

Le Grand Livre de

SecuriteInfo.com

<http://www.securiteinfo.com>

19 février 2004

Tous droits réservés (c) 2002-2004 Securiteinfo.com

Table des matières

Les attaques.....	12
Le Hacking.....	12
Qu'est-ce que c'est ?.....	12
Le but du hacking.....	12
Le hacking légal.....	12
Les types d'attaques.....	12
Introduction.....	12
Les attaques directes.....	13
Les attaques indirectes par rebond.....	13
Les attaques indirectes par réponse.....	14
Conclusion.....	15
L'attaque +++ATHZero.....	15
Qu'est-ce que c'est ?.....	15
Conséquences.....	15
Comment s'en protéger ?.....	15
L'attaque Boink.....	16
Qu'est-ce que c'est ?.....	16
Conséquences.....	16
Comment s'en protéger ?.....	16
L'attaque Cisco ® 7161.....	16
Qu'est-ce que c'est ?.....	16
Conséquences.....	16
Comment s'en protéger ?.....	16
L'attaque Click - WinNewk.....	16
Qu'est-ce que c'est ?.....	17
Conséquences.....	17
Comment s'en protéger ?.....	17
Le Mail Bombing.....	17
Qu'est-ce que c'est ?.....	17
L'attaque.....	17
Comment réagir ?.....	19
Vous avez été attaqué.....	24
Conclusion.....	24
L'attaque Out Of Band (OOB).....	25
Qu'est-ce que c'est ?.....	25
Conséquences.....	25
Comment s'en protéger ?.....	25
L'attaque NT Inetinfo.....	25
Qu'est-ce que c'est ?.....	25
Conséquences.....	26
Comment s'en protéger ?.....	26
Ping of death.....	26
Qu'est-ce que c'est ?.....	26
Qui peut provoquer cette attaque ?.....	26
Conséquences.....	26

Comment s'en protéger ?.....	26
L'attaque par requête HTTP incorrecte.....	26
Qu'est-ce que c'est ?.....	26
Conséquences	27
Comment s'en protéger ?.....	27
L'attaque Snork.....	27
Qu'est-ce que c'est ?.....	27
Conséquences.....	27
Comment s'en protéger ?.....	27
L'attaque SMTPd overflow.....	27
Qu'est-ce que c'est ?.....	27
Conséquences.....	27
Comment s'en protéger ?.....	28
L'ARP redirect.....	28
Qu'est-ce que c'est ?.....	28
Conséquences.....	28
Comment s'en protéger ?	28
L'attaque Bonk	28
Qu'est-ce que c'est ?.....	29
Conséquences	29
Comment s'en protéger ?	29
L'attaque BrKill	29
Qu'est-ce que c'est ?.....	29
Conséquences.....	29
Comment s'en protéger ?.....	29
L'attaque Coke.....	29
Qu'est-ce que c'est ?.....	29
Conséquences.....	30
Comment s'en protéger ?.....	30
Le FTP Bounce.....	30
Qu'est-ce que c'est ?.....	30
Conséquences.....	31
Comment s'en protéger ?	31
Land attack	31
Qu'est-ce que c'est ?.....	31
Conséquences.....	31
Comment s'en protéger ?.....	31
L'attaque NT Stop.....	31
Qu'est-ce que c'est ?.....	31
Conséquences	32
Comment s'en protéger ?	32
L'attaque Oshare.....	32
Qu'est-ce que c'est ?.....	32
Conséquences	32
Comment s'en protéger ?	32
Ping flooding.....	32
Qu'est-ce que c'est ?.....	32
Qui peut provoquer cette attaque ?.....	33
Conséquences.....	33

Comment s'en protéger ?	33
L'attaque Pong.....	33
Qu'est-ce que c'est ?.....	33
Conséquences.....	33
Comment s'en protéger	33
Les attaques Smack - Bloop	34
Qu'est-ce que c'est ?	34
Conséquences.....	34
Comment s'en protéger ?	34
L'attaque "Smurf".....	34
Qu'est-ce que c'est ?.....	34
Conséquences.....	34
Comment s'en protéger ?.....	35
L'attaque sPing - Jolt - IceNewk.....	35
Qu'est-ce que c'est ?.....	35
Conséquences.....	35
Comment s'en protéger ?.....	35
L'attaque Tear Drop.....	35
Qu'est-ce que c'est ?.....	35
Conséquences.....	35
Comment s'en protéger ?.....	36
Les trous de sécurité applicatifs.....	36
Qu'est-ce que c'est ?.....	36
Qui peut provoquer cette attaque ?	36
Conséquences	36
Comment s'en protéger ?.....	36
L'attaque UDP 0	36
Qu'est-ce que c'est ?.....	36
Conséquences	37
Comment s'en protéger ?.....	37
Les attaques WinArp - Poink	37
Qu'est-ce que c'est ?.....	37
Conséquences.....	37
Comment s'en protéger ?.....	37
L'attaque WINS 53 flood.....	37
Qu'est-ce que c'est ?.....	37
Conséquences	37
Comment s'en protéger ?.....	38
L'attaque WINS 137 flood	38
Qu'est-ce que c'est ?.....	38
Conséquences.....	38
Comment s'en protéger ?.....	38
Le Cross Site Scripting	38
Introduction	38
Le principe.....	38
Les conséquences possibles.....	39
Comment éviter ce type de faille.....	39
Les buffers overflow	39
Qu'est-ce que c'est ?.....	39

En bref.....	39
Technique.....	40
Solutions	42
Le Déni de Service (DoS)	42
Background.....	42
Définition.....	42
Types d'attaques.....	42
Contre-mesures	43
Le DNS Spoofing.....	43
Qu'est-ce que c'est ?.....	44
DNS Cache Poisoning.....	44
Comment s'en protéger ?.....	45
L'IP Spoofing.....	45
Qu'est-ce que c'est ?.....	45
Description de l'attaque.....	45
Conséquences	46
Comment s'en protéger ?.....	47
Dictionary Cracking	47
Qu'est-ce que c'est ?.....	47
Qui peut provoquer cette attaque ?.....	47
Conséquences	47
Comment s'en protéger ?	47
Brute Force Cracking.....	47
Qu'est-ce que c'est ?.....	48
Qui peut provoquer cette attaque ?	48
Conséquences.....	48
Un exemple : distributed.net.....	48
Comment s'en protéger ?	50
Tempest.....	50
Qu'est-ce que c'est ?.....	50
A quoi cela sert-il ?.....	50
Comment créer un système Tempest ?.....	50
Les avantages	50
Les limitations.....	50
Le futur.....	50
Les cartes magnétiques	51
Introduction	51
Enregistrement et lecture magnétique.....	51
La sécurité	54
Les chevaux de Troie.....	54
Qu'est-ce que c'est ?.....	54
Objectifs.....	54
Mode d'action.....	54
Contre-mesures	55
Cas concrets.....	55
Back Orifice 2000.....	58
Back Orifice 2000 : fiche technique.....	61
Conclusion.....	62
Les Key Loggers.....	62

Qu'est ce que c'est ?.....	62
Objectif.....	62
Mode d'action.....	62
Contre-mesures.....	65
Conclusion.....	66
Les espiogiciels.....	66
Qu'est-ce qu'un espiogiciel ?.....	67
Comment s'en protéger ?.....	67
La stéganographie.....	68
Qu'est-ce que c'est ?.....	68
Comment est-ce possible ?.....	70
Social Engineering.....	70
Qu'est-ce que c'est ?.....	70
Par téléphone.....	71
Comment parer cette méthode ?.....	71
Par lettre.....	71
Comment parer cette méthode ?.....	71
Par internet.....	71
Comment parer cette méthode ?.....	71
Par contact direct.....	72
Comment parer cette méthode ?.....	72
Conclusion.....	72
Les vers informatiques.....	72
Qu'est-ce que c'est ?.....	72
Qui peut provoquer cette attaque ?.....	72
Conséquences.....	73
Comment s'en protéger ?.....	73
Les virus informatiques.....	73
Qu'est-ce que c'est ?.....	73
Qui peut provoquer cette attaque ?.....	73
Conséquences.....	73
Comment s'en protéger ?.....	74
Cryptographie.....	75
La cryptographie.....	75
Qu'est-ce que c'est ?.....	75
La cryptographie symétrique et la cryptographie asymétrique	75
L'intégrité des informations	75
L'authentification des correspondants.....	76
PKI.....	76
SPKI.....	77
L'aspect légal.....	77
La cryptographie à algorithmes symétriques.....	77
Qu'est-ce que c'est ?.....	77
Le chiffrement par flot.....	77
Le chiffrement par bloc.....	78
Les Fonctions de Hachage.....	80
Background.....	80
Destruction d'information - Conservation de propriétés.....	80
Pourquoi hacher?.....	81

Ceci est un exemple, cliquez sur le lien de téléchargement pour obtenir le cours complet.

