti.....	185
7.1 Programování.....	186
7.1.1 Programování jako řešení problémů.....	186
7.1.2 Pseudokód.....	187
7.1.3 Programátor versus hacker.....	188
7.1.4 Odkazy.....	189
7.2 Programovací jazyk C.....	189
7.2.1 Základní konstrukce.....	189
Funkce main.....	189
Funkce.....	190
Proměnné.....	190
Funkce printf.....	191
Funkce scanf.....	191
Funkce střepy a střepey.....	192
Cykly for a while.....	192
Podmíněné vyhodnocení.....	193
Komentáře.....	193
7.2.2 Ukázkový program.....	193
7.2.3 Příklad sgcc.....	194
7.2.4 Odkazy.....	195
7.3 Počítačová paměť.....	195
7.3.1 Paměť s náhodným přístupem.....	195
7.3.2 Endianita.....	195
7.3.3 Segmentace paměti.....	196
7.3.4 Programy v paměti.....	196
Kód.....	196
Inicializované proměnné.....	196
Neinitializované proměnné.....	196

	Halda.....	196
	Zásobník.....	197
	Parametry a proměnné prostředí.....	197
7.3.5	Buffery.....	197
7.3.6	Řetězce v paměti.....	197
7.3.7	Ukazatele.....	197
7.3.8	Poskládání kousků paměti.....	198
7.3.9	Odkazy.....	198
7.4	Procesory Intel.....	199
7.4.1	Registry.....	199
7.4.2	Aritmeticko-logická jednotka (ALU).....	200
7.4.3	Čítač instrukcí.....	200
7.4.4	Řídicí jednotka.....	200
7.4.5	Sběrnice.....	200
7.4.6	Odkaz.....	201
7.5	Základy assembleru.....	201
7.5.1	Strojový kód, assembler a C.....	201
7.5.2	AT&T versus NASM.....	201
	mov.....	202
	add a sub.....	202
	push a pop.....	202
	xor.....	203
	jne,je,jz, jnzajmp.....	203
	callaret.....	203
	inc a dec.....	203
	lea.....	203
	int.....	203
7.5.3	Způsoby adresování.....	204
7.5.4	Struktura souborů v assembleru.....	204
7.5.5	Překlad.....	205
7.5.6	Odkazy.....	205
7.6	Ladění sgdb.....	205
7.6.1	Základy gdb.....	206
7.6.2	Disasemblování v gdb.....	208
7.6.3	Odkazy.....	209
7.7	Shmutí.....	209
7.7.1	Otázky.....	210
7.7.2	Odpovědi.....	211

8. Základní exploits pro Linux	213
8.1 Operace se zásobníkem	214
8.1.1 Struktura zásobníku.....	214
8.1.2 Implementace zásobníku.....	214
8.1.3 Volání funkcí.....	215
Prolog.....	215
Epilog.....	215
8.1.4 Odkazy.....	216
8.2 Přetečení bufferu	216
8.2.1 Ukázkové přetečení bufferu.....	216
8.2.2 Přetečení programu meetc.....	217
8.2.3 Důsledky přetečení bufferu.....	220
8.2.4 Odkazy.....	221
8.3 Místní přetečení bufferu	221
8.3.1 Složení exploitu.....	222
NOPsaně.....	222
Shellkód.....	222
Návratová adresa.....	223
Exploitový sendvič.....	223
8.3.2 Exploitování zásobníku z příkazové řádky.....	223
8.3.3 Obecný exploit pro přeplnění zásobníku.....	224
8.3.4 Exploitování malých bufferů.....	227
8.3.5 Odkazy.....	229
8.4 Vzdálené přetečení bufferu	229
8.4.1 Model klient/server.....	229
Děravý server.....	230
8.4.2 Zjištění hodnoty registru ESP.....	231
8.4.3 Perl a hledání ESP hrubou silou.....	232
8.4.4 Odkazy.....	234
8.5 Shmutí	234
8.5.1 Otázky.....	235
8.5.2 Odpovědi.....	236
9. Složitější exploits pro Linux	237
9.1 Exploitování formátovacích funkcí	238
9.1.1 Problém.....	238
Formátovací řetězce.....	238
Takto ano.....	239

Takto ne.....	239
Formátovací funkce a zásobník.....	240
Důsledky.....	241
Ukázkový děravý program.....	241
9.1.2 Čtení z libovolné adresy.....	242
Mapování zásobníku pomocí %x.....	242
Čtení libovolných řetězců pomocí %s.....	242
Čtení z libovolné adresy.....	242
Přímý přístup k parametrům.....	243
9.1.3 Zápis na libovolnou adresu.....	243
Magická formule.....	243
Cvičení s kanárkem.....	244
9.1.4 Od destruktorů k rootu.....	245
Souborový formát elf32.....	245
Destruktoři.....	246
Jak to všechno dát dohromady.....	247
9.1.5 Odkazy.....	248
9.2 Přetečení haldy.....	248
9.2.1 Princip přetečení haldy.....	248
Příklad přetečení haldy.....	248
Důsledky.....	249
9.2.2 Přídělování paměti.....	250
9.2.3 dmalloc.....	250
Cíle.....	250
Rozdělení paměti.....	251
Interní data.....	251
Adresáře.....	252
Funkce malloc.....	252
Funkce calloc.....	253
Funkce realloc.....	253
Funkce free.....	253
9.2.4 Jak přetečení haldy zneužít.....	254
unlink exploit.....	254
Ukázkový exploit.....	255
9.2.5 Další exploity.....	257
frontlink exploit.....	257
Destruktoři.....	258
9.2.6 Odkazy.....	258

9.3	Ochrana paměti	258
9.3.1	Libsafe	258
9.3.2	CRSecurity	258
	Openwall	258
	Náhodný mmap	259
	PaX	259
9.3.3	Odkazy	259
9.4	Shmutí	259
9.4.1	Otázky	260
9.4.2	Odpovědi	262
10.	Psaní linuxového shellkódu	263
10.1	Základy linuxového shellkódu	264
10.1.1	Systémová volání	264
	Systémová volání v C	265
	Systémová volání v assembleru	266
10.1.2	Systémové volání exit	266
	Volání z jazyka C	266
	Přechod k assembleru	267
	Příklad, sestavení a testování	268
	Sledování pomocí strace	268
10.1.3	Systémové volání setreuid	268
	Parametry volání setreuid	268
	Volání z assembleru	269
	Příklad, sestavení a testování	269
	Ověření pomocí strace	269
10.1.4	Spuštění shellu pomocí execve	269
	Systémové volání execve	270
	Volání z assembleru	270
	Příklad, sestavení a testování	271
	Jak získat kódy instrukcí	271
	Testování shellkódu	272
10.1.5	Odkazy	273
10.2	Shellkód pro síťový server	273
10.2.1	Vytvoření socketu v C	273
	IP síť používají síťové pořadí bajtů	273
	Struktura sockaddr	274
	Sokety	274
	port_bind.c	275
10.2.2	Vytvoření socketu v assembleru	276

Systemové volání socketcall.....	276
port_bind_asmasm.....	276
10.2.3 Testování shellkódu.....	278
Jak získat kódy instrukcí.....	278
port_bind_scc.....	280
10.2.4 Odkazy.....	281
10.3 Shellkód pro zpětné připojení.....	281
10.3.1 Zpětné připojení v C.....	281
10.3.2 Zpětné připojení v assembleru.....	282
10.3.3 Odkazy.....	284
10.4 Shmutí.....	284
10.4.1 Otázky.....	286
10.4.2 Odpovědi.....	287
11. Základní exploity pro Windows.....	289
11.1 Příklad a ladění programů pro Windows.....	289
11.1.1 Překladače pro Windows.....	290
Parametry překladače.....	291
11.1.2 Ladění ve Windows.....	291
CDB, NTSD nebo WinDbg?.....	292
Příkazy debuggeru.....	293
Symboly a symbol server.....	294
Spuštění debuggeru.....	294
Další funkce debuggeru.....	297
Disasemblování v cdb.....	299
11.1.3 Vytvoření základního exploitu pro Windows.....	300
Nabourání programu meetexe a přepis EIP.....	300
Testování shellkódu.....	302
Zjištění návratové adresy.....	303
Sestavení exploitu.....	304
11.2 Shmutí.....	307
11.2.1 Otázky.....	308
11.2.2 Odpovědi.....	309
Část čtvrtá: Analýza slabých míst.....	311
12. Pasivní analýza.....	313
12.1 Reverse engineering.....	314

12.1.1 K čemu reverse engineering?	314
12.1.2 Odkazy	315
12.2 Automatická analýza zdrojového kódu	316
12.2.1 Pohled bílého hackera	317
12.2.2 Pohled černého hackera	318
12.2.3 Pohled šedého hackera	318
12.2.4 Odkazy	319
12.3 Ruční analýza zdrojového kódu	319
12.3.1 Zdroje uživatelských dat	319
12.3.2 Nalezení chyby v programu find.c	320
12.4 Automatická analýza binárního kódu	323
12.4.1 BugScam	324
12.4.2 BugScan	324
12.4.3 Odkazy	326
12.5 Ruční analýza binárního kódu	326
12.5.1 Zpětný překlad a Java	326
12.5.2 Zpětný překlad v jiných jazycích	328
Disassembly	328
IDA Pro	329
Práce s IDA Pro	329
Navigace v disassembleru	331
Jak se vyznat v kódu	331
Hledání chyb	333
find.c na závěr	333
12.5.3 Odkazy	335
12.6 Shmutí	336
12.6.1 Otázky	336
12.6.2 Odpovědi	337
13. Pokročilý reverse engineering	339
13.1 Proč trápit software	340
13.2 Vývoj softwaru	341
13.3 Nástroje pro analýzu softwaru	341
13.3.1 Debugger	342
13.3.2 Analýza pokrytí kódu	344
13.3.3 Profily	344
13.3.4 Analýza toku	344
13.3.5 Sledování paměti	345

valgrind.....	346
IBM Rational Purify / PurifyPlus.....	349
13.3.6 Odkazy.....	349
13.4 Fuzz testy.....	349
13.5 Fuzzingové nástroje.....	350
13.5.1 Jednoduchý URLfuzzer.....	350
13.5.2 Fuzzing neznámých protokolů.....	353
13.5.3 SPIKE.....	353
Funkce pro vytvoření bodce.....	354
Funkce pro práci se statickým obsahem.....	354
Funkce pro práci s boky.....	355
Funkce pro fuzzing.....	355
Skriptovací funkce.....	356
Jednoduchý příklad.....	356
13.5.4 SPIKE Proxy.....	357
13.5.5 Sharefuzz.....	357
13.5.6 Odkazy.....	357
13.6 Shmutí.....	358
13.6.1 Otázky.....	358
13.6.2 Odpovědi.....	359
14. Od chyby k exploitu.....	361
14.1 Zneužitelnost chyb.....	362
14.1.1 Debugger.....	362
14.1.2 Úvodní analýza.....	363
Analýza ukazatele instrukcí.....	363
Analýza obecných registrů.....	364
Zvýšení spolehlivosti exploitu.....	364
14.1.3 Odkaz.....	366
14.2 Analýza problému.....	366
14.2.1 Vstupní a výstupní podmínky.....	366
14.2.2 Opakovatelnost exploitu.....	367
14.2.3 Předvídatelné chování zásobníku.....	367
Inicializace procesu.....	368
Co s vyčpaným zásobníkem.....	370
14.2.4 Využití jména programu.....	370
14.2.5 Hrátky slibů.....	373
Obrana proti návratu do libc.....	374
14 9 fi CHka7v.....	37-5

14.3 Dokumentace chyb	375
14.3.1 Pozadí problému.....	375
14.3.2 Okolnosti.....	375
14.3.3 Výsledky výzkumu.....	375
14.4 Shmutí.....	376
14.4.1 Otázky.....	376
14.4.2 Odpovědi.....	378
15. Přechodná obrana	381
15.1 Možnosti přechodné obrany.....	382
15.1.1 Klepání na porty.....	382
15.1.2 Odkazy.....	382
15.1.3 Přechod na jiný software.....	383
Přechod na jiný operační systém.....	383
Přechod na jinou aplikaci.....	383
15.1.4 Odkazy.....	383
15.2 Záplatování	384
15.2.1 Záplatování zdrojového kódu.....	384
15.2.2 Kdy záplatovat.....	384
15.2.3 Co záplatovat.....	384
15.2.4 Psaní a použití záplat.....	385
díř.....	385
patch.....	386
15.2.5 Binární záplatování.....	386
Proč záplatovat?.....	386
Formáty spustitelných souborů.....	386
Psaní a použití záplat.....	387
Omezení.....	388
15.2.6 Odkazy.....	389
15.3 Shmutí.....	389
15.3.1 Otázky.....	389
15.3.2 Odpovědi.....	391
Rejstřík.....	393