Table des matières

À propos de l'auteur IX

Remerciements X

Préface XI

0x100 Introduction 1

0x200 Programmation 7

0x210 Qu'est-ce que programmer ? 8

0x220 Pseudo-code 9

0x230 Structures de contrôle 9

0x231 If-Then-Else 10

0x232 Boucles while/until 11

0x233 Boucles for 12

0x240 Autres concepts fondamentaux de la programmation 13

0x241 Variables 13

0x242 Opérateurs arithmétiques 14

0x243 Opérateurs de comparaison 16

0x244 Fonctions 18

0x250 Mettre les mains dans le cambouis 21

0x251 Un ensemble plus vaste 22

0x252 Le processeur x86 26

0x253 Langage assembleur 27

0x260 Retour aux fondamentaux 40

0x261 Chaîne de caractères 40

0x262 Signé, non signé, long et court 44

0x263 Pointeurs 46

0x264 Chaînes de format 50

0x265 Forçage de type 54

0x266 Arguments de la ligne de commande 61

0x267 Portée d'une variable 65

0x270 Segmentation de la mémoire 72
0x271 Segments de mémoire en C 79
0x272 Utiliser le tas 81
0x273 malloc() avec gestion des erreurs 84
0x280 Extension des fondamentaux 85
0x281 Accès aux fichiers 86
0x282 Autorisations de fichiers 91
0x283 Identifiants d'utilisateurs 93
0x284 Structures 101
0x285 Pointeurs de fonction 105
0x286 Nombres pseudo-aléatoires 106
0x287 Un jeu de hasard 108

0x300 Exploitation 121
0x310 Techniques d'exploitation généralisées 124
0x320 Débordements de tampon 124
0x321 Débordement de tampon basé sur une pile 128
0x330 Expériences avec BASH 140
0x331 Utiliser l'environnement 149
0x340 Débordements dans d'autres segments 157
0x341 Débordement de base dans le tas 157
0x342 Débordement des pointeurs de fonction 163
0x350 Chaînes de format 175
0x351 Paramètres de format 175
0x352 Vulnérabilité de la chaîne de format 178
0x353 Lire à des adresses mémoire quelconques 180
0x354 Écrire à des adresses mémoire quelconques 181
0x356 Utiliser des écritures courtes 190
0x357 Détours par .dtors 192
0x358 Autre vulnérabilité de notesearch 197
0x359 Écraser la Global Offset Table 199

0x400 Réseau 203
0x410 Modèle OSI 203
0x420 Sockets 206
0x421 Fonctions pour les sockets 207

0x422 Adresses de socket 209
0x423 Ordre des octets du réseau 211
0x424 Convertir une adresse Internet 211
0x425 Exemple de serveur simple 212
0x426 Exemple de client Web 216
0x427 Un miniserveur Web 222
0x430 Plonger dans les couches inférieures 226
0x431 Couche liaison de données 227
0x432 Couche réseau 229
0x433 Couche transport 231
0x440 Renifler le réseau 233
0x441 Renifleur de socket en mode raw 236
0x442 Renifleur avec libpcap 237
0x443 Décoder les couches 240
0x444 Reniflage actif 249
0x450 Déni de service 262
0x451 Saturation SYN 262
0x452 Le ping de la mort 267
0x453 Attaque teardrop 267
0x454 Saturation de ping 267
0x455 Attaques par amplification 268
0x456 DoS distribué 269
0x460 Détournement TCP/IP 269
0x461 Détournement RST 270
0x462 Détournement continu 275
0x470 Scanner les ports 275
0x471 Scan SYN furtif 275
0x472 Scans FIN, X-mas et Null 276
0x473 Forger des leurres 276
0x474 Scan passif 277
0x475 Défense proactive 279
0x480 Attaquer quelqu'un 285
0x481 Analyser avec GDB 286
0x482 C'est presque gagné 288
0x483 Shellcode de liaison à un port 291

0x500 Shellcode 295
0x510 Assembleur contre langage C 295
0x511 Appels système Linux en assembleur 298
0x520 Vers un shellcode 300
0x521 Utiliser la pile en assembleur 301
0x522 Enquêter avec GDB 303
0x523 Supprimer les octets nuls 304
0x530 Shellcode de lancement d'un shell 310
0x531 Une question de privilèges 314
0x532 Toujours plus petit 317
0x540 Shellcode de liaison à un port 318
0x541 Dupliquer des descripteurs de fichiers standard 322
0x542 Branchements 324
0x550 Shellcode connect-back 329

0x600 Contre-mesures 335
0x610 Contre-mesures de détection 336
0x620 Démons système 336
0x621 Formation rapide aux signaux 338
0x622 Démon tinyweb 340
0x630 Outils 345
0x631 Outil d'exploitation de tinywebd 345
0x640 Fichiers des journaux 350
0x641 Se fondre dans la foule 351
0x650 Passer à côté de l'évident 353
0x651 Une chose à la fois 353
0x652 Tout remettre ensemble 357
0x653 Faire travailler les enfants 363
0x660 Camouflage élaboré 365
0x661 Mystifier l'adresse IP consignée 365
0x662 Mener un exploit sans journalisation 369
0x670 Infrastructure complète 372
0x671 Réutiliser une socket 372
0x680 Charge utile clandestine 376
0x681 Coder une chaîne de caractères 377
0x682 Cacher un sled 380

0x690 Restrictions sur les tampons 381
0x691 Shellcode polymorphe à caractères ASCII imprimables 383
0x6a0 Renforcer les contre-mesures 394
0x6b0 Pile non exécutable 394
0x6b1 ret2libc 395
0x6b2 Retourner dans system() 395
0x6c0 Zone de pile aléatoire 397
0x6c1 Investigations avec BASH et GDB 399
0x6c2 Rebondir contre linux-gate 403
0x6c3 Appliquer les connaissances 406
0x6c4 Une première tentative 406
0x6c5 Jouer de chance 408

0x700 Cryptologie 411
0x710 Théorie de l'information 412
0x711 Sécurité inconditionnelle 412
0x712 Masques jetables 412
0x713 Cryptographie quantique 413
0x714 Sécurité informatique 414
0x720 Temps d'exécution d'un algorithme 414
0x721 Notation asymptotique 416
0x730 Chiffrement symétrique 416
0x731 Algorithme de recherche quantique de Lov Grover 418
0x740 Chiffrement asymétrique 418
0x741 RSA 418
0x742 Algorithme de factorisation quantique de Peter Shor 423
0x750 Chiffrement hybride 424
0x751 Attaque de l'homme du milieu 425
0x752 Différencier les empreintes d'hôtes du protocole SSH 429
0x753 Empreintes floues 432
0x760 Craquer des mots de passe 437
0x761 Attaques par dictionnaire 438
0x762 Attaques exhaustives par force brute 441
0x763 Table de correspondance hachée 443
0x764 Matrice de probabilité des mots de passe 443

0x770 Chiffrement dans les réseaux sans fil 802.11b 454
0x771 Wired Equivalent Privacy 454
0x772 Chiffrement par flot RC4 456
0x780 Attaques du WEP 457
0x781 Attaques hors ligne par force brute 457
0x782 Réutiliser la séquence d'octets 458
0x783 Tables de déchiffrement par dictionnaire basé sur les IV 459
0x784 Redirection IP 459
0x785 Attaque Fluhrer, Mantin et Shamir 461

0x800 Conclusion 473
0x810 Références 474
0x820 Sources 476

Index 477

Mises à jour 499

À propos de l'environnement de développement et de test 499