

---

# Table des matières

<b>Avant-propos</b> .....	XI
<b>Préface</b> .....	XIII
<b>Remerciements</b> .....	XV
<b>Introduction</b> .....	XVII
Pourquoi faire un pentest ? .....	XVII
Pourquoi Metasploit ? .....	XVII
Un bref historique de Metasploit.....	XVIII
<b>À propos de ce livre</b> .....	XIX
Qu'y a-t-il dans ce livre ? .....	XIX
Une note sur l'éthique. ....	XX
<b>1. Les bases du test d'intrusion</b> .....	1
Les phases du PTES.....	1
<i>Préengagement</i> .....	2
<i>Collecte de renseignements</i> .....	2
<i>Détermination de la menace</i> .....	3
<i>Analyse des vulnérabilités</i> .....	3
<i>L'exploitation</i> .....	3
<i>Post exploitation</i> .....	3
<i>Le rapport</i> .....	4
Types de tests de pénétration.....	5
<i>Test de pénétration de type boîte blanche</i> .....	5
<i>Test de pénétration de type boîte noire</i> .....	5
Scanners de vulnérabilité.....	6
En résumé.....	6
<b>2. Les bases de Metasploit</b> .....	7
Terminologie.....	7
<i>Exploit</i> .....	8
<i>Payload</i> .....	8
<i>Shellcode</i> .....	8
<i>Module</i> .....	8

<i>Listener</i> .....	8
Les interfaces de Metasploit .....	9
MSFconsole .....	9
<i>Démarrer MSFconsole</i> .....	9
MSFcli .....	10
Armitage .....	12
Utilitaires de Metasploit .....	13
MSFpayload .....	13
MSFencode .....	14
<i>Nasm Shell</i> .....	15
Metasploit Express et Metasploit Pro .....	15
Conclusion .....	15
<b>3. Collecte de renseignements</b> .....	17
Collecte d'informations passive .....	18
<i>whois lookups</i> .....	19
Netcraft .....	19
NSLookup .....	20
Collecte d'informations active .....	21
<i>Le scan de ports avec Nmap</i> .....	21
<i>Travailler avec des bases de données dans Metasploit</i> .....	23
<i>Scan de ports avec Metasploit</i> .....	30
Scan ciblé .....	31
<i>Scan de Server Message Block</i> .....	31
<i>À la recherche de serveurs Microsoft SQL mal configurés</i> .....	33
<i>Scan de serveurs SSH</i> .....	34
<i>Scan FTP</i> .....	35
<i>Balayage de SNMP (Simple Network Management Protocol)</i> .....	37
Développement d'un scanner personnalisé .....	38
Perspectives .....	41
<b>4. Le scan de vulnérabilité</b> .....	43
Le scan de vulnérabilité de base .....	44
Scan avec <i>NeXpose</i> .....	45
<i>Configuration</i> .....	45
L'assistant "nouveau site" .....	46
Le nouvel assistant pour les scans manuels .....	48
<i>L'assistant d'édition de nouveau rapport</i> .....	49
<i>Importer le rapport dans le framework Metasploit</i> .....	51
<i>Exécuter NeXpose dans msfconsole</i> .....	51
Scan avec Nessus .....	53
<i>Configurer Nessus</i> .....	54

<i>Créer une politique de scan Nessus</i> .....	54
<i>Exécuter un scan Nessus</i> .....	56
<i>Rapports Nessus</i> .....	57
<i>Importer des résultats dans le framework Metasploit</i> .....	58
<i>Scanner avec Nessus depuis Metasploit</i> .....	59
Scanners de vulnérabilité spécialisés .....	62
<i>Valider des connexions SMB (Server Message Block)</i> .....	62
<i>Recherche d'accès VNC ouverts (Virtual Network Computing)</i> .....	64
<i>Scan pour trouver des serveurs X11 ouverts</i> .....	66
Utilisation des résultats de scan pour <i>Autopwning</i> .....	68
<b>5. Les joies de l'exploitation</b> .....	71
L'exploitation de base .....	72
Msf> show exploits .....	72
Msf> show auxiliary .....	72
Msf> show options .....	72
Msf> show payloads .....	75
Msf> show targets .....	77
Info .....	78
Set <i>et</i> unset .....	78
setg <i>et</i> unsetg .....	79
save .....	79
Exploitation d'une première machine .....	79
Exploitation d'une machine Ubuntu .....	85
Les payload pour tous les ports : bruteforcing de ports .....	89
Fichiers de ressources .....	91
Conclusion .....	93
<b>6. Meterpreter</b> .....	95
Compromission d'une machine virtuelle Windows XP .....	96
<i>Scan de ports avec Nmap</i> .....	96
<i>Attaque de MS SQL</i> .....	97
<i>Bruteforcing de MS SQL Server</i> .....	99
xp_cmdshell .....	101
<i>Commandes de base de Meterpreter</i> .....	103
<i>Capturer des keystrokes</i> .....	104
Récupération des noms d'utilisateurs et des mots de passe .....	105
<i>Extraire les mots de passe hachés</i> .....	105
<i>Découvrir le mot de passe d'un hash</i> .....	106
<i>Pass-the-hash</i> .....	108
<i>Escalade de privilège</i> .....	109
Usurpation de ticket Kerberos .....	111

Utilisation de <i>ps</i> .....	112
<i>Pivot</i> sur d'autres systèmes .....	114
Utilisation de scripts Meterpreter .....	118
<i>Migration d'un processus</i> .....	119
<i>Tuer un logiciel antivirus</i> .....	119
<i>Obtenir les hashes des mots de passe du système</i> .....	120
<i>Voir tout le trafic sur un ordinateur cible</i> .....	120
<i>Scraping d'un système</i> .....	120
<i>Utiliser Persistence</i> .....	121
Utilisation des modules de postexploitation .....	122
Upgrade d'un shell de commandes à un shell Meterpreter .....	123
Manipulation des API Windows avec l'add-on <i>Railgun</i> .....	125
Conclusion .....	126
<b>7. Éviter la détection</b> .....	127
Création de binaires autonomes avec <i>MSFPayload</i> .....	128
Échapper à la détection antivirus .....	130
Multiencodage .....	132
Modèles d'exécutables personnalisés .....	134
Lancement furtif d'un payload .....	135
Les packers .....	137
Un dernier mot sur le contournement d'antivirus .....	138
<b>8. Exploitation utilisant les attaques côté client</b> .....	139
Les exploits basés sur les navigateurs .....	140
<i>Comment les exploits basés sur les navigateurs fonctionnent-ils ?</i> .....	141
<i>À propos des NOP</i> .....	142
Utilisation d' <i>Immunity Debugger</i> pour décrypter du shellcode .....	143
Exploration de l'exploit <i>Aurora</i> d'Internet Explorer .....	146
Les exploits sur les formats de fichiers .....	151
Envoi du payload .....	153
Conclusion .....	154
<b>9. Metasploit : les modules auxiliaires</b> .....	155
Modules auxiliaires en pratique .....	159
Anatomie d'un module auxiliaire .....	163
Aller plus loin .....	169
<b>10. La boîte à outils du social engineer (SET, Social Engineer Toolkit)</b> .....	171
Configuration du SET .....	172
Le vecteur d'attaque <i>spear-phishing</i> .....	173

Vecteurs d'attaque web .....	180
Applet Java .....	180
<i>Exploits web côté client</i> .....	185
<i>Recueillir des noms d'utilisateurs et des mots de passe</i> .....	187
Tabnabbing .....	190
<i>MLITM (Man-Left-in-the-Middle)</i> .....	190
Web-jacking .....	191
<i>Tout rassembler dans une attaque sur plusieurs fronts</i> .....	193
Générateur de médias infectés .....	198
Le vecteur d'attaque <i>Teensy USB HID</i> .....	198
Caractéristiques supplémentaires du SET .....	202
Aller plus loin.....	202
<b>11. FAST-TRACK</b> .....	205
Microsoft SQL Injection.....	206
<i>SQL Injector – Attaque d'une Query String</i> .....	207
<i>SQL Injector – Attaque par le paramètre POST</i> .....	208
<i>Injection manuelle</i> .....	210
MSSQL Bruter .....	211
SQLPwnage.....	216
Le générateur de binaire-hexadécimal.....	219
Attaque massive côté client.....	220
Quelques mots à propos de l'automatisation .....	222
<b>12. Karmetasploit</b> .....	223
Configuration.....	224
Lancement de l'attaque .....	225
Recueil d'informations.....	228
Obtenir un shell.....	229
Conclusion.....	233
<b>13. Construire son propre module</b> .....	235
Exécuter une commande dans Microsoft SQL.....	236
Exploration d'un module Metasploit existant .....	238
Création d'un nouveau module.....	239
Powershell.....	240
<i>Exécuter l'exploit shell</i> .....	242
<i>Créer powershell_upload_exec</i> .....	244
<i>Convertir Hex en binaire</i> .....	245
<i>Compteurs</i> .....	246
<i>Exécuter l'exploit</i> .....	248
Le pouvoir de la réutilisation du code.....	249

<b>14. Créer votre propre exploit.....</b>	251
L'art du <i>fuzzing</i> .....	252
Contrôle du SEH.....	257
Contournement des restrictions du SEH.....	259
Trouver une adresse de retour .....	262
Mauvais caractères et exécution du code à distance.....	268
En conclusion .....	272
<b>15. Porter des exploits sur le framework Metasploit.....</b>	273
Fondamentaux de langage assembleur.....	274
<i>Registres EIP et ESP</i> .....	274
<i>Le set d'instruction JMP</i> .....	274
<i>NOP et slides NOP</i> .....	274
Port d'un <i>buffer overflow</i> .....	275
<i>Dépouiller l'exploit existant</i> .....	276
<i>Configurer la section exploit</i> .....	279
<i>Tester notre exploit de base</i> .....	279
<i>Implémenter des caractéristiques du framework</i> .....	281
<i>Ajouter de la randomisation</i> .....	282
<i>Retirer le slide NOP</i> .....	283
<i>Retirer le faux shellcode</i> .....	284
<i>Notre module complet</i> .....	285
Exploit par écrasement du SEH.....	287
En conclusion .....	297
<b>16. Scripts Meterpreter.....</b>	299
Les bases du scripting Meterpreter.....	299
L'API de Meterpreter.....	307
<i>Afficher une sortie</i> .....	308
<i>Appels API de base</i> .....	309
<i>Les mixins Meterpreter</i> .....	309
Les règles pour écrire des scripts Meterpreter .....	311
Création d'un script Meterpreter.....	312
Conclusion.....	320
<b>17. Simulation de pentest .....</b>	321
Pré-engagement.....	322
Collecte de renseignements.....	322
Modélisation des menaces .....	323
Exploitation.....	325
Personnalisation de la console MSF.....	325
Postexploitation.....	328

---

<i>Scanner le système Metasploitable</i> .....	329
<i>Identifier des services vulnérables</i> .....	331
Attaque d'Apache Tomcat .....	332
Attaque de services cachés .....	335
Effacement des traces .....	337
Conclusion.....	340
<b>Annexe A. Configurer les machines cibles</b> .....	341
Installation et paramétrage du système.....	341
Démarrage des machines virtuelles Linux.....	342
Mise en place d'un Windows XP vulnérable.....	343
<i>Configurer un serveur web sur Windows XP</i> .....	343
<i>Construire un serveur SQL</i> .....	344
<i>Mettre Back Track à jour</i> .....	348
<b>Annexe B. Aide-mémoire</b> .....	351
Commandes <i>MSFconsole</i> .....	351
Commandes Meterpreter.....	354
Commandes <i>MSFpayload</i> .....	357
Commandes <i>MSFencode</i> .....	358
Commandes <i>MSFcli</i> .....	358
<i>MSF, Ninja, Fu</i> .....	359
<i>MSFvenom</i> .....	359
Commandes Meterpreter postexploitation .....	360
<b>Index</b> .....	363