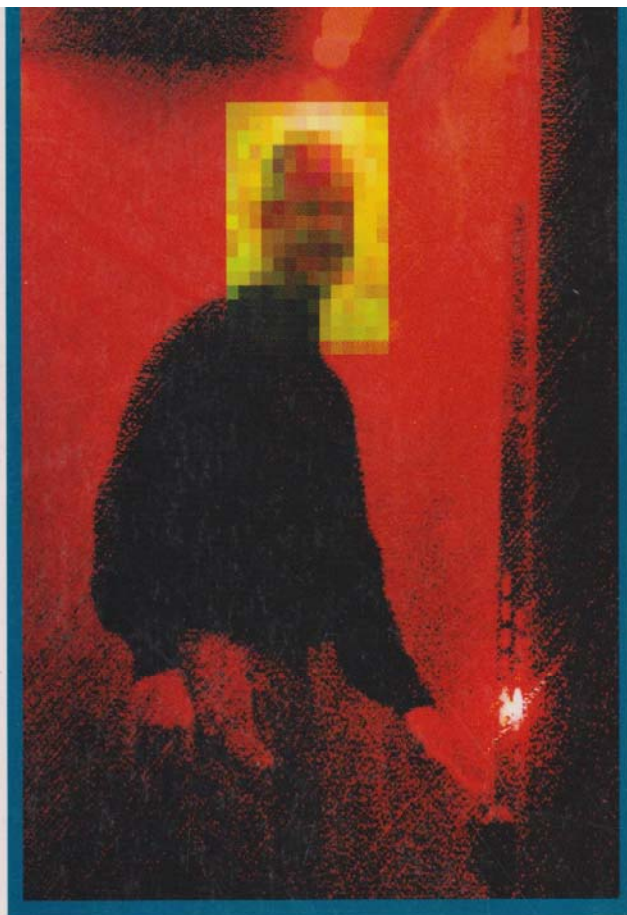




Eric Cole

*Écrit par
un expert de la
— CIA —*

Hackers

Attention danger !

Collection

Référence



CAMPUSPRESS

Les codes sources sont disponibles sur

www.campuspress.net



005-446-1

2-005-446-1

Table des matières

Hackers Attention danger !

Eric Cole




CAMPUSPRESS

Retrouvez
tous nos livres sur
www.campuspress.net

Table des matières

Introduction	1
Chapitre 1. Introduction	3
L'âge d'or du piratage informatique	4
L'ampleur du problème	5
La tendance générale	6
Comment est-on arrivé à cette situation ?	11
Que font les entreprises	13
La tolérance zéro	14
L'occultation du problème de la sécurité par l'effet de masse	15
Les systèmes sécurisés après coup	15
L'erreur du découragement	15
Que doivent faire les entreprises	16
Investir dans la prévention et la détection	16
Supprimer les plus gros trous de sécurité	17
Elever le niveau de sécurité pour décourager les attaques les plus triviales	17
La priorité de la détection	18
La sensibilisation des employés	19
La défense en profondeur	20
L'objectif de ce livre	20
Du côté du droit	21
Les sujets abordés dans ce livre	21
En résumé	22
Chapitre 2. Les techniques des pirates et leurs motivations	23
Qu'est-ce qu'un exploit ?	23
Les différentes phases d'une attaque	25
La reconnaissance passive	27
La reconnaissance active	28
L'exploitation d'un système	30
Le téléchargement de programmes	34
Le transfert de données	35

La préservation de l'accès	35
L'effacement des traces	36
Les différents types d'attaques	37
Les différentes catégories d'exploits	39
Les attaques via Internet	39
Les attaques sur un réseau local	42
Les attaques locales	47
Les attaques hors ligne	51
Les accès empruntés par les attaquants	52
Les ports	53
Les objectifs poursuivis par les attaquants	57
La confidentialité	57
L'intégrité	58
La disponibilité	59
En résumé	59
Chapitre 3. La collecte des informations	61
Les étapes de la collecte d'informations	62
La recherche des informations préliminaires	63
La détermination de la plage des adresses du réseau	70
La recherche d'hôtes actifs	77
La recherche des ports ouverts	79
La détermination du système d'exploitation	83
La détermination des services exécutés sur les différents ports ouverts	85
L'établissement de la carte du réseau	87
Le bilan de la collecte d'informations	90
Un test d'intrusion	90
Whois	91
La recherche Web dans la base de données de l'ARIN	93
traceroute	94
La carte du réseau	98
Le lancement d'un exploit	101
En résumé	101
Chapitre 4. Les attaques par usurpation	103
Pourquoi usurper	104
Les types d'usurpations	104
L'usurpation de l'adresse IP	104
L'usurpation de l'adresse e-mail	114

L'usurpation Web	121
Les usurpations non techniques	136
En résumé	139
Chapitre 5. Le détournement de session	141
L'usurpation et le détournement de session	142
Les différents types de détournement de session	143
Les concepts de TCP/IP	144
Le protocole TCP	144
Les étapes d'un détournement de session	147
La recherche d'une cible	148
L'évaluation de la prévisibilité des numéros de séquence	148
La recherche d'une session active	150
La prévision des numéros de séquence	151
La déconnexion de l'utilisateur	151
La prise de contrôle de la session	151
Les tempêtes d'ACK	152
Les programmes de détournement de session	153
Juggernaut	153
Hunt	164
TTY Watcher	172
IP Watcher	173
Le profil de la menace	174
Se protéger contre les attaques par détournement de session	175
Le cryptage des communications	175
L'utilisation d'un protocole sécurisé	176
Les restrictions sur les connexions entrantes	176
La minimisation des accès distants	176
Le recours (inefficace) à des procédures d'authentification robustes	177
En résumé	177
Chapitre 6. Les attaques par déni de service	179
Qu'est-ce qu'une attaque par déni de service ?	180
Les différents types d'attaques par déni de service	180
Qu'est-ce qu'une attaque par déni de service distribuée ?	181
Pourquoi est-il difficile de se protéger contre les attaques DoS ?	182
Les différents types d'attaques DoS	184
Le ping de la mort	185
SSPing	188

Land	190
Smurf	194
SYN flood	198
La monopolisation du processeur, ou l'exploit CPU Hog	203
Win Nuke	207
RPC Locator	210
Caractéristiques de l'exploit	210
Jolt2	213
Bubonic	219
Microsoft Incomplete TCP/IP Packet Vulnerability, ou la vulnérabilité des systèmes Microsoft vis-à-vis des paquets TCP/IP incomplets	225
HP Openview Node Manager SNMP DoS Vulnerability, ou la vulnérabilité aux attaques DoS du nœud Manager SNMP dans HP Openview	226
NetScreen Firewall Denial of Service Vulnerability, ou la vulnérabilité du pare-feu NetScreen aux attaques DoS	227
Checkpoint Firewall DoS Vulnerability, ou la vulnérabilité du pare-feu Checkpoint aux attaques DoS	228
Les outils d'attaque DoS	229
Targa	229
Les outils d'attaque DDoS	231
TFN2K (Tribal Flood Network 2000)	232
Trinoo	235
Stacheldraht	238
Empêcher les attaques par déni de service	238
La configuration et le fonctionnement du réseau	238
La mise en place de limitations quant à l'usage de la bande passante	239
Appliquer tous les correctifs logiciels appropriés aux systèmes	239
Exécuter le moins de services possible	240
N'autoriser que le trafic nécessaire	240
Bloquer des adresses IP	241
Empêcher les attaques DDoS	241
Veiller à la sécurité des systèmes informatiques	242
Installer des systèmes de détection des intrusions	242
Auditer le réseau avec des scanners	243
Exécuter Zombie Zapper	244
En résumé	245

Chapitre 7. Les attaques par débordement de tampon	247
Qu'est-ce qu'un débordement de tampon ?	249
Comment les débordements de tampons fonctionnent-ils ?	250
Les types d'attaques par débordement de tampon	253
Pourquoi tant de programmes sont-ils vulnérables ?	253
Exemple d'attaque par débordement de tampon	254
Exemple de mise en œuvre d'une protection du code	255
Dix attaques par débordement de tampon	255
Le débordement de tampon dans NetMeeting	256
Le débordement de tampon dans Outlook	261
Le débordement de tampon dans Linuxconf	265
Le débordement de tampon ToolTalk	269
Le débordement de tampon IMAPD	273
Le débordement de tampon dans AOL Instant Messenger	276
Le débordement de tampon dans BuddyIcon, de AOL Instant Messenger	277
Le débordement de tampon dans les contrôles ActiveX de Microsoft Windows 2000	279
Le débordement de tampon dans le serveur du répertoire téléphonique d'IIS 4.0/5.0	280
Les procédures stockées étendues de SQL Server 2000	282
Se protéger des attaques par débordement de tampon	286
Fermer le port du service	286
Appliquer le correctif logiciel du vendeur	287
Filtrer le trafic spécifique à l'application au niveau du pare-feu	287
Tester les applications stratégiques	287
Exécuter les logiciels avec le minimum de privilèges	288
En résumé	288
Chapitre 8. La sécurité par mots de passe	289
Exemple d'une attaque type	290
L'état actuel de la sécurité par mots de passe	291
L'histoire de la sécurité par mots de passe	293
L'avenir de la sécurité par mots de passe	295
La gestion des mots de passe	298
Pourquoi les mots de passe sont-ils nécessaires ?	298
Pourquoi faut-il une stratégie de mots de passe ?	299
Qu'est-ce qu'un mot de passe robuste ?	300
Comment choisit-on des mots de passe robustes ?	301

Comment les mots de passe sont-ils protégés ?	301
L'encryptage	303
Les attaques sur les mots de passe	305
Qu'est-ce que le craquage des mots de passe ?	305
Pourquoi le craquage des mots de passe est-il important ?	308
Les types d'attaques sur les mots de passe	311
Les autres types d'attaques sur les mots de passe	315
En résumé	316
Chapitre 9. Les logiciels craqueurs de mots de passe pour Microsoft NT	319
Où les mots de passe sont-ils conservés dans NT ?	321
Le fonctionnement de l'encryptage des mots de passe dans NT	321
Tous les mots de passe peuvent être craqués	321
Les hachages de LAN Manager	322
Le "salt" des mots de passe	323
Les programmes de craquage des mots de passe NT	324
L0phtcrack	325
NTSweep	339
NTCrack	341
PWDump2	342
La comparaison des différents programmes	343
L'extraction des hachages des mots de passe	344
Se protéger des programmes craqueurs de mots de passe	345
La désactivation de l'authentification LAN Manager	345
L'application de la stratégie de sécurité pour les mots de passe	348
Mettre en place une stratégie de mots de passe robustes	350
Implémenter SYSKEY	351
Les mots de passe à usage unique	352
La biométrie	353
Auditer les accès aux fichiers stratégiques	354
Auditer les systèmes pour détecter la présence d'éventuels outils de craquage	354
Assurer la maintenance de la liste des comptes actifs	354
Limiter le nombre de personnes ayant un accès d'administrateur	355
En résumé	355
Chapitre 10. Les logiciels craqueurs de mots de passe pour UNIX	357
L'emplacement du fichier des mots de passe sur un système UNIX	358
Les fichiers shadow	360
L'encryptage des mots de passe sous UNIX	362

Les programmes de craquage des mots de passe	364
Crack	365
John the Ripper (John)	375
XIT	380
Slurpie	383
La comparaison des programmes	387
Se protéger des programmes de craquage de mots de passe	389
Utiliser des fichiers shadow	389
Passwd+ et le contrôle de la robustesse des mots de passe	390
En résumé	391
Chapitre 11. Les fondamentaux de Microsoft NT	393
Aperçu sur la sécurité de NT	394
La disponibilité du code source des exploits	395
Les principales fonctionnalités de NT	396
L'architecture générale de NT	397
La sécurité physique	398
Le Registre	399
Les services exécutés	403
L'administration des comptes	404
Les paramètres réseau	405
L'audit	407
NetBIOS	411
Les service packs	412
Les kits de ressources	413
Les guides de sécurisation de NT	418
En résumé	418
Chapitre 12. Exploits spécifiques à Windows NT	419
Les exploits visant NT	420
GetAdmin	421
SecHole	425
Red Button	429
Le trou de sécurité de RDS dans Microsoft IIS	432
Les partages Microsoft	438
Legion	445
La vulnérabilité "Relative shell Path"	460
Le détournement des DSN de NT avec les outils ODBC	465

Winfreeze	472
La vulnérabilité du Media Player de Windows aux URL JavaScript	473
La vulnérabilité de mstask.exe d'Internet Explorer	474
La vulnérabilité de MSHTML.DLL	475
La vulnérabilité "2001 IIS 5.0 Allows File Viewing"	476
La vulnérabilité de Media Player 7 exploitable via IE et Java	477
IE 5.x/Outlook permet l'exécution de programmes arbitraires .chm	478
IIS 5.0 permet l'exécution de commandes arbitraires sur le serveur Web	480
La vulnérabilité du contrôleur de domaine WINS à l'usurpation	481
En résumé	483
Chapitre 13. Les principes fondamentaux d'UNIX	485
Linux	485
Les zones de vulnérabilité d'UNIX	486
Les scripts exemple	486
Les logiciels superflus	488
Les ports ouverts	489
Les systèmes sans correctifs logiciels	489
Quelques aspects fondamentaux d'UNIX	490
Les commandes essentielles	491
Les permissions d'accès aux fichiers	491
Inetd	494
Netstat	496
Tripwire	496
TCP Wrappers	497
Lsof	498
Suid	498
En résumé	499
Chapitre 14. Les exploits particuliers à UNIX	501
Les exploits UNIX	502
Aglimpse	502
Campas	507
NetPR	510
DTprintinfo	520
L'exploit Sadmin	531
XWindows	537
La vulnérabilité de Catman	549
L'exploit rpc.statd	550
En résumé	552

Chapitre 15. La préservation des accès : backdoors et troyens	553
Porte dérobée et cheval de Troie	554
QAZ	556
Les agents en écoute des programmes troyens	557
Les rootkits	558
Les rootkits de niveau fichier	558
Les rootkits de niveau noyau	560
Les rootkits NT	561
Les rootkits UNIX	561
Les portes dérobées sur NT	564
L'exploit Brown Orifice	564
Donald Dick 1.55	570
SubSeven	579
Back Orifice	588
Les programmes "enveloppes", ou wrappers, de Back Orifice	591
En résumé	592
Chapitre 16. La dissimulation des traces	593
Comment les attaquants masquent-ils leurs traces ?	594
Les journaux	595
La journalisation Linux	595
La journalisation NT	607
Les attributs des fichiers	610
Les importations de fichiers	613
Se protéger des importations de fichiers	614
La dissimulation des traces sur le réseau	615
Loki	615
Reverse www Shel	616
La création de canaux de communication secrets avec Covert TCP	617
En résumé	618
Chapitre 17. Les autres types d'attaques	619
L'exploit Bind 8.2 NXT	620
Caractéristiques de l'exploit	620
Description du protocole	620
Description des variantes	621
Fonctionnement de l'exploit	622
Mise en œuvre de l'exploit	622
Signature de l'attaque	624

Comment se protéger de cette attaque ?	626
Code source/pseudocode	627
Les cookies comme mécanisme de transmission d'une attaque	
par débordement de tampon	627
Caractéristiques de l'exploit	627
Description du protocole CGI	628
Cookies : description du protocole	629
Fonctionnement de l'exploit	630
Comment se protéger de cet exploit ?	632
Code source/pseudocode	633
Les chaînes Community de SNMP	636
Caractéristiques de l'exploit	636
Description du protocole	637
Fonctionnement de l'exploit	640
Mise en œuvre de l'exploit	641
Signature de l'attaque	646
Code source/pseudocode	648
Dispositifs vulnérables	648
Informations supplémentaires	649
Dsniff et la capture des paquets sur le réseau	649
Caractéristiques de l'exploit	650
Description du protocole	650
Variantes	650
Présentation de Dsniff	651
Réalisation de l'exploit	655
Signature de l'attaque	656
Comment se protéger de cette attaque ?	657
Code source/pseudocode	658
Informations supplémentaires	658
L'exploit PGP ADK	658
Caractéristiques de l'exploit	658
Description du protocole	659
Fonctionnement de l'exploit	661
Schéma de l'exploit	667
Mise en œuvre de l'exploit	667
Signature de l'attaque	670
Comment se protéger de cette attaque ?	673
Informations supplémentaires	673

La vulnérabilité affectant les mots de passe de l'IOS Cisco	673
Caractéristiques de l'exploit	674
Qu'est-ce que l'IOS de Cisco ?	674
Différents types de mots de passe de l'IOS Cisco	675
Description des variantes	676
Fonctionnement de l'exploit	676
Mise en œuvre de l'exploit	680
Signature de l'attaque	681
Comment se protéger de cette attaque ?	682
Code source/pseudocode	683
Informations supplémentaires	684
L'attaque de "l'homme du milieu" contre la clé de session	684
Caractéristiques de l'exploit	684
Présentation	685
Description du protocole	685
Notions de base	686
Spécification du protocole d'échange de clés Otway-Rees	687
Fonctionnement de l'exploit	690
Description des variantes	692
Mise en œuvre de l'exploit	693
Signature de l'attaque	694
Comment se protéger de cet exploit ?	695
Code source/pseudocode	697
Informations supplémentaires	698
L'exploit HTTP Tunnel	698
Caractéristiques de l'exploit	698
Description du protocole	699
Mise en œuvre de l'exploit	700
L'outil HTTP Tunnel	701
Signature de l'attaque	701
Recommandations	702
Informations supplémentaires	702
En résumé	703
Chapitre 18. Les dix vulnérabilités majeures du classement du SANS	705
Les exploits du Top 10 du SANS	706
1. Les vulnérabilités BIND permettant une compromission root immédiate	707
2. Les programmes CGI vulnérables et les extensions d'application	708
3. Les failles dans les RPC	711

4. Les trous de sécurité des RDS	712
5. Les vulnérabilités aux débordements de tampon de Sendmail	713
6. Sadmin et mountd	714
7. Le partage des fichiers et la diffusion d'informations via NetBIOS	714
8. Les comptes utilisateur (ou root/administrateur) sans mot de passe ou avec des mots de passe faibles	716
9. Les vulnérabilités aux débordements de tampons de IMAP et de POP	718
10. Les chaînes community de SNMP définies par défaut à public et private	719
Complément : les vulnérabilités d'Internet Explorer et d'Office 2000 aux scripts	720
Les ports les plus menacés	721
Se protéger des vulnérabilités du Top 10 du SANS	723
En résumé	723
Chapitre 19. Quelques scénarios d'intrusions	725
Différents scénarios d'attaques	726
Scénario 1 : les attaques contre les modems	727
Scénario 2 : l'ingénierie sociale	728
Scénario 3 : l'exploitation de failles dans la sécurité physique	729
Scénario 4 : une attaque contre un système NT	730
Scénario 5 : une attaque contre un système UNIX	731
En résumé	732
Chapitre 20. Conclusion	733
Il n'est pas possible d'ignorer la sécurité	734
Quelques conseils d'ordre général pour protéger un site	734
Le principe de la défense en profondeur	735
Le principe du moindre privilège	736
Savoir ce qui est exécuté sur les systèmes	737
La primauté de la détection sur la prévention	737
Les tests et l'application des correctifs logiciels	738
Le contrôle régulier des systèmes	738
Les perspectives à court et moyen termes	739
Les perspectives à long terme	739
L'augmentation des incidents de sécurité	740
La survenue d'un incident majeur	740
L'obligation pour les vendeurs de fournir des produits plus sûrs	742

Annexe A. Ressources	745
Les sites généraux consacrés à la sécurité informatique	745
2600.com	745
allhack.com	745
Alw.nih.gov	746
anticode.com	746
auscert.org.au	746
Astalavista.com	746
bugtraq.com	746
CERIAS.CS.PURDUE.EDU	746
Cert.org	746
CIAC.LLNL.GOV	746
cultdeadcow.com	747
ftp.cert.dfn.de	747
deny.de	747
elitehackers.com	747
ENSLAVER.COM	747
firosoft.com/security/philez	747
First.org	747
ftp.nec.com	747
ftp.porcupine.org	747
ftp.win.tue.nl	748
geek-speak.net	748
hack.co.za	748
Hackernews.com	748
hackersclub.com	748
infosyssec.net	748
infowar.co.uk	748
insecure.org	748
L0pht.com	748
net.tamu.edu	749
neworder.box.sk	749
ntobjectives.com	749
packetstormsecurity.com	749
Phrack.org	749
porcupine.org	749
rogenic.com	749
SANS.ORG	749
securiteam.com	749

Securityfocus.com	750
Securitysearch.net	750
Sysinternals.com	750
technotronic.com	750
torus.ndirect.co.uk	750
ussrback.com	750
warmaster.de	750
whitehats.com	750
Wiretrip.net/rfp	750
www-arc.com	750
xforce.iss.net	751
Outils de piratage et de sécurité	751
Sites liés à la sécurité informatique	754
Sites et groupes de discussion	754
Listes de diffusion	756
Les vulnérabilités par systèmes d'exploitation	757
Sites sur la programmation	759
C/C++	759
MS-DOS	760
Visual Basic	760
Divers	761
Documentation en ligne	761
Moteurs de recherche	761
Cracks, Wares...	762
Trouver quelqu'un sur Internet	762
Sites consacrés au phreaking	763
Scanners en ligne	763
Index	765