

Proxmox

1. Présentation	9
2. Installation	11
3. Configuration	20
3.1 Présentation de l'interface	20
3.2 Les conteneurs OpenVZ	22
3.3 Travailler avec une ISO et KVM	34
3.4 Effectuer des sauvegardes	42
3.5 Les commandes de base	48
3.5.1 Administrer autrement Proxmox	48
3.5.2 Petit tour dans l'arborescence de Proxmox	51
3.5.3 Les commandes utiles	55
4. Conclusion	77

Machines virtuelles et services

1. Introduction	79
2. Serveur DHCP	80
2.1 Installation des paquets nécessaires	80
2.2 Configuration	81
3. OpenVPN	88
3.1 Installation des paquets	89
3.2 Configuration	90
3.2.1 Serveur	90
3.2.2 Client	96

4. Serveur FTP	100
4.1 Installation	100
4.2 Configuration	100
5. Serveur web	105
5.1 Installation	105
5.2 Configuration	105
6. Serveur Asterisk	119
6.1 Installation	119
6.2 Configuration	120
6.2.1 Sip.conf	120
6.2.2 Extensions.conf	121
6.3 Ajout de fonctions	123
6.3.1 Transfert d'appel	123
6.3.2 Mise en attente	124
6.3.3 Messagerie vocale	125
6.3.4 Configuration du MTA pour la messagerie vocale	126
6.4 Configuration d'un client SIP	127
7. Nagios	135
7.1 Nagios avec les fichiers sources	135
7.1.1 Installation	135
7.1.2 Configuration	139
7.2 Nagios avec les dépôts	140
7.2.1 Configuration d'Apache	140
7.2.2 Configurer Nagios pour le réseau LAN	142
7.2.3 Configurer Nagios pour le réseau WAN	147
7.2.4 Utilisation de NSClient	152
8. Conclusion	154

Mise en place des épreuves

1. Introduction	155
2. Création de cinq épreuves applicatives	156
2.1 Configuration de la machine	156
2.2 Les épreuves	159
2.2.1 Épreuve level1	159
2.2.2 Épreuve level2	160
2.2.3 Épreuve level3	160
2.2.4 Épreuve level4	161
2.2.5 Épreuve level5	162
2.3 Solutions	162
3. Création de cinq épreuves logiques	173
3.1 Épreuve level1	173
3.2 Épreuve level2	174
3.3 Épreuve level3	175
3.4 Épreuve level4	175
3.5 Épreuve level5	176
3.6 Solution des épreuves	177
4. Création d'épreuves crackme	181
4.1 Crackme 1	181
4.2 Épreuve crackme2	182
4.3 Solution crackme	183
4.3.1 Crackme1	183
4.3.2 Solution crackme2	185
4.4 D'autres crackmes	185
5. Création des épreuves web	186
5.1 Préparation du serveur	186
5.2 Des protections qui n'en sont pas	193
5.2.1 Création de la structure du site des épreuves	193

5.2.2 Implémentation de la première épreuve	197
5.2.3 Solution de la première épreuve	199
5.2.4 Implémentation de la deuxième épreuve	200
5.2.5 Solution de la deuxième épreuve	203
5.2.6 Implémentation de la troisième épreuve	205
5.2.7 Solution de la troisième épreuve	207
5.3 Des pages pas vraiment cachées	209
5.3.1 Implémentation de la quatrième épreuve	209
5.3.2 Solution de la quatrième épreuve	210
5.4 Mieux vaut avoir un mot de passe fort	214
5.4.1 Implémentation de la cinquième épreuve	214
5.4.2 Solution de la cinquième épreuve	215
5.5 L'accès aux bases de données	218
5.5.1 Implémentation de la sixième épreuve	218
5.5.2 Solution de la sixième épreuve	220
5.6 Passer les CAPTCHA	223
5.6.1 Implémentation de la septième l'épreuve	223
5.6.2 Solution de la septième épreuve	228

Plateformes d'entraînement

1. Introduction	233
2. Metasploitable	233
2.1 Liste des services	235
2.2 Services : les bases UNIX	236
2.3 Services : Backdoors	238
2.4 Vulnerable Web Services	242
2.4.1 Vulnérabilité web : Mutillidae	244
2.4.2 Vulnérabilité web : DVWA	245
2.4.3 Vulnérabilité web : Information Disclosure	246
2.5 Metasploit	247
2.5.1 Metasploit Command Line Interface (MSFCLI)	248
2.5.2 Metasploit Console (MSFCONSOLE)	251

2.5.3 Metasploit Web Interface (MSFWEB)	252
2.5.4 Meterpreter Payload	255
2.5.5 Framework 3	259
2.5.6 Fasttrack	264
3. WebGoat	266
3.1 Présentation	266
3.2 Installation de WebGoat	266
3.3 Utilisation de WebGoat	271
4. Conclusion	281

Le matériel indispensable

1. Introduction	283
2. Wi-Fi	284
2.1 Kit en vente en Chine	284
2.2 PirateBox	286
2.3 Wifi-Box	288
2.4 Routeur Wi-Fi	289
2.5 Wi-Fi Alfa USB	291
3. RFID	292
3.1 Distribution Linux	292
3.2 Nabaztag	295
3.3 Proxmark3	296
3.4 Lecteur de cartes RFID 125 KHz	297
3.5 Fabriquer soi-même	298
4. Bluetooth	299
4.1 Adaptateur Bluetooth	299
4.2 Ubetooth	299

4.3 Transmetteur Bluetooth.....	300
5. Cartes à puce	301
5.1 Lecteur de cartes à puce.....	302
5.2 Basic Card.....	303
6. Cartes magnétiques.....	305
7. Autres matériels	307
7.1 Arduino.....	307
7.2 Teensy.....	309
8. Lock picking.....	310
9. Carte SIM.....	311
10. Récupération de données	312
10.1 Adaptateur USB vers SATA et IDE.....	312
10.2 Bloqueur d'écriture.....	312
10.3 Bus Pirate.....	313
11. Conclusion	314

Sécurisation du PC

1. Introduction	315
2. Sécurisation sous Linux	315
2.1 Fail2ban.....	315
2.2 Snort.....	320
2.2.1 Installation.....	320
2.2.2 Configuration de la base de données MySQL.....	321

2.2.3 Configuration de snort pour SQL	322
2.2.4 Configuration de Snort	323
2.2.5 Initialisation des règles (attaques)	323
2.2.6 Comment exploiter les résultats	323
2.2.7 L'interface de Snort : BASE	324
2.3 Syslog	327
2.3.1 Fonctionnalités	328
2.3.2 Sévérité	329
2.3.3 Priorité	330
2.3.4 Configuration détaillée	333
2.4 Portsentry	336
2.4.1 Configuration de Portsentry	336
2.5 Iptables	338
2.5.1 Concepts	338
2.5.2 Comment définir une règle	339
2.5.3 Protection de la machine locale	340
2.5.4 Le suivi de connexion	343
2.5.5 Masquerade	346
2.6 Test de la machine	347
3. Sécurisation sous Windows	347
3.1 Maintenez à jour votre système	347
3.2 Vérifiez la protection de votre système	352
3.3 Installez un antivirus	354
3.3.1 Préambule	354
3.3.2 ClamWin	354
3.3.3 Avast	357
3.3.4 Kaspersky	361
3.4 Restez attentif	370
3.5 Conclusion sur la sécurisation de Windows	371
Index	373