

Table des matières

1. LA SÉCURITÉ ET LE SYSTÈME LINUX	1
Enjeux et objectifs de sécurité 2	
La menace 2	
Principaux facteurs de motivation des pirates 3	
Risques liés au type de connexion 3	
Risques liés aux failles des systèmes 4	
Émergence des systèmes Linux 4	
Linux et la sécurité 5	
Des distributions Linux sécurisées 5	
En résumé... 6	
2. L'ÉTUDE DE CAS : UN RÉSEAU À SÉCURISER	9
Une jeune entreprise 10	
Les besoins de la société en termes de services 10	
Les choix techniques initiaux de Tamalo.com 11	
Web et services associés 12	
Transfert de fichiers 12	
Base de données 12	
Résolution de noms 12	
Messagerie électronique 13	
Partage de fichiers 13	
Impression réseau 13	
L'infrastructure informatique vieillissante et vulnérable 13	
La compromission du site 14	
Mise en évidence des vulnérabilités 15	
La refonte du système informatique 15	
Le projet d'une nouvelle infrastructure réseau 16	
Études des flux réseau 18	
Vers des outils de communication sécurisés 18	
Un suivi et une gestion quotidienne du système d'information 20	
En résumé... 20	
3. ATTAQUES ET COMPROMISSIONS DES MACHINES	23
Kiddies, warez et rebonds 24	
Scénario de l'attaque du réseau de Tamalo.com 26	
Une faille dans le système 26	
L'exploitation de la faille (« exploit ») 26	
Utilité des scans réseau 26	
La compromission 27	
Analyse de la machine compromise 28	
Traces visibles sur le système avant réinitialisation 28	
Sauvegarde du système compromis 29	
Analyse fine de l'image du disque piraté 29	
Montage pour l'analyse 29	
Étude des fichiers de démarrage et configuration 30	
Étude des fichiers créés lors du piratage 30	
Analyse avec The Coroner toolkit 30	
Trousse à outils du pirate : le rootkit t0rn 33	
Sniffer réseau d'un rootkit 33	
Le mode promiscuous 35	
Rootkit : effacer les traces et masquer la présence du pirate 37	
Rootkit : la porte dérobée (backdoor) 38	
Rootkit t0rn : conclusion 38	
Détecter la compromission à partir des logs 39	
Origine de l'attaque 40	
En résumé... 42	
4. CHIFFREMENT DES COMMUNICATIONS AVEC SSH ET SSL 45	
Les quatre objectifs du chiffrement 46	
Authentification 46	
Intégrité 46	
Confidentialité 47	
Signature électronique 47	
Facteurs de fiabilité des techniques de chiffrement 47	
Algorithmes de chiffrement symétrique et asymétrique 48	
Chiffrement symétrique 48	
Chiffrement asymétrique 49	
Le protocole SSL (Secure Socket Layer) 51	
Qu'est ce que SSL ? 51	
SSL, comment ça marche ? 51	
Les certificats X.509 52	

- Authentification et établissement de la connexion SSL 53
- Utilisation de SSL par les applications client/serveur 54

Le protocole SSH (Secure Shell) 54

- Qu'est-ce que SSH ? 54
 - À quels besoins répond SSH ? 54
 - Caractéristiques d'OpenSSH 56
 - Installation d'OpenSSH 57
 - Fichiers de configuration d'OpenSSH 58
 - Activation et lancement du serveur SSH 58
 - Désactivation et arrêt du serveur SSH 59
 - Utilisation de SSH 59
 - Connexion interactive 59
 - Exécution de commandes à distance 59
 - Copie distante de fichiers ou de répertoires 60
 - Transfert interactif de fichiers 60
 - Options des commandes SSH 60
 - Authentification avec SSH 60
 - Configuration du service SSH 60
 - Authentification par mot de passe 61
 - Authentification à clé publique 61
 - Relais d'affichage X11 64
 - Gestion des accès au service SSH 65
- Dépannage 65
- L'alternative VPN 66
- En résumé... 67

5. SÉCURISATION DES SYSTÈMES 69

- Installation automatisée 70
- Mise à jour régulière des systèmes 73
 - Mise à jour et installation optimale avec APT 74
 - Mise à jour avec Red Hat Network 74
- L'indispensable protection par mot de passe au démarrage 74
- Mise en configuration minimale, limitation des services actifs 75
 - Identification des processus 76
 - Identification des ports réseau utilisés 76
 - Identification des services actifs 77
 - Désactivation des services inutiles 78
- Sécurisation du système de fichiers 79
 - Permissions des fichiers 79
 - Détection des fichiers dotés de droits trop permissifs 80
 - Droits suid et sgid 80
 - Alternative à la protection suid : sudo 81
 - Options de montage des systèmes de fichiers 82
- Gestion des accès et stratégie locale de sécurité 82
 - Compte privilégié root 82
 - Blocage des comptes inutiles 83
 - Filtrage réseau avec TCP Wrapper 83
- Configuration des services système cron et syslog 84
 - cron 84
 - syslog 84
- Configuration sécurisée de la pile TCP/IP 85
 - Ignorer certains messages ICMP 85

- ICMP Redirect 85
- ICMP Echo request 87
- ICMP Ignore Bogus Response 87
- Interdiction du source routing 87
- Surveillance des martiens ! 88
- Protection contre les attaques IP spoofing et SYN flooding 88
- Configuration en pare-feu avec IPtables 89
- Extension du noyau 89
- Serveur d'affichage X11 et postes de travail 89

En résumé... 90

6. SÉCURISATION DES SERVICES RÉSEAU : DNS, WEB ET MAIL 93

- Bases de la sécurisation des services réseau 94
- Service de résolution de noms DNS 95
 - Comment ça marche ? 96
 - Serveurs de noms et sécurité 97
 - Installation du logiciel BIND 97
 - Configuration des serveurs DNS 98
 - Compte non privilégié 98
 - Changement de la racine du système de fichiers avec « chroot » 98
 - Activation et lancement du serveur 103
 - Configuration des clients DNS 104
- Messagerie électronique 104
 - Comment ça marche ? 104
 - Les logiciels de transfert de courrier 105
 - Messagerie électronique et sécurité 106
 - Spam et relais ouvert 106
 - L'architecture du système de messagerie 107
 - Installation de sendmail 109
 - Activation de sendmail 109
 - Configuration de sendmail 110
 - Sendmail et Milter 115
 - Configuration antivirus et antispam à Tamalo.com 116
 - Lutte antivirus : Sendmail, Milter et ClamAV 117
 - Lutte antispam : Sendmail, milter et milter-greylst. 121
 - Installation d'IMAP 124
 - Configuration et activation du serveur IMAPS 124
- Serveur Web 125
 - Serveur Web et sécurité 125
 - Installation de HTTPD 125
 - Configuration et activation de HTTPD 126
- Sécurisation des accès nomades à la messagerie avec stunnel 127
 - Configuration du serveur stunnel accessible depuis l'extérieur 127
 - Authentification du serveur 127
 - Authentification des utilisateurs 128
 - Configuration de stunnel sur le serveur 129
 - Configuration d'un client nomade supportant SSL et l'authentification par certificat 132
 - Configuration d'un client nomade ne supportant pas SSL ou l'authentification par certificat 134
- En résumé... 135

7. FILTRAGE EN ENTRÉE DE SITE	137
But poursuivi	138
Principes de base du filtrage en entrée de site	138
Filtrage sans état	139
Adresses IP source et destination	139
Protocole, ports source et destination	139
Drapeaux TCP et filtrage en entrée	140
Les limites du filtrage sans état	142
Filtrage avec états	143
Politique de filtrage : avant la compromission, « tout ouvert sauf »	144
Politique de filtrage : du « tout ouvert sauf » au « tout fermé sauf »	145
Déploiement de service FTP avec (et malgré) les filtres	146
Filtrage d'un client FTP actif	147
Filtrage d'un serveur FTP destiné à fonctionner en mode actif	150
Filtrage d'un client FTP passif	150
Filtrage du serveur FTP passif, limitation du serveur à une plage de ports	150
En résumé...	151
8. TOPOLOGIE, SEGMENTATION ET DMZ	153
Pourquoi cloisonner ?	154
Définition des zones du réseau de Tamalo.com	155
Définition des flux à l'extérieur et à l'intérieur du réseau de Tamalo.com	155
Postes de travail	155
Serveurs applicatifs internes	155
Serveurs accessibles depuis l'extérieur et l'intérieur : DMZ	155
Topologie du réseau	156
Topologie à un seul pare-feu	156
Topologie à double pare-feu adoptée pour le réseau de Tamalo.com	157
Détails de la configuration réseau de Tamalo.com	158
DMZ	158
Services internes	160
Postes de travail	160
Comment segmenter ? Les VLAN et leurs limites	160
VLAN par port physique	160
VLAN par adresse MAC	161
Configuration VLAN retenue pour Tamalo.com	162
Proxy et NAT	163
Proxy	163
Traduction d'adresses NAT	165
Source NAT – un pour un – ou NAT statique	166
Source NAT -N pour M – ou NAT dynamique	168
Proxy versus NAT	171
Netfilter/IPtables	171
Fonctionnalités d'IPtables	171
Tables et chaînes	171
Écriture des règles	173
Suivi de connexion	173
Journalisation	173
Traduction d'adresses – NAT	174
Filtrage	174
Configuration IPtables des deux pare-feu Linux	175
Configuration IPtables de chaque poste de travail	177
Configuration IPtables du serveur SMTP	178
Marquage de paquets avec IPtables	178
Modification des champs TOS, TTL	178
Marquage simple du paquet	179
Pare-feu transparent, mode bridge	180
Positionnement du pare-feu transparent	180
Adressage IP	180
Proxy ARP	181
Configuration pratique du pare-feu transparent	182
Configuration en proxy ARP coté DMZ	182
Configuration en proxy ARP coté interne	182
Configuration des interfaces et mise en place des routes	182
Configuration IPtables	183
Sécurité du réseau sans fil	183
Risque d'accès frauduleux au réseau	183
Le protocole 802.1X	184
Risque d'écoute du réseau	185
En résumé...	186
9. SURVEILLANCE ET AUDIT	189
Des traces partout	190
Linux et le syslog	190
Empreinte des machines : Tripwire	192
Métrologie réseau avec MRTG	193
Installation et configuration de MRTG chez Tamalo.com	195
Configuration SNMP du firewall A pour accepter les requêtes MRTG	195
Installation et configuration de MRTG sur la machine d'analyse	196
NMAP	197
Audit réseau avec Nessus	197
Configuration de Nessus	198
Rapport d'audit	200
Détection d'intrusion : Snort	201
Mise en place de la sonde Snort	201
Configuration et validation de Snort, détection des scans	201
Le pot de miel	203
Tableau de bord de la sécurité	204
Les indicateurs de sécurité	204
Synthèses des indicateurs dans un tableau de bord	206
En résumé...	206

10. GESTION DES COMPTES UTILISATEUR ET AUTHENTIFICATION 209**Gestion centralisée des comptes utilisateur 210**

Authentification et identification 210

Pourquoi authentifier ? 211

Le système d'authentification 211

Linux et l'authentification 212

Le fichier /etc/group 212

Le fichier /etc/passwd 212

Le fichier /etc/shadow 213

Le fichier /etc/gshadow 214

Format du mot de passe chiffré 214

Gestion des comptes utilisateur 215

Principe de l'authentification par mot de passe 215

Linux et PAM 216

Linux et Name Service Switch 217

Network Information Service - NIS 217

Fonctionnement 218

Affichage des informations contenues dans les maps NIS 219

Répartition de charge et disponibilité 219

Rejoindre un domaine NIS et trouver son serveur 220

Limites du système NIS 220

Lightweight Directory Access Protocol - LDAP 221

Fonctionnement 221

LDAP et la sécurité 222

Répartition de charge et disponibilité 222

Limitation du système LDAP 222

Kerberos 223

Fonctionnement 223

Kerberos et la sécurité 224

Authentification unique ou « Single Sign On » 224

Limites du système Kerberos 225

Interopérabilité 225**En résumé... 226****A. INFRASTRUCTURE À GESTION DE CLÉS : CRÉATION DE L'AUTORITÉ DE CERTIFICATION DE TAMALO.COM 227****OpenSSL et les IGC 228****Création des certificats X.509 228**

Bi-clés RSA 228

Certificat X.509 auto-signé de l'autorité de certification 229

Demande de certificats utilisateur 231

Signature des certificats par l'autorité de certification 231

Création d'un fichier contenant la clé privée et le certificat au format PKCS12 232

Mise en œuvre d'un serveur Web sécurisé HTTPS 233

Création du certificat du serveur www.tamalo.com 233

Installation de la chaîne de certification sur le client 234

Installation d'un certificat personnel dans le navigateur 236

Utilisation des certificats pour signer et/ou chiffrer les courriers électroniques 237**En conclusion 239****B. AUTHENTIFICATION, MISE EN ŒUVRE DE NIS, LDAP ET KERBEROS 241****Mise en œuvre de NIS 241**

Installation du système NIS 241

Installation des paquetages NIS 242

Configuration du serveur maître NIS 242

Le fichier /etc/ypserv.conf 242

Le fichier /var/yp/securenets 243

Configuration du nom de domaine NIS 244

Lancement du serveur NIS 244

Configuration d'un client NIS 245

Le fichier de configuration /etc/yp.conf 245

Lancement du client NIS 246

Configuration de l'identification et de l'authentification 246

Création de comptes utilisateur 247

Modification du fichier /var/yp/Makefile 247

Création d'un groupe et d'un compte utilisateur 247

Consultation des maps NIS 248

Mise en œuvre de OpenLDAP 248

Introduction 248

Installation des paquetages OpenLDAP 249

Redirection des messages de logs 249

Configuration du serveur OpenLDAP 249

Comment le mot de passe du rootdn a-t-il été généré ? 250

Quelles sont les restrictions d'accès ? 251

Lancement du serveur OpenLDAP 251

Configuration des commandes client 251

Création du schéma de la base de données 251

Création d'un groupe 252

Création d'un compte utilisateur 253

Affichage d'un enregistrement 253

Configuration de l'identification et de l'authentification 254

Mise en œuvre de Kerberos 255

Installation d'un serveur Kerberos 5 255

Installation des paquetages Kerberos 5 256

Configuration du serveur Kerberos 5 256

Le fichier /etc/krb5.conf 256

Le fichier /var/kerberos/krb5kdc/kdc.conf 257

Le fichier /var/kerberos/krb5kdc/kadm5.acl 258

Création de la base de données Kerberos 5 258

Ajout d'un compte administrateur Kerberos 258

Création du fichier /var/kerberos/krb5kdc/kadm5.keytab 258

Lancement des instances Kerberos sur le serveur KDC 259

Configuration de l'authentification Kerberos 259

Création des comptes Kerberos 260

Définition des utilisateurs 260

INDEX 261