

Chapitre 1 Introduction

A. La certification LPI	22
1. Intérêt de la certification	22
2. La certification LPI en quelques points	22
3. Le programme de la certification LPI	22
a. Niveau 1	22
b. Niveau 2	22
c. Niveau 3	23
4. Le passage d'examen	23
B. Ce livre	24
1. Les informations techniques	24
2. Les travaux pratiques	24
C. Préparation des travaux pratiques	25
1. Téléchargement des logiciels	25
2. Installation du serveur alpha	26
a. Éléments nécessaires	26
b. Création de la machine virtuelle	26
c. Personnalisation de la machine virtuelle	26
d. Démarrage de la machine virtuelle et installation du système	26
3. Installation du serveur beta	28
a. Éléments nécessaires	28
b. Création de la machine virtuelle	28
c. Personnalisation de la machine virtuelle	28
d. Démarrage de la machine virtuelle et installation du système	29
e. Personnalisation du système installé	30
4. Installation de la station de travail	30
a. Éléments nécessaires	30
b. Création de la machine virtuelle	30
c. Personnalisation de la machine virtuelle	31
d. Démarrage de la machine virtuelle et installation du système	31
e. Configuration de l'adresse IP de la station	31

5. Ajout de périphérique supplémentaire à une machine existante	32
a. Ajout de disque dur (SATA)	32
b. Affectation du disque dur à la machine virtuelle	32
c. Ajout de carte réseau	32
d. Activation de la carte réseau sur la machine virtuelle	32

Chapitre 2 Gestion du stockage

A. Gestion et configuration des systèmes de fichiers	35
1. Gestion des systèmes de fichiers	35
a. Les systèmes de fichiers courants	35
b. Les systèmes de fichiers virtuels ou pseudo-filesystems	36
c. Création des filesystems	37
d. Vérification des filesystems	37
e. Commandes spécialisées des filesystems ext	38
f. Création de filesystem ext	38
g. Affichage et modification des filesystems ext	38
h. Dénomination des systèmes de fichiers	40
2. Gestion du swap	41
a. Pourquoi le swap et en quelle quantité ?	41
b. Optimisation du swap	42
3. Montage des filesystems	44
a. Montage et démontage	44
b. Visualisation des filesystems montés	45
c. Fichier fstab	45
d. Automontage	47
4. Protection des données stockées	49
a. Protection au niveau fichier	49
b. Protection au niveau disque ou partition	50
c. Protection au niveau filesystem	51
5. Gestion des disques durs	53
a. Détermination des fichiers spéciaux	53
b. Informations sur les périphériques de stockage	54
c. Gestion des performances avec hdparm	56

d. Gestion des défaillances matérielles.....	57
B. Sauvegardes.....	58
1. Les utilitaires d'archivage.....	58
a. La commande tar.....	58
b. La commande cpio.....	59
2. Les sauvegardes au niveau filesystem.....	60
a. Sauvegardes de filesystems ext.....	60
b. Sauvegardes de filesystems xfs.....	62
3. Les logiciels de sauvegarde.....	64
a. AMANDA.....	64
b. Bacula.....	64
c. BackupPC.....	64
d. Les logiciels commerciaux.....	64
4. Duplication et synchronisation de données.....	64
a. Copie binaire avec dd.....	64
b. Génération de fichier iso avec mkisofs.....	65
c. Synchronisation de données avec rsync.....	66
C. RAID.....	69
1. Les principaux niveaux de RAID.....	69
a. Le RAID 0.....	69
b. Le RAID 1.....	69
c. Le RAID 5.....	69
2. Configuration du RAID.....	70
a. Création du volume RAID.....	70
b. Vérification d'un volume RAID.....	70
c. Exploitation des volumes RAID.....	72
D. Logical Volume Manager.....	72
1. Architecture des volumes logiques.....	72
2. Commandes LVM.....	73
a. Création des éléments.....	73
b. Diagnostics LVM.....	74
c. Extension de volume logique.....	76

d. Réduction de LV	77
3. Exploitation des volumes logiques	78
a. Données sur les volumes logiques	78
b. Exploitation du snapshot LVM pour les sauvegardes	79
E. Validation des acquis : questions/réponses	81
F. Travaux pratiques	83
a. Création d'un fichier de swap	83
b. Activation de l'espace de swap	85
c. Référencement dans fstab	85
a. Installation de la gestion RAID	86
b. Inventaire des disques installés	86
c. Création du disque RAID	87
a. Installation des outils de gestion des LVM	88
b. Création du volume logique	89
c. Création de filesystem	91
d. Montage du filesystem	92
a. Agrandissement du LV	94
b. Agrandissement du filesystem	96

Chapitre 3 Démarrage du système

A. Le processus init et les niveaux d'exécution	101
1. Les niveaux d'exécution	101
a. Qu'est-ce qu'un niveau d'exécution ?	101
b. Les niveaux d'exécution possibles	101
c. Qui décide de ce qu'on met dans les différents niveaux ?	102
2. Configuration du processus init	102
a. Le premier processus démarré sur le système	102
b. Le fichier inittab	103
c. Rappels sur le lancement des services	104
d. Liens entre les niveaux d'exécution et les services	105
e. Gestion des niveaux d'exécution	105
f. Commandes de gestions des liens de services	106
g. Script indépendant du niveau d'exécution : rc.local	107
3. Utilisation des niveaux d'exécution	108
B. Démarrage et chargement du noyau	108
1. Le gestionnaire de démarrage GRUB	108
a. Configuration de GRUB 1	109
b. Configuration de GRUB 2	110
c. Le fonctionnement de GRUB	111
2. Utilisation de GRUB 1 en mode interactif	111
a. Édition des sections déjà présentes	111
b. Chargement d'un noyau non listé	112
3. Réinstallation de GRUB	112
a. Réinstallation simple depuis un système actif	112
b. Réinstallation depuis un système non démarrable	113
4. Maintenance et mode single	114
a. Passage en mode single planifié	114
b. Ouverture d'un shell en cas d'échec au démarrage	114
C. Validation des acquis : questions/réponses	115

D. Travaux pratiques	117
a. Définition des besoins fonctionnels	117
b. Création de l'application spécifique	117
c. Modification du niveau personnalisé	119
d. Changement de niveau d'exécution à chaud	120
e. Suppression des liens	121
a. Création d'une machine de test	122
b. Copie des données du disque	122
c. Création de la machine virtuelle clone	125
d. Installation de GRUB	126
e. Démarrage et vérification	126

Chapitre 4 Gestion du réseau local

A. Configuration du réseau	129
1. Adressage IP	129
a. Adressage IPv4 et notation CIDR	129
b. Adressage IPv6	130
2. Configuration universelle du réseau	131
a. Détermination de l'interface réseau	131

b. Affectation de l'adresse IP : ifconfig	132
c. Configuration du client DNS : fichier /etc/resolv.conf	132
d. Configuration de la passerelle par défaut : route	133
e. Configuration du nom d'hôte : hostname	134
3. Spécificité des distributions	134
a. Configuration réseau dans /etc/network	134
b. Configuration réseau dans /etc/sysconfig/network-scripts	135
4. Autres commandes et fichiers de gestion du réseau	136
a. Gestion des adresses MAC avec arp	136
b. TCP Wrappers	137
5. Configuration Wi-Fi	138
a. Détermination de l'interface Wi-Fi	138
b. Visualisation des réseaux disponibles	139
c. Connexion à un réseau non sécurisé	140
B. Diagnostic réseau	140
1. Outils de diagnostics en couche réseau	140
a. Ping et ping6	140
b. Indicateurs de la commande route	141
c. traceroute	141
2. Outils de diagnostics en couches transport et application	142
a. netstat	142
b. nc	142
3. Diagnostics et informations en couche application	143
a. Isof	143
b. Journaux sur /var/log/syslog & /var/log/messages	143
4. Libpcap et les captures de paquets	144
a. La bibliothèque libpcap	144
b. tcpdump	144
c. Wireshark	145
C. Configuration automatique avec DHCP	147
1. Le protocole DHCP	147
a. Fonctionnement	147
b. Le service DHCP sur les systèmes Linux	148

2. Configuration du serveur	148
a. Le fonctionnement général du serveur	148
b. Les paramètres transmis aux clients	149
c. Déclaration de plages d'adresses	149
d. Paramètres spécifiques à une machine	150
e. Serveur à plusieurs interfaces	150
f. Visualisation des baux dhcp	150
3. Configuration du client	151
4. Agent relais DHCP	152
a. Principe du relais DHCP	152
b. Configuration de l'agent de relais	153
D. Validation des acquis : questions/réponses	153
E. Travaux pratiques	155
a. Configuration d'une adresse IP fixe pour le serveur alpha	155
b. Installation des paquetages applicatifs	157
c. Configuration du service	157
a. Configuration de la station de travail	158
b. Réservation d'une adresse IP pour une imprimante	159
c. Capture de paquets depuis la station de travail : échanges DHCP	159
 Chapitre 5 Authentification des utilisateurs	
A. Évolution de l'authentification	165
1. Les premiers systèmes Unix et le fichier passwd	165

a. Mots de passe dans le fichier /etc/passwd	165
b. Mots de passe dans le fichier /etc/shadow	165
2. D'autres bases d'informations	165
3. NSS	165
4. Modules d'authentification	166
B. PAM	167
1. Le principe	167
2. Les modules PAM	168
a. Les principaux modules PAM	168
b. Fonctionnement en piles de modules	169
3. Configuration de PAM	169
a. Structure des fichiers de configuration	169
b. Les types d'action de PAM	170
c. Les comportements des modules	171
C. LDAP	172
1. Généralités	172
a. Les annuaires	172
b. Structure et terminologie	173
c. Schéma	173
d. Le protocole LDAP	174
e. Désignation des objets	174
f. Authentification auprès d'un annuaire LDAP	175
g. Le format LDIF	175
2. Le serveur OpenLDAP	175
a. Gestion du service	176
b. Configuration	176
3. Les outils clients LDAP	177
a. Recherche d'informations avec ldapsearch	177
b. Ajout d'objets dans un annuaire avec ldapadd	179
c. Modification d'objet existant avec ldapmodify	180
d. Suppression d'objet avec ldapdelete	180
e. Modification de mot de passe avec ldappasswd	180
f. Allègement des syntaxes pour les utilitaires clients LDAP	181

g. Clients graphiques	182
D. Authentification par LDAP des systèmes Linux	183
1. Configuration NSS	183
a. Configuration de la bibliothèque NSS pour LDAP	183
b. Renseignement des sources de nom	183
c. Vérification des sources de noms	183
2. Configuration PAM	184
a. Identification des services nécessaires	184
b. Configuration des fichiers pam	184
E. Validation des acquis : questions/réponses	185
F. Travaux pratiques	187
a. Installation des paquetages applicatifs	187
b. Configuration de l'annuaire	187
c. Interrogation simple de l'annuaire	191
d. Création du contexte de base	192
e. Création de comptes utilisateur	192
f. Interrogation d'un annuaire peuplé	193
g. Interrogation de l'annuaire depuis un client	194
a. Installation des éléments applicatifs nécessaires à l'authentification LDAP	196
b. Configuration de la résolution de noms LDAP	196

c. Configuration de l'authentification pam avec LDAP	197
d. Validation fonctionnelle	198

Chapitre 6 Partage de fichiers

A. Partage de données avec NFS	201
1. Partage de répertoires	201
a. Observation des partages actifs	201
b. Partage ponctuel	202
c. Service NFS et partage permanent	202
d. Options de partage	203
2. Configuration des clients	203
a. Affichage des partages distants	203
b. Montage d'un répertoire distant	204
3. Gestion des identités	204
a. Les droits du client	204
b. Le cas particulier du superutilisateur	204
B. Partage de données avec SAMBA	204
1. Configuration générale	205
a. Les démons samba	205
b. Les fichiers de configuration	205
c. Configuration globale	206
2. Partage de répertoire	207
3. Gestion des identités	207
a. Algorithmes de hachage et stockage des mots de passe	207
b. Authentification auprès des serveurs Samba	208
c. Génération des mots de passe MD4	208
d. Synchronisation avec les mots de passe Linux	208
e. Suppression ou désactivation d'un compte samba	209
4. Le client Samba	209
a. Exploitation ponctuelle de ressources avec smbclient	209

b. Montage d'un partage smb avec smbmount.....	211
c. Montage d'un partage CIFS.....	211
C. Partage de fichiers avec FTP	212
1. Le protocole FTP.....	212
a. Historique.....	212
b. Paramètres techniques.....	212
c. Mode FTP actif et FTP passif.....	212
2. Les clients FTP.....	212
a. Les clients FTP graphiques.....	212
b. Le client FTP en lignes de commande.....	213
3. Le serveur Pure-FTPd.....	213
a. Fonctionnement pour accès des utilisateurs à leurs répertoires personnels.....	213
b. Fonctionnement en accès anonyme.....	213
c. Options de fonctionnement.....	214
4. Le serveur vsftpd.....	214
D. Validation des acquis : questions/réponses.....	215
E. Travaux pratiques.....	217
a. Installation des services applicatifs.....	217
b. Affichage de la configuration par défaut.....	217
c. Gestion des mots de passe.....	219
d. Accès des utilisateurs à leurs répertoires personnels depuis la station de travail.....	219
e. Création d'un partage commun.....	220
f. Accès des utilisateurs au nouveau partage.....	221

a. Installation des services applicatifs	221
b. Configuration du partage	221
c. Connexion depuis la station cliente	222
a. Installation du service applicatif	223
b. Configuration et lancement du service	223
c. Connexion depuis la station cliente Ubuntu	225

Chapitre 7 Résolution de noms DNS

A. Généralités	229
1. Les débuts de la résolution de noms et l'apparition du DNS	229
2. Concept de zones DNS	229
3. Mécanisme de la résolution de noms	230
4. Les enregistrements	232
a. Enregistrement de type A	232
b. Enregistrement de type AAAA	232
c. Enregistrement de type PTR	232
d. Enregistrement de type CNAME	233
e. Enregistrement de type MX	233
f. Enregistrement de type SOA	233
g. Enregistrement de type NS	233
5. DNS sur Linux	234
a. Le serveur DNS	234
b. Le client DNS	234
B. Configuration de base du serveur	234

1. Fonctionnement du serveur BIND	234
a. Structure du fichier named.conf et principaux éléments de configuration	234
b. Les fichiers de définition de zone pré-installés	235
2. Serveur de cache	236
a. Configuration du serveur de cache	236
b. Redirection	237
3. Commande de pilotage rndc	237
C. Gestion de zones DNS	238
1. Gestion de zones locales	238
a. Création d'un fichier de zone directe	238
b. Création d'un fichier de zone inverse	239
c. Création d'enregistrements dans les fichiers de zone	240
d. Déclaration de zone principale dans le fichier named.conf	240
e. Prise en compte de la nouvelle configuration	241
2. Gestion de zones secondaires	241
a. Déclaration de la zone secondaire dans named.conf	241
b. Prise en compte de la nouvelle configuration	242
3. Délégation de zone	242
4. Outils de test	243
a. ping	243
b. nslookup	243
c. dig	244
d. host	245
e. Mesure des performances	246
D. Sécurisation du DNS	247
1. Limitation des clients	247
2. Utilisation d'un compte de service	247
a. Pourquoi un compte de service ?	247
b. Lancement de named avec un compte de service	247
3. Bind en mode chroot	248
a. Pourquoi enfermer le processus ?	248
b. Création de l'environnement nécessaire	248
c. Lancement du programme en mode chroot	249

4. Échange sécurisé entre serveurs	249
a. Génération du secret partagé	249
b. Déclaration du secret dans named.conf	250
c. Les deux serveurs doivent utiliser la clé	251
d. Tout service est refusé en l'absence de signature	251
E. Validation des acquis : questions/réponses	252
F. Travaux pratiques	254
a. Installation des services applicatifs	254
b. Vérification	254
c. Configuration des clients	255
a. Vérification de la résolution des noms dans l'espace de noms public	256
b. Essais de mise en cache (facultatif)	256
c. Redirection	257
a. Création des fichiers de zones sur le serveur A	258
b. Déclaration des fichiers de zone	259
c. Création d'enregistrements	260
a. Utilisation de nslookup	261
b. Utilisation de dig	262

a. Configuration du serveur secondaire	263
b. Configuration du serveur primaire	265

Chapitre 8 Serveur web Apache

A. Configuration de base d'un serveur Apache	271
1. Apache et les serveurs web	271
2. Fichier de configuration	271
a. Format du fichier de configuration	271
b. Les directives de conteneur	272
c. Validation de la syntaxe	273
d. Démarrage et arrêt du serveur	273
3. Les modules Apache	273
a. Chargement des modules	273
b. Visualisation des modules	274
c. Choix des modules	275
4. Gestion des ressources	276
B. Hôtes virtuels	277
1. Configuration globale	277
a. Gestion des contenus	277
b. Organisation des sites virtuels	277
2. Configuration des hôtes virtuels	277
a. Hôtes virtuels sur adresse IP	278
b. Hôtes virtuels sur nom d'hôte	278
C. Restriction de l'accès utilisateur	279
1. Restriction de l'accès aux pages web	279
a. Déclaration du répertoire à protéger	279
b. Directives d'authentification	280
2. Authentification locale	280

a. Création d'une base de compte locale	280
b. Chargement des modules d'authentification	281
c. Configuration de l'authentification locale	281
3. Authentification par annuaire LDAP	282
a. Vérification de disponibilité des informations de l'annuaire	282
b. Chargement des modules nécessaires	283
c. Configuration de l'authentification	283
4. Authentification simple par fichier .htaccess	283
D. Configuration d'Apache avec SSL	285
1. Cryptographie et certificats	285
a. Concepts cryptographiques	285
b. Les certificats numériques X509	285
c. Génération locale d'un certificat	286
2. Configuration ssl	287
a. Chargement du module SSL	287
b. Configuration des clés de serveur	287
c. Gestion du fonctionnement SSL	288
d. Authentification des clients par certificat	288
E. Serveur proxy	288
1. Les serveurs proxy	288
a. Protection des clients	289
b. Serveurs de cache	289
c. Filtrages	289
d. Inconvénients	289
2. Le serveur proxy squid	289
a. Configuration de base	289
b. Gestion des accès clients	291
F. Validation des acquis : questions/réponses	293
G. Travaux pratiques	295

a. Gestion des noms DNS	295
b. Gestion des contenus	296
c. Génération d'un fichier de configuration simple	297
d. Adaptation pour gestion de sites virtuels	298
a. Génération des certificats	300
b. Configuration SSL	301
c. Gestion de l'authentification	302
a. Installation des binaires	303
b. Configuration de base	304
c. Déclaration et autorisation des acl	305
d. Validation fonctionnelle	306

Chapitre 9 Messagerie

A. Les MTA	309
1. Le protocole SMTP	309
2. Présentation de Sendmail	310
3. Présentation d'Exim	310
4. Présentation de Postfix	310

B. Le serveur SMTP Postfix	310
1. Configuration de Postfix	310
a. Gestion des identités	310
b. Gestion des alias	311
c. La commande postfix	311
d. Les fichiers de configuration	312
e. Vérification de la configuration active	313
2. Gestion de domaines virtuels	313
a. Définition des domaines virtuels	313
b. Gestion des identités pour les domaines virtuels	313
3. Gestion de quotas	314
C. Remise locale des messages	314
1. La commande mail	315
a. Envoi de courrier avec la commande mail	315
b. Lecture de courrier avec la commande mail	316
2. Formats mbox et maildir	317
a. Le format mbox	317
b. Le format maildir	317
c. Utilisation du format maildir par postfix	317
3. Procmal	318
a. Demander à postfix d'utiliser procmal	318
b. Configurer procmal	318
4. Alternatives à la messagerie	319
a. write et wall	319
b. issue et issue.net	319
c. motd	319
D. Remise distante des messages	320
1. Fonctionnement conjoint des MTA, MDA et des MUA	320
a. Le protocole POP3	320
b. Le protocole IMAP4	320
2. Serveurs Courier-IMAP et Courier-POP	320
a. Format de messages pour les services courrier	320

b. Configuration des services	320
c. Validation de l'authentification	321
3. Serveur Dovecot	321
a. Configuration de Dovecot	322
b. Visualisation de la configuration	322
E. Validation des acquis : questions/réponses	323
F. Travaux pratiques	325
a. Installation d'un serveur postfix sur le serveur alpha	325
b. Configuration du service	325
c. Gestion des alias postfix	326
d. Intégration DNS	327
e. Envoi et réception de mails en lignes de commande depuis le serveur alpha	328
f. Passage de postfix au format maildir	329
a. Installation d'un serveur Courier-IMAP sur le serveur alpha	330
b. Envoi d'un message à l'utilisateur toto	330
c. Gestion du courrier depuis le poste de travail	331
 Chapitre 10 Protection des réseaux	
A. Routage et filtrage	339

1. Configuration d'un serveur Linux en tant que routeur	339
a. Activation du routage sur un serveur Linux	339
b. Consultation de la table de routage	339
c. Gestion des routes statiques	340
2. Iptables	341
a. Les tables	341
b. Les chaînes	342
c. Les actions	342
d. Le traitement des règles	342
B. Administration d'un pare-feu avec les iptables	343
1. Politiques	343
a. Principe des politiques de pare-feu	343
b. Configuration d'une politique de base	344
2. Filtrage de paquets	344
a. Politique et règles	344
b. Création de règle	344
c. Gestion des règles	345
d. Gestion des flux retours	346
3. Gestion du NAT	347
a. Rappel sur le principe du NAT	347
b. Diagnostic de la configuration NAT d'un routeur	348
c. Connexion d'un réseau privé à un réseau public	348
4. Scripts de configuration des règles de filtrage	349
a. Red Hat et les iptables	349
b. Création de service personnalisé de pare-feu avec les iptables	349
C. Détection des intrusions et des vulnérabilités	350
1. Les systèmes IDS	350
a. Les limitations des pare-feu	350
b. Techniques d'analyse	350
c. Sources d'information	351
2. SNORT	351
a. Les composants	351
b. Gestion des sources d'information	352

c. Gestion des alertes	352
3. OpenVAS	352
a. Le serveur OpenVAS	352
b. Les clients OpenVAS	352
c. Récupération des vulnérabilités	353
D. Validation des acquis : questions/réponses	353
E. Travaux pratiques	355
a. Ajout d'une interface réseau sur le serveur beta	355
b. Adresses IP du serveur beta	357
c. Gestion du client en réseau privé	358
d. Gestion du serveur alpha en réseau privé	360
a. Configuration du NAT	361
b. Politique de filtrage sévère	363
c. Autorisation du trafic utile	364
d. Gestion sous forme de service	364
Chapitre 11 Sécurisation du trafic	
A. OpenSSH	369
1. Utilisations de OpenSSH	369
2. Gestion des authentifications	369
a. Authentification par mot de passe	369

b. Authentification par clés	370
c. L'agent SSH	371
3. Confidentialité des communications	372
a. Session interactive avec SSH	372
b. Copie de fichiers avec SSH	373
c. Utilisation d'applications dans des tunnels SSH	373
d. Renvoi de sessions X11 via SSH	374
B. OpenVPN	375
1. Les modes de fonctionnement OpenVPN	375
a. Authentification	375
b. Confidentialité	375
c. Fonctionnement réseau	375
2. Création d'un tunnel point-à-point	376
a. Gestion de l'authentification	376
b. Fichiers de configuration	376
c. Mise en œuvre du tunnel vpn	377
C. Validation des acquis : questions/réponses	378
D. Travaux pratiques	380
a. Repositionnement de la station de travail	380
b. Arrêt du pare-feu	381
c. Installation de l'intranet	382
a. Gestion de l'authentification	382
b. Création du tunnel	384
c. Validation	384

a. Installation des binaires	385
b. Gestion de l'authentification	386
c. Configuration du client	387
d. Configuration du serveur	387
e. Validation	388

Chapitre 12 Compilation des applications et du noyau Linux

A. Compilation des applications	393
1. Généralités	393
a. Principe de la compilation	393
b. Quand faut-il compiler ?	393
c. Rappels sur les utilitaires de décompression	393
2. Procédure de compilation GNU	394
a. Récupération des sources	394
b. Configuration de la compilation	394
c. Personnalisation des programmes compilés	395
d. Compilation	396
e. Les cibles de la commande make	397
f. Installation des binaires	397
g. Nettoyage des sources	397
h. Désinstallation d'un programme	398
3. Environnement des applications	398
a. Les bibliothèques	398
b. Visualisation des appels système	400
B. Compilation du noyau	401
1. Les composants du noyau	401

a. Le cœur de noyau	401
b. Les modules	401
c. Autour du noyau	403
d. Gestion des versions du noyau	403
2. Procédure de compilation et d'exploitation	404
a. Récupération des sources	404
b. Génération du fichier de réponse	404
c. Compilation du noyau et des modules	407
d. Installation des modules	407
e. Installation du noyau	408
f. Création du ramdisk des modules	408
g. Configuration du gestionnaire de démarrage	409
C. Patch du noyau	409
1. Ajout de patch	409
2. Retrait de patches	411
D. Validation des acquis : questions/réponses	411
E. Travaux pratiques	413
a. Téléchargement des sources	413
b. Compilation des sources	413
c. Installation des binaires	415
d. Nettoyage des sources	415
a. Récupération des sources	416
b. Suppression du module existant	416

c. Compilation des sources	417
d. Chargement du module de noyau et installation du module	418
a. Récupération des sources et du fichier de patch	419
b. Application du patch	419
c. Retrait du patch	420
a. Installation des outils nécessaires à la compilation	421
b. Téléchargement des sources d'un nouveau noyau	421
c. Configuration et compilation du noyau	422
d. Installation du nouveau noyau et de ses modules	423
e. Génération du ramdisk de démarrage	424
f. Configuration du gestionnaire de démarrage en GRUB 2	425
g. Configuration du gestionnaire de démarrage en GRUB 1 (option)	426