

Obsah

Předmluva	11
Poděkování	11
Kapitola 0x100 Úvod	13
0x110 Obraz 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 Blíž 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 Záписы двoubajtových 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	Odoslouchávání provozu na síti (network sniffing)	264
0x441	Odoslouchávání nezpracovaných socketů	266
0x442	Odoslouchávací knihovna libpcap	268
0x443	Dekódování vrstev	270
0x444	Aktivní odposlouchávání	281
0x450	Odmítnutí služby	295
0x451	Zahlčení podvrženými SYN pakety	296
0x452	Ping smrti	301
0x453	Slza	301
0x454	Zahlčení 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 návody	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 nazývá 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	Systémové 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	Nezaprotokeovaná 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	Polymorfni 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	Odskakování 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