

OBSAH

0x100

ÚVOD 11

0x200

PROGRAMOVÁNÍ 17

0x210	Co je programování?	18
0x220	Exploitování programu	21
0x230	Obecné exploitovací techniky	24
0x240	Víceuživatelská přístupová práva k souborům	25
0x250	Paměť	26
0x251	<i>Deklarace paměti</i>	27
0x252	<i>Ukončení nulovým bajtem</i>	27
0x253	<i>Segmentace paměti programu</i>	28
0x260	Přetečení paměti	31
0x270	Přetečení zásobníku	33
0x271	<i>Exploitování bez kódu exploitu</i>	38
0x272	<i>Používání prostředí</i>	41
0x280	Přetečení v segmentech haldy a bss	51
0x281	<i>Základní přetečení v haldě</i>	52
0x282	<i>Přetečení ukazatelů na funkce</i>	57
0x290	Formátovací řetězce	65
0x291	<i>Formátovací řetězce a funkce printf()</i>	65
0x292	<i>Slabina ve formátovacích řetězcích</i>	71
0x293	<i>Čtení z libovolné paměťové adresy</i>	73
0x294	<i>Zápis na libovolnou paměťovou adresu</i>	75
0x295	<i>Přímý přístup k parametru</i>	83
0x296	<i>Objížďky s destruktory</i>	86
0x297	<i>Přepisování tabulky globálních offsetů</i>	93
0x2a0	Psaní shellkódu	97
0x2a1	<i>Běžné instrukce assembleru</i>	98
0x2a2	<i>Linuxová systémová volání</i>	98
0x2a3	<i>Ahoj světe!</i>	100
0x2a4	<i>Kód spouštějící shell</i>	103
0x2a5	<i>Nepoužívání jiných segmentů programu</i>	105
0x2a6	<i>Odstranění nulových bajtů</i>	107
0x2a7	<i>Ještě menší shellkód použitím zásobníku</i>	111

0x2a8	Tisknutelné ASCII instrukce	114
0x2a9	Polymorfní shellkód	116
0x2aa	Polymorfní tisknutelný shellkód	116
0x2ab	Disassembler	132
0x2b0	Návrat do libc	145
0x2b1	Návrat do system()	145
0x2b2	Zřetězení volání návratu do libc	147
0x2b3	Použití pomocného programu	149
0x2b4	Zapísování nul s návratem do libc	150
0x2b5	Zapísování více slov jediným voláním	153

0x300

SÍŤ 157

0x310	Co jsou sítě?	157
0x311	Model OSI	158
0x320	Zajímavé vrstvy v detailech	160
0x321	Síťová vrstva	160
0x322	Transportní vrstva	161
0x323	Linková vrstva	163
0x330	Odposlouchávání na síti	164
0x331	Aktivní odposlouchávání	167
0x340	Únos TCP/IP spojení	175
0x341	Únos přes RST	176
0x350	Odmítnutí služby	179
0x351	Ping smrti	180
0x352	Siza	180
0x353	Zahlčení přes ping	180
0x354	Zesilující se útoky	181
0x355	Distribuované DoS zahlčení	181
0x356	Zahlčení přes SYN pakety	181
0x360	Skenování portů	182
0x361	Tajné SYN skenování	182
0x362	Skenování FIN, X-mas a Null	183
0x363	Podvržené návsnady	183
0x364	Nečinné skenování	183
0x365	Proaktivní obrana	185

0x400

KRYPTOLOGIE 195

0x410	Teorie informace	196
0x411	Bezpodmínečná bezpečnost	196

	0x412	<i>One-time pad</i>	197
	0x413	<i>Distribuce kvantových klíčů</i>	197
	0x414	<i>Výpočetní bezpečnost</i>	198
0x420		Běh algoritmu	199
	0x421	<i>Asymptotické vyjádření</i>	200
0x430		Symetrické šifrování	201
	0x431	<i>Lov Groverův kvantový vyhledávací algoritmus</i>	202
0x440		Asymetrické šifrování	202
	0x441	<i>RSA</i>	203
	0x442	<i>kvantový faktorizační algoritmus Petera Shora</i>	206
0x450		Hybridní šifry	208
	0x451	<i>Útoky typu muž-uprostřed</i>	208
	0x452	<i>Rozdíly v otiscích hostitele protokolu SSH</i>	211
	0x453	<i>Fuzzy otisky</i>	214
0x460		Lámání hesel	219
	0x461	<i>Slovníkové útoky</i>	220
	0x462	<i>Důkladné útoky hrubou silou</i>	222
	0x463	<i>Vyhledávací tabulka hašů</i>	223
	0x464	<i>Pravděpodobnostní matice hesla</i>	224
0x470		Bezdrátové 802.11b šifrování	236
	0x471	<i>Wired Equivalent Privacy (WEP)</i>	236
	0x472	<i>Proudová šifra RC4</i>	237
0x480		WEP útoky	238
	0x481	<i>Offline útoky hrubou silou</i>	238
	0x482	<i>Opětovné použití klíče</i>	239
	0x483	<i>Dekódovací slovníkové tabulky založené na IV</i>	240
	0x484	<i>Přesměrování IP</i>	240
	0x485	<i>Útok Flunder, Mantin a Shamir (FMS)</i>	242

0x500

ZÁVĚR 253

Odkazy	254
Software	256

REJSTŘÍK 257