
Table des matières

Remerciements	VII
Ma femme	VII
Mes filles	VII
Ma famille.....	VII
Dave Kennedy	VII
Jared DeMott	VIII
À l'équipe de Syngress.....	VIII
À propos de l'auteur	IX
Introduction	XI
Nouveautés de la 2 ^e édition	XII
Public du livre	XIII
Singularité du livre.....	XIII
Raisons du choix de ce livre	XV
Suivre les exemples	XV
1. Tests d'intrusion	1
Introduction	1
<i>Préparer le terrain</i>	2
Introduction à Kali et à BackTrack Linux.....	4
Machine d'attaque	9
Mettre en place un laboratoire de hacking.....	12
Phases d'un test d'intrusion.....	15
Et ensuite.....	19
En résumé.....	20
2. Reconnaissance	21
Introduction	21
HTTrack	25
Opérateurs Google	28
The Harvester.....	34
Whois.....	37
Netcraft.....	40
Host	42
Extraire des informations du DNS	43

<i>NSLookup</i>	44
<i>Dig</i>	46
Fierce	47
Extraire des informations des serveurs de messagerie.....	47
MetaGooFil.....	48
ThreatAgent.....	50
Ingénierie sociale.....	51
Passer les informations au crible.....	53
Mettre en pratique cette phase.....	53
Et ensuite.....	54
En résumé.....	55
3. Scans	57
Introduction	57
Ping et balayage ping	61
Scan des ports	63
<i>Connexion en trois étapes</i>	65
<i>Scans TCP Connect avec Nmap</i>	66
<i>Scans SYN avec Nmap</i>	68
<i>Scans UDP avec Nmap</i>	69
<i>Scans Xmas avec Nmap</i>	72
<i>Scans Null avec Nmap</i>	73
<i>Le moteur de script de Nmap</i>	74
<i>Conclusion</i>	76
Scan de vulnérabilités.....	77
Mettre en pratique cette phase.....	81
Et ensuite.....	83
En résumé.....	83
4. Exploitation	85
Introduction	85
Medusa	87
Metasploit.....	91
John the Ripper	103
<i>Craquage local des mots de passe</i>	106
<i>Craquage à distance des mots de passe</i>	113
<i>Craquage des mots de passe Linux et élévation des privilèges</i>	114
Réinitialisation des mots de passe	115
Wireshark.....	118
Macof.....	119
Armitage	124
<i>Pourquoi apprendre cinq outils alors qu'un seul suffit ?</i>	126

Mettre en pratique cette phase.....	129
Et ensuite.....	132
En résumé.....	134
5. Ingénierie sociale	135
Introduction	135
Les bases de SET.....	136
Sites web en tant que vecteurs d'attaque.....	139
Le moissonneur d'informations de connexion.....	144
Autres options de SET	146
En résumé.....	148
6. Exploitation web	149
Introduction	149
Les bases du hacking web.....	150
Nikto	152
w3af.....	153
Indexation web	156
Intercepter des requêtes avec WebScarab.....	159
Attaques par injection de code	161
Cross-site scripting	166
Zed Attack Proxy.....	169
<i>Interception dans ZAP</i>	<i>170</i>
<i>Indexation dans ZAP.....</i>	<i>172</i>
<i>Scan dans ZAP</i>	<i>172</i>
Mettre en pratique cette phase.....	173
Et ensuite.....	174
Ressources supplémentaires	174
En résumé.....	175
7. Postexploitation et maintien d'accès.....	177
Introduction	177
Netcat.....	178
Cryptcat.....	184
Rootkits	185
<i>Hacker Defender</i>	<i>186</i>
Détecter les rootkits et s'en défendre.....	191
Meterpreter	192
Mettre en pratique cette phase.....	195
Et ensuite.....	196
En résumé.....	197

8. Conclusion d'un test d'intrusion	199
Introduction	199
Rédiger le rapport de test d'intrusion	200
<i>Synthèse</i>	201
<i>Rapport détaillé</i>	201
<i>Sorties brutes</i>	203
Participer	206
Et ensuite	208
Conclusion	210
Le cercle de la vie	210
En résumé	211
 Index	 213