



# Travaux Pratiques Administration Système Linux

Année 2019-2020

Master I : Info et 3IR  
Version 3.1

Mamadou SOW, [mamadou.sow@lipn.univ-paris13.fr](mailto:mamadou.sow@lipn.univ-paris13.fr)  
Thomas RYBKA, [thomas.rybka@univ-paris13.fr](mailto:thomas.rybka@univ-paris13.fr)

## Sommaire

<b>1 TP1 : Virtualbox et Marionnet, logiciels</b>	<b>1</b>
<b>2 TP2 : DHCP et DNS, serveurs</b>	<b>6</b>
<b>3 TP3 : LDAP, serveur et clients</b>	<b>8</b>
<b>4 TP4 : NFS et WEB, serveurs</b>	<b>9</b>
<b>5 TP5 : Postfix, serveur de messagerie</b>	<b>10</b>
<b>6 TP6 : Sécurisation des machines</b>	<b>11</b>
<b>Bibliographie</b>	<b>11</b>
<b>Table des matières</b>	<b>12</b>

# TP1 : Virtualbox et Marionnet, logiciels

L'objectif de ce TP est :

1. de tester l'installation d'un système Linux à travers Virtualbox
2. de vous initier à l'utilisation du logiciel Marionnet
3. de mettre en place des procédures de sauvegarde de vos travaux
4. de réaliser des tâches courantes d'administration sur une machine locale
5. d'analyser un système Linux (mémoire, processus...)

## NB :

- Chaque séance de TP correspond un TP différent vous avez 15 jours pour terminer et rendre le compte-rendu du TP courant. Les Enseignants vous rendront les compte-rendus corrigés au fil du temps.
- Les Compte-Rendus seront corrigés et les notes seront prises en compte en fin d'année.
- Vous devez ouvrir un document Word (TP-numéro-nom\_prénom.doc) pour rédiger votre compte-rendu et insérer les captures d'écran qui justifieront votre travail avec des commentaires ou des réponses si cela est nécessaire.
- Le document en format .doc sera converti en TP-numéro-nom\_prénom.pdf et pour impression ou être envoyé aux Chargés de TP.
- Lisez bien la description du TP avant d'effectuer les opérations demandées. Vous trouverez le cours, les données et des exemples nécessaires à la réalisation du TP à l'adresse :  
<https://lipn.univ-paris13.fr/~sow/masterinfo/>

login	masterinfo
mot de passe	master2020info3ir

## 1.1 Installation d'un système Linux

Sur les machines de TP, le logiciel Virtualbox est installé et il se lance avec la commande **virtualbox &**. Vous êtes invité après prendre connaissance des paramètres de configuration de Virtualbox.

- Pour éviter d'avoir des problèmes d'espace disque sur le serveur NFS, vous pouvez installer votre machine virtuelle en local c'est-à-dire dans /tmp dans le poste du travail en faisant des modifications dans le lieu de stockage des machines, voici le cheminement Menu “/Ficher/Paramètres/Général/Dossier par défaut des machines”
- Les images d'installation sont en accès libre sur internet. L'image à utiliser est un **Debian 9** dont l'iso se trouve dans le dossier **/LOCAL/iso** de votre machine locale
- Avant de démarrer la machine virtuelle, il faut placer l'image iso dans le lecteur CD de la machine virtuelle en faisant des modifications dans le lecteur CD/DVD, voici le cheminement Menu “/Configuration/Stockage/Attributs/Lecteur CD/DVD/Choisissez un fichier de CD/DVD virtuel”
- Créer une machine virtuelle de type Linux Debian, avec 1Go de Ram, un disque dur de 10Go au format VDI, dynamiquement alloué
- Effectuez l'installation en mode texte (non graphique) et manuel en vérifiant chaque étape avec des partitions suivants : une racine / de 5Go, un swap de 2 Go et /personnel de 3Go
- Faites l'installation des logiciels
  - d'environnement d'un bureau Debian
  - du serveur d'impression
  - du serveur ssh
  - des utilitaires usuels du système
- Durant la phase d'installation vous pouvez passer à l'étape 2 du TP : Tutorial du logiciel Marionnet
- La fin de cette section est marquée par une capture d'écran d'un terminal et avec la page d'accueil de l'Institut Galilée dans le navigateur firefox
- Après avoir arrêté la machine virtuelle, vous pouvez créer une sauvegarde de votre machine Debian 9 en faisant une exportation en format OVA. Cette machine virtuelle peut être réutilisée ailleurs en faisant une simple importation

---

**Remarque :** Par défaut, le réseau est activé pour la machine virtuelle. N'hésitez pas à tester les autres fonctionnalités !

→ N'oubliez pas de faire de régulièrement des captures d'écran à insérer dans votre compte-rendu.

## 1.2 Tutoriel du logiciel Marionnet

Le logiciel Marionnet ([www.marionnet.org](http://www.marionnet.org)) offre la possibilité de simuler un réseau de machines Linux. Dans ce tutoriel, vous allez apprendre à utiliser le logiciel. Vous effectuerez différentes manipulations sur un réseau de test.

Lors du partiel, qui aura lieu sur machine, vous utiliserez le même logiciel.

**NB : Ces opérations sont importantes car elles vous permettront de construire votre réseau, le faire évoluer, sauvegarder son état à la fin du TP et le restaurer au TP suivant. Le document bash.pdf en ligne peut vous servir pour la suite du TP.**

### 1.2.1 Démarrage de Marionnet

Pour démarrer le logiciel depuis un terminal, tapez simplement : **marionnet &** (l'exécutable se trouve dans **/LOCAL/marionnet/bin/marionnet**).

Vous disposez ainsi d'une interface graphique vous permettant de configurer votre réseau et de lancer la simulation.

### 1.2.2 Définition et mise en place d'un réseau

Le menu Projet propose les actions standard : Nouveau/New (création d'un projet), Ouvrir (un projet existant), Enregistrer/Save (un projet), Enregistrer sous/Save as...

- Créer un nouveau projet dans le répertoire courant ou dans un répertoire de votre choix, avec un nom explicite (par exemple, TP1-nom-prenom)
- Créer trois machines en utilisant l'interface graphique. La distribution à utiliser s'appelle **debian-lenny-sid-21906** au lieu de **debian-lenny-sid-2008**. La distribution **debian-lenny-sid-21906** contient au préalable les fichiers de configuration à la fois des serveurs DHCP, DNS, LDAP, NFS, WEB et MAIL alors vous n'avez plus besoin de faire d'installation de paquets .deb avec les utilitaires (apt, apt-get, ...)
- Ajouter un switch (6 ports) et connecter les machines. Pourquoi un switch de 6 ports ? Parce que vous pouvez utiliser cette configuration pour réaliser l'ensemble des TPs les uns à la suite des autres
- Démarrer tous les éléments de votre réseau.

Le démarrage du réseau lance autant de terminaux que de machines virtuelles créées. Il est possible qu'un problème se produise au niveau de la lecture du système de fichiers.

Pour le régler, il suffit généralement d'arrêter et de démarrer à nouveau le réseau.

Vous vous connecterez en tant qu'utilisateur **root**. Si un mot de passe vous est demandé, il s'agit de '**root**'. Vous pouvez le modifier avec la commande **passwd**.

- Stoppez votre réseau en arrêtant proprement les machines (Tout arrêter). Vous pouvez également choisir de n'arrêter ou de ne redémarrer que certaines machines.

**Conseils :** N'hésitez pas à repartir les différents terminaux (correspondant aux machines virtuelles) sur plusieurs bureaux virtuels. Cela vous aidera à bien identifier sur quelle machine vous travaillez.

→ Réaliser des captures d'écran à insérer dans votre compte-rendu

### 1.2.3 Communication machine locale ↔ machine virtuelle

#### Espaces partagés

Il est possible d'échanger des fichiers entre machine virtuelle Marionnet et machine réelle. Chaque machine virtuelle dispose d'un dossier **/mnt/hostfs/** dont le contenu est visible sur la machine réelle dans un dossier type **/tmp/marionnet-XXXXX/nom\_projet/hostfs/Y/**, où X et Y sont des nombres.

## SSH via l'interface TAP (Point d'Accès de Test)

Sans configuration, une machine virtuelle peut être contactée par l'adresse 172.23.0.X (1< X <253). La machine locale prend l'adresse 172.23.0.254.

Il est alors possible de se connecter en SSH ou faire des transferts entre la machine locale et les machines virtuelles via scp.

- Faites des transferts de documents via la commande scp, par exemple à partir de la machine locale vers la machine virtuelle m1 :  
`scp /etc/hosts root@172.23.0.1:/root/`
  - Vérifier que le fichier /root/hosts existe bien sur la machine virtuelle.
  - Faites l'opération inverse : transfert d'un fichier sur la machine virtuelle vers votre dossier local. Votre mot de passe des salles de TP vous sera demandé.
- Réaliser des captures d'écran à insérer dans votre compte-rendu

## 1.3 Sauvegarde

Vous devez être capable d'effectuer deux types de sauvegarde :

- le projet en entier.
- les commandes de configuration de chaque machine virtuelle.
- les fichiers de configuration modifiés dans chaque machine virtuelle.

Cela doit être réalisé au minimum à la fin de chaque séance, pour éviter de refaire le même travail le TP suivant.

### 1.3.1 Sauvegarde du projet

Vous êtes invité à sauvegarder régulièrement votre projet via le menu “Projet→Enregistrer Sous” afin d'éviter de perdre totalement votre travail en cas de problème.

Les fichiers .mar contiennent l'ensemble des modifications du disque depuis le démarrage des machines. Ils peuvent être relativement gros. Pensez à éliminer les sauvegardes inutiles.

### 1.3.2 Sauvegarde des commandes de configuration

Vous pouvez sauvegarder les commandes de configuration de chaque machine virtuelle à l'aide du script SaveSystemFiles.sh disponible à l'adresse suivante :

<https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp1/SaveCommands.sh>

1. Télécharger le fichier dans le répertoire de connexion
2. Sur la machine réelle, ouvrir le script dans un éditeur de texte et modifier la valeur de la variable LOGIN en indiquant votre login dans les salles de TP.
3. Copier le script sur les machines virtuelles dans le répertoire à créer /root/bin (via scp par exemple).
4. Sur la machine virtuelle, placer les droits en exécution.
5. Sur la machine virtuelle, exécuter la commande suivante :  
`history > /root/history-'hostname'.txt`  
**ATTENTION** : il s'agit de quotes inversées (AltGr 7)
6. Sur la machine virtuelle, exécuter le script `SaveCommands.sh`.  
Un fichier /root/SystemSave-hostname.tar.gz (où hostname est le nom de la machine) est créé et transféré dans votre répertoire de connexion, sur la machine réelle.

A chaque sauvegarde, il vous suffit de répéter les opérations 5 et 6.

→ Réaliser des captures d'écran à insérer dans votre compte-rendu

### Sauvegarde « manuelle » des fichiers de configuration

Vous pouvez également sauvegarder les fichiers de configuration de chaque machine virtuelle.

On suppose ici, que les fichiers modifiés sont /etc/passwd et /etc/shadow

1. Sur la machine virtuelle : Réalisez une archive contenant les fichiers modifiés :  
`cd /`  
`tar czvf /root/TP1-machine1.tar.gz etc/passwd etc/shadow`

- 
2. sur la machine réelle : créez une répertoire (par machine) qui contiendra l'archive  
`mkdir $HOME/ADSYS/TP1/machine1`
  3. Sur la machine virtuelle : transférez les fichiers vers la machine réelle via scp :  
`scp /root/TP1-machine1.tar.gz 123456789@172.23.0.254:~/ADSYS/TP1/machine1`

### 1.3.3 Restauration du projet

La restauration d'un projet consiste à ouvrir le fichier depuis Marionnet (**Open** dans le menu **Projet**). Le réseau de machines virtuelles peut alors être démarré.

## 1.4 Administration locale du système

Dans cette partie, vous allez mettre en place les tâches locales d'administration d'un système, après avoir démarré correctement Marionnet.

Vous devrez également écrire des scripts Bash réalisant ces tâches.

Vous ne considérez ici l'administration que d'une seule machine virtuelle.

### 1.4.1 Crédation (massive) de comptes utilisateur

- Écrire un script shell Bash réalisant la création de comptes utilisateurs à partir d'informations stockées dans un fichier (nom, prénom, login, séparés par des espaces).  
Vous utiliserez les commandes `adduser` ou `useradd`.
- Tester le script avec le fichier :  
`https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp1>ListeUtilisateurs.txt`

→ Réaliser des captures d'écran et le script à insérer dans votre compte-rendu

### 1.4.2 Suppression d'utilisateurs

- Écrire un script qui supprime des utilisateurs à partir de leur login tout en créant une sauvegarde en format `.tar.bz2`
- Créer le fichier `ListeLogins.txt` avec la liste des 10 premiers login du fichier `ListeUtilisateurs.txt` avec la commande en dessous  
`cat ListeUtilisateurs.txt | awk 'print $3' | head -10 > ListeLogins.txt`
- Tester le script

→ Réaliser des captures d'écran et le script à insérer dans votre compte-rendu

### 1.4.3 Sauvegarde des fichiers utilisateurs

Vous allez mettre en place une sauvegarde régulière des données des utilisateurs (fichiers présents dans le répertoire de travail `/home/$login` et dans les boîtes aux lettres `/var/mail`) que vous venez de créer dans le répertoire `/var/tmp`.

- Écrire un script Bash effectuant cette sauvegarde. Naturellement, ce script doit s'adapter automatiquement à la liste des utilisateurs existants sur la machine.
- N'oubliez pas de créer un script de création des répertoires des boîtes aux lettres des utilisateurs existants sur la machine.
- Ajouter une entrée dans votre crontab pour que la sauvegarde s'effectue régulièrement.

→ Réaliser des captures d'écran et le script à insérer dans votre compte-rendu

### 1.4.4 Sauvegarde des fichiers système

Vous allez mettre en place une sauvegarde régulière des fichiers de configuration du système à l'aide d'un script et du cron.

- Écrire un script Bash qui identifie les fichiers de configuration modifiés depuis le démarrage de la machine.  
Vous indiquerez les fichiers et répertoires que vous avez choisi de sauvegarder.
- Ajouter une entrée dans votre crontab pour que la sauvegarde s'effectue régulièrement.

→ Réaliser des captures d'écran et le script à insérer dans votre compte-rendu

---

## 1.5 Analyse du système

En vous aidant de README-TP1.pdf en ligne, des supports de cours, de vos connaissances antérieures et vos recherches, identifiez les informations présentées en cours :

- Utilisation mémoire et disque
- Charge CPU
- Niveau de démarrage du système
- Services lancés au démarrage
- ...

Examinez les différents fichiers de log et le résultat de la commande dmesg.

→ Réaliser des captures d'écran à insérer dans votre compte-rendu

# TP2 : DHCP et DNS, serveurs

L'objectif de ce TP est de concevoir sur le logiciel Marionnet :

1. un réseau composé de quelques machines,
2. d'installer un serveur DHCP et un serveur DNS.
3. c'est-à-dire créer un fichier .mar exemple : votrenom-dhcp-dns.mar
4. assurez-vous que les serveurs DHCP, DNS sont correctement configurés.
5. sauvegarder les fichiers de configuration avec les scripts du TP1 à la fin de la séance

Lisez bien la description du TP avant d'effectuer les opérations demandée.

Vous trouverez le cours, les documents (plan\_adressage.pdf, README-TP2.pdf, DNS-HOWTO-fr.pdf, DHCP-HOWTO-fr.pdf, ...) et les données nécessaires à la réalisation du TP à l'adresse :

<https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp2>

## 2.1 Conception du réseau

Le réseau que vous allez installer et configurer sera composé de 6 machines (virtuelles) utiles pour les autres TPs. Avant de lancer le logiciel Marionnet, définissez certains paramètres de votre réseau :

- Les adresses IP affectées aux machines devront être choisies dans la plage d'adresses IP privées de la classe C

Classe	Préfixe	Plage IP	Nombre d'adresses
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255	$2^{32-8} = 16777216$
B	172.16.0.0/12	172.16.0.0 – 172.31.255.255	$2^{32-12} = 1048576$
C	192.168.0.0/16	192.168.0.0 – 192.168.255.255	$2^{32-16} = 65536$

- Nom du domaine (situé, par exemple, dans le domaine votrenom.nom-prenom.fr)
- Nom des machines avec l'adresse IP correspondante

Adresse IP	Nom de la machine hébergeant
	la passerelle :
	le serveur DHCP :
	le serveur DNS primaire (DNS1) :
	le serveur DNS secondaire (DNS2) :

Démarrez votre réseau et configurez les adresses de vos 3 serveurs.

### NB : Pourquoi un réseau local composé de 6 machines ?

1. Obtenir à la fin du module un réseau local avec l'ensemble des divers serveurs DHCP, DNS, LDAP, NFS, WEB, MAIL
2. Travailler avec une copie du fichier .mar du TP précédent ou en faisant une restauration de fichiers est un gain en temps

## 2.2 Mise en place d'un service DHCP

Vous allez installer un serveur DHCP sur votre serveur dédié. En vous aidant du cours et de la documentation fournie, vous modifierez le fichier `/etc/dhcp3/dhcpd.conf` du serveur de manière à l'adapter à votre réseau. Configurez les deux machines comme clientes DHCP, une dans une plage dynamique, l'autre statiquement.

→ Réaliser des captures d'écran et des tests à insérer dans votre compte-rendu

---

## 2.3 Mise en place du service DNS

Utilisez le cours et la documentation fournie pour mettre en place le service DNS :

- le serveur DNS1 est le serveur primaire de la zone
- le serveur DNS2 est le serveur secondaire

**NOTE :** Avant de configurer le secondaire, assurez-vous que le primaire fonctionne... Configurez les autres machines pour qu'elles interrogent ce serveur DNS pour effectuer les résolutions d'adresses.

**ATTENTION :** Les chemins et les commandes indiquées dans la documentation peuvent ne pas être les mêmes.

→ Réaliser des captures d'écran et des tests à insérer dans votre compte-rendu

## 2.4 Sauvegardes

Adaptez les sauvegardes faites au premier TP pour pouvoir restaurer rapidement vos configurations DNS et DHCP.

# TP3 : LDAP, serveur et clients

L'objectif de ce TP est d'installer un serveur et un client LDAP, vous pouvez

1. utiliser la copie du fichier .mar du TP2 (ldap-dhcp-dns.mar par exemple) pour réaliser le TP3 en ensuite modifier 2 machines pour être le serveur LDAP et la machine cliente LDAP
2. utiliser un switch de 6 ports, configurer une machine serveur de LDAP et une machine cliente sur laquelle viendront se connecter des utilisateurs
3. utiliser les fichiers de configuration des serveurs DHCP et DNS primaire du TP2 ou le résultat du TP2
4. restaurer les fichiers de configuration du TP2 avec les scripts du TP1 si cela est nécessaire
5. sauvegarder les fichiers de configuration avec les scripts du TP1 à la fin du TP
6. utiliser la distribution debian-lenny-21906 pour la création de vos machines
7. assurez-vous que les serveurs DHCP, DNS et LDAP sont correctement configurés.
8. utiliser le cours, le fichier README et les documents (HowToLdap,configuration-ldap-serveur,guide\_ldap\_installation\_dans-ldap) en lignes situées sur la page  
<https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp3> pour réaliser le TP.

## 3.1 Configuration et initialisation du service

Installer un serveur LDAP sur la machine dédiée en vous aidant du cours :

- le suffixe LDAP est nom-prenom.fr
- configurer les autorisations pour que l'utilisateur `cn=manager,dc=nom-prenom,dc=fr` soit administrateur
- créer un script permettant d'initialiser la base LDAP
- créer une branche people dans laquelle seront enregistrés tous vos utilisateurs
- créer un utilisateur dans l'annuaire qui pourra se connecter sur le serveur
- configurer le client LDAP (PAM) et tester l'authentification de l'utilisateur
- configurer ou transformer une seconde machine pour être client du serveur LDAP et n'oublier pas de faire un test

→ Réaliser des captures d'écran, des tests montrant le bon fonctionnement du système et du compte utilisateur, captures à insérer dans votre compte-rendu

## 3.2 Crédation (massive) de comptes utilisateur

- Écrire un script shell (Bash) générant un fichier LDIF permettant la création de comptes utilisateurs dans la base LDAP, à partir d'informations stockées dans un fichier (nom, prénom, login, séparés par des espaces).
- Tester le script avec le fichier  
<https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp3/ListeUtilisateurs.txt>
- Insérer les données du LDIF

→ Réaliser des captures d'écran du script, des tests de la création de comptes utilisateurs avec le script, des répertoires utilisateurs, de l'existence des comptes, captures à insérer dans votre compte-rendu

## 3.3 Suppression d'utilisateurs

- Écrire un script qui génère un fichier LDIF permettant la suppression des utilisateurs dans la base LDAP à partir de leur login
- Tester le script avec le fichier  
<https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp3/ListeLogins.txt>
- Supprimer les données du LDIF

→ Réaliser des captures d'écran du script, des tests montrant la suppression ces comptes et répertoires, captures à insérer dans votre compte-rendu

## TP4 : NFS et WEB, serveurs

L'objectif de ce TP est d'installer les serveurs NFS, WEB et les clients associés, vous pouvez

1. utiliser la copie du fichier .mar du TP 3 (nfs-web-ldap-dhcp-dns.mar par exemple) pour réaliser le TP4 modifier 2 machines pour être les serveurs NFS et WEB
2. utiliser les fichiers de configuration des serveurs DHCP, DNS primaire et LDAP du TP3 ou le résultat du TP3
3. restaurer les fichiers de configuration du TP3 avec les scripts du TP1 si cela est nécessaire
4. sauvegarder les fichiers de configuration avec les scripts du TP1 à la fin du TP
5. utiliser la distribution debian-lenny-21906 pour la création de vos machines
6. assurez-vous que les serveurs DHCP, DNS, LDAP, NFS et WEB sont correctement configurés.
7. utiliser le cours, le fichier README et les documents (exemple-web-ftp-mysql, plan-adressage, nfs-server-vitux, ...), <https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp4>

### 4.1 Mise en place de montage par NFS

- Configurer le serveur NFS hébergeant ces données afin qu'elle puisse les exporter via des montages NFS.
- Les données utilisateurs doivent très accessibles sur l'ensemble des stations de travail du réseau.  
→ Réaliser des captures d'écran et des tests avec une machine cliente à insérer dans votre compte-rendu

### 4.2 Mise en place d'un serveur Web

Vous allez configurer un serveur Web lancé en *standalone* parmi les machines.

- Implémenter une machine dans le réseau précédent destiné à héberger le serveur web
- En vous aidant du cours, modifier le fichier `/etc/apache2/apache2.conf` de manière à l'adapter à vos contraintes (nom du serveur, etc).
- Définir une zone dont l'accès sera restreint aux machines de votre réseau (intranet).
- Modifier le serveur DNS pour permettre un accès aisé au serveur web.  
→ Réaliser des captures d'écran et des tests à insérer dans votre compte-rendu

## TP5 : Postfix, serveur de messagerie

L'objectif de ce TP est d'installer un service de messagerie sous Postfix ainsi qu'un serveur d'envoi et de réception de courrier électronique, vous pouvez

1. utiliser la copie du fichier .mar du TP4 (mail-nfs-web-ldap-dhcp-dns.mar par exemple) pour réaliser TP5
2. utiliser les fichiers de configuration des serveurs DHCP, DNS primaire, LDAP, NFS et WEB du TP4 ou le résultat du TP4
3. restaurer les fichiers de configuration du TP4 avec les scripts du TP1 si cela est nécessaire
4. sauvegarder les fichiers de configuration avec les scripts du TP1 à la fin du TP
5. utiliser la distribution debian-lenny-21906 pour la création de vos machines
6. assurez-vous que les serveurs DHCP, DNS, LDAP, NFS, WEB et MAIL sont correctement configurés.

**NB :** En plus du cours, vous pouvez consulter les différentes HowTO disponibles sur le web,  
<https://lipn.univ-paris13.fr/~sow/masterinfo/tp/tp5>

### Mise en place du service de messagerie

- Configurer 3 machines : un serveur de mails, un serveur DNS et une station cliente
- Configurer le service réseau sur chaque machine
- Configurer Postfix sur le serveur de mails
- Créer un utilisateur et activer son compte
- Tester l'envoi et la réception des mails
- Modifier la station pour qu'elle utilise le service de messagerie
- Configurer le serveur DNS (exemple avec une zone votrenom.nom-prenom.fr)
- Tester l'envoi et la réception de mails dans la zone

→ Réaliser des captures d'écran et des tests à insérer dans votre compte-rendu

# TP6 : Sécurisation des machines

L'objectif de ce TP est :

1. est de sécuriser les machines de votre réseau
2. et des outils de sécurité réseau pour
3. identifier les failles de sécurité sur vos machines.
4. Vous utiliserez le logiciel Marionnet.

**NB :** en plus du cours, vous pouvez consulter les différentes HowTO disponibles sur le web  
A la fin du TP, n'oubliez pas de sauvegarder votre réseau. Vous pouvez aussi sauvegarder les fichiers de configuration des serveurs NFS et Web et des clients NFS à l'aide du script écrit dans le TP 1.

## 6.1 Sécurisation du réseau et des machines

Vous allez sécuriser vos machines en restreignant les possibilités d'y accéder. Il s'agit d'une part de restriction au niveau des machines autorisées mais aussi au niveau des services proposées.

Il s'agit de ne jamais laisser ouverts des accès à des services que vous n'utilisez pas. Pour la suite, vous définirez un réseau de 4 machines, dont l'une sera considérée comme un serveur SSH, les autres des clients.

Plusieurs aspects sont à prendre en compte lors de la sécurisation de votre réseau :

- Configuration et restriction des services Un certain nombre de services peuvent être disponibles sur les machines (ldap, dns, pop, etc.). Ces services peuvent être à l'origine d'intrusion sur votre machine. Il est préférable de les fermer si elles ne sont pas nécessaires.  
Sur Linux, ces serveurs sont généralement autonomes. Il suffit de ne pas lancer les programmes correspondant au démarrage (voir les fichiers dans /etc/init.d ou /etc/rc.d).  
Sur votre serveur, consultez et modifiez les liens dans les répertoires /etc/rcX.d, où X est le numéro du mode de démarrage afin de ne conserver que les services vraiment nécessaires.
- Utilisation du mécanisme de contrôle d'accès Le démon tcpd se charge de filtrer les machines autorisées à utiliser un service sur votre machine. Pour effectuer le filtrage, il lit le fichier /etc/hosts.allow qui contient les machines autorisées pour des services donnés, et le fichier /etc/hosts.deny qui contient les machines interdites de connexion pour des services donnés. Puis modifiez les fichiers /etc/hosts.deny et /etc/hosts.allow afin de n'autoriser que les connexions à partir des machines clientes de votre réseau.
- Vérifier sur votre serveur que le service de connexion sécurisé (ssh) est correctement installé.
- Installer un firewall sur votre serveur pour contrôler l'accès à votre serveur ssh. Dans votre réseau, placez les règles, ne laissez les connexions ouvertes que pour une machine spécifique.

→ Réaliser des captures d'écran et des tests à insérer dans votre compte-rendu

## 6.2 Utilisation d'outils d'audit de sécurité

Vous pouvez utiliser divers outils de sécurité pour identifier les failles de sécurité sur vos machines :

- tcpdump et traceroute pour visualiser le trafic sur votre réseau (écoute de paquets)
- john the ripper pour identifier les mots de passe faibles de vos utilisateurs. Après avoir redéfini le mot de passe d'un utilisateur, vous tenterez de le retrouver (vous définirez un mot de passe simple afin de limiter les temps de calcul).

→ Réaliser des captures d'écran et des tests à insérer dans votre compte-rendu

# Table des matières

<b>1 TP1 : Virtualbox et Marionnet, logiciels</b>	<b>1</b>
1.1 Installation d'un système Linux . . . . .	1
1.2 Tutoriel du logiciel Marionnet . . . . .	2
1.2.1 Démarrage de Marionnet . . . . .	2
1.2.2 Définition et mise en place d'un réseau . . . . .	2
1.2.3 Communication machine locale ↔ machine virtuelle . . . . .	2
Espaces partagés . . . . .	2
SSH via l'interface TAP (Point d'Accès de Test) . . . . .	3
1.3 Sauvegarde . . . . .	3
1.3.1 Sauvegarde du projet . . . . .	3
1.3.2 Sauvegarde des commandes de configuration . . . . .	3
Sauvegarde « manuelle » des fichiers de configuration . . . . .	3
1.3.3 Restauration du projet . . . . .	4
1.4 Administration locale du système . . . . .	4
1.4.1 Création (massive) de comptes utilisateur . . . . .	4
1.4.2 Suppression d'utilisateurs . . . . .	4
1.4.3 Sauvegarde des fichiers utilisateurs . . . . .	4
1.4.4 Sauvegarde des fichiers système . . . . .	4
1.5 Analyse du système . . . . .	5
<b>2 TP2 : DHCP et DNS, serveurs</b>	<b>6</b>
2.1 Conception du réseau . . . . .	6
2.2 Mise en place d'un service DHCP . . . . .	6
2.3 Mise en place du service DNS . . . . .	7
2.4 Sauvegardes . . . . .	7
<b>3 TP3 : LDAP, serveur et clients</b>	<b>8</b>
3.1 Configuration et initialisation du service . . . . .	8
3.2 Création (massive) de comptes utilisateur . . . . .	8
3.3 Suppression d'utilisateurs . . . . .	8
<b>4 TP4 : NFS et WEB, serveurs</b>	<b>9</b>
4.1 Mise en place de montage par NFS . . . . .	9
4.2 Mise en place d'un serveur Web . . . . .	9
<b>5 TP5 : Postfix, serveur de messagerie</b>	<b>10</b>
<b>6 TP6 : Sécurisation des machines</b>	<b>11</b>
6.1 Sécurisation du réseau et des machines . . . . .	11
6.2 Utilisation d'outils d'audit de sécurité . . . . .	11
<b>Bibliographie</b>	<b>11</b>
<b>Table des matières</b>	<b>12</b>