

Indice generale

Prefazione all'edizione italiana	XI
Prefazione all'edizione originale.....	XIII
Capitolo 1 Introduzione.....	1
Capitolo 2 Programmazione	5
0x210 Che cos'è la programmazione?	6
0x220 Pseudocodice	7
0x230 Strutture di controllo.....	7
0x231 If-Then-Else	8
0x232 Cicli while/until	9
0x233 Cicli for	10
0x240 Altri concetti fondamentali di programmazione	11
0x241 Variabili	11
0x242 Operatori aritmetici	12
0x243 Operatori di confronto.....	13
0x244 Funzioni	15
0x250 Iniziamo a sporcarci le mani	18
0x251 Il quadro d'insieme.....	19
0x252 Il processore x86	22
0x253 Il linguaggio assembly	24
0x260 Torniamo alle basi.....	35
0x261 Stringhe	36
0x262 Valori con segno, senza segno, long e short	39
0x263 Puntatori	41
0x264 Stringhe di formato.....	45
0x265 Typcasting.....	48
0x266 Argomenti della riga di comando.....	55
0x267 Ambito delle variabili	59

0x270 Segmentazione della memoria	65
0x271 Segmenti di memoria in C	72
0x272 Uso dell'heap	74
0x273 malloc() con controllo degli errori	76
0x280 Costruire sulle fondamenta	78
0x281 Accesso ai file	78
0x282 Permessi sui file	83
0x283 ID utente	84
0x284 Strutture	92
0x285 Puntatori a funzione	95
0x286 Numeri pseudocasuali	96
0x287 Un gioco di fortuna	98

Capitolo 3 Exploit.....111

0x310 Tecniche di exploit generalizzate	114
0x320 Buffer overflow	114
0x321 Vulnerabilità a buffer overflow basate sullo stack	117
0x330 Esperimenti con la shell BASH	128
0x331 Uso dell'ambiente	136
0x340 Overflow in altri segmenti	144
0x341 Un overflow di base fondato sull'heap	144
0x342 Overflow di puntatori a funzioni	149
0x350 Stringhe di formato	160
0x351 Formato dei parametri	160
0x352 Vulnerabilità delle stringhe di formato	162
0x353 Lettura da indirizzi di memoria arbitrari	164
0x354 Scrittura su indirizzi di memoria arbitrari	165
0x355 Accesso diretto ai parametri	172
0x356 Uso di short write	174
0x357 Deviazioni con .dtors	175
0x358 Un'altra vulnerabilità di noteseach	180
0x359 Sovrascrittura della tabella GOT	182

Capitolo 4 Reti185

0x410 Il modello OSI	185
0x420 Socket	187
0x421 Funzioni per i socket	188
0x422 Indirizzi dei socket	190
0x423 Ordinamento byte di rete	192
0x424 Conversione dell'indirizzo Internet	192
0x425 Un semplice esempio di server	193
0x426 Un esempio di client web	196
0x427 Un piccolo server web	202

0x430 I livelli inferiori	206
0x431 Livello di collegamento dati	207
0x432 Livello di rete	208
0x433 Livello di trasporto	210
0x440 Sniffing di rete	213
0x441 Sniffer di socket raw	215
0x442 Sniffer libpcap	217
0x443 Decodifica dei livelli	219
0x444 Sniffing attivo	228
0x450 DoS (Denial of Service)	240
0x451 SYN flooding	240
0x452 Ping of Death	244
0x453 Teardrop	244
0x454 Ping flooding	245
0x455 Attacchi di amplificazione	245
0x456 Attacco DoS distribuito	246
0x460 Dirottamento TCP/IP	246
0x461 Dirottamento RST	247
0x462 Ancora sul dirottamento	251
0x470 Scansione di porte	252
0x471 Scansione SYN stealth	252
0x472 Scansioni FIN, X-mas e Null	252
0x473 Esche (decoy)	253
0x474 Scansione idle	253
0x475 Difesa proattiva	255
0x480 Qualche hack in pratica	260
0x481 Analisi con GDB	261
0x482 Attacco con bombe a mano	263
0x483 Shellcode per il binding di porte	266

Capitolo 5 Shellcode269

0x510 Assembly e C	269
0x511 Chiamate di sistema Linux in assembly	272
0x520 Il percorso dello shellcode	274
0x521 Istruzioni assembly che usano lo stack	275
0x522 Esame con GDB	277
0x523 Rimozione dei byte null	278
0x530 Shellcode che avvia una shell	283
0x531 Questione di privilegi	287
0x532 Ancora più piccolo	289
0x540 Shellcode per il binding di porte	291
0x541 Duplicazione di descrittori di file standard	295
0x542 Strutture di controllo per diramazione del codice	296
0x550 Shellcode di connect-back	301

Capitolo 6 Contromisure307

0x610	Contromisure che rilevano gli attacchi.....	308
0x620	Daemon di sistema	309
0x621	Corso rapido sui segnali	310
0x622	Il daemon tinyweb	312
0x630	Strumenti del mestiere.....	316
0x631	Lo strumento di exploit tinywebd	316
0x640	File di log.....	321
0x641	Mescolarsi tra la folla	322
0x650	Trascurare l'ovvio.....	323
0x651	Un passo per volta.....	324
0x652	Rimettere insieme il tutto	327
0x653	I figli al lavoro	333
0x660	Camuffamento avanzato	335
0x661	Spoofing dell'indirizzo IP registrato nei log	335
0x662	Exploit senza tracce nei log	339
0x670	L'infrastruttura completa.....	341
0x671	Riuso di socket	342
0x680	Contrabbando del payload.....	346
0x681	Codifica di stringhe.....	346
0x682	Come nascondere un NOP sled.....	349
0x690	Restrizioni per i buffer	350
0x691	Shellcode polimorfico con caratteri ASCII stampabili ..	352
0x6a0	Rafforzare le contromisure.....	362
0x6b0	Stack non eseguibile	362
0x6b1	ret2libc	363
0x6b2	Ritorno in system().....	363
0x6c0	Spazio nello stack a generazione casuale	365
0x6c1	Investigazioni con BASH e GDB.....	366
0x6c2	Giocare di sponda con linux-gate	370
0x6c3	Applicazione delle conoscenze	373
0x6c4	Un primo tentativo	374
0x6c5	Giocare le proprie carte.....	375

Capitolo 7 Crittologia379

0x710	Teoria dell'informazione	380
0x711	Sicurezza incondizionata	380
0x712	One-time pad	380
0x713	Distribuzione quantistica della chiave	381
0x714	Sicurezza computazionale.....	382
0x720	Tempo di esecuzione di un algoritmo	382
0x721	Notazione asintotica.....	383
0x730	Cifratura simmetrica.....	384
0x731	Algoritmo di ricerca quantistica di Lov Grover	385

0x740 Cifratura asimmetrica	386
0x741 RSA	386
0x742 Algoritmo di fattorizzazione quantistica di Peter Shor	389
0x750 Sistemi di cifratura ibridi	391
0x751 Attacchi man-in-the-middle	391
0x752 Fingerprint di host diversi sul protocollo SSH	395
0x753 Fingerprint fuzzy	398
0x760 Cracking delle password	402
0x761 Attacchi con dizionario	404
0x762 Attacchi di forza bruta esaustivi.....	406
0x763 Tabella di lookup degli hash.....	408
0x764 Matrice di probabilità delle password.....	408
0x770 Cifratura su reti wireless 802.11b.....	417
0x771 WEP (Wired Equivalent Privacy).....	418
0x772 Sistema di cifratura a flusso RC4.....	419
0x780 Attacchi WEP.....	420
0x781 Attacchi di forza bruta offline	420
0x782 Riutilizzo del keystream	421
0x783 Tabelle di dizionario per la decifrazione basate su IV	422
0x784 Reindirizzamento IP.....	422
0x785 Attacco FMS (Fluhrer, Mantin e Shamir)	424

Capitolo 8 Conclusione.....433

0x801 Riferimenti bibliografici.....	434
0x802 Fonti.....	435

Indice analitico.....437