

# Laboratoire 1 - Linux

## 1 Durée prévue : 1h30

## 2 Introduction à Linux

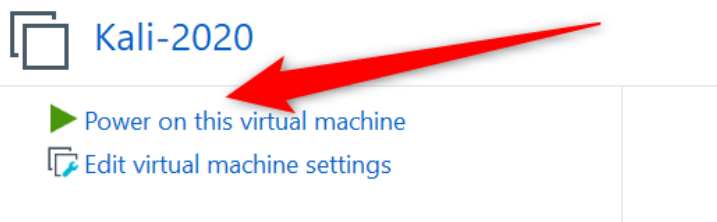
Linux est un système d'exploitation, au même titre que Windows ou encore Mac OS. Il y a des versions variées de Linux appelées **distributions**, pour répondre aux besoins des utilisateurs débutants ou avancés ainsi que des distributions hautement personnalisées pour des usages précis. Voir le fichier **Linux Distribution Timeline.svg** pour se faire une idée du panel des distributions.

Pour l'apprentissage des systèmes d'exploitation Linux, nous allons utiliser la distribution Kali Linux. Il s'agit d'une des meilleures distributions de **piratage éthique** que nous pouvons trouver à ce jour. Cette distribution, basée sur Debian, apporte tous les outils nécessaires pour permettre d'effectuer toutes sortes de tests en sécurité, offrant aux utilisateurs un environnement simple et sûr pour effectuer leurs tâches de « *pentesting* ». Bien que ces activités ne soient pas à l'ordre du jour de nos laboratoires, il nous semble nécessaire d'apprendre les bases sur une distribution que vous serez amenés à utiliser durant votre formation en sécurité des systèmes et espérons-le durant votre future carrière.

## 3 Exercice 1 – Démarrage et arrêt du système

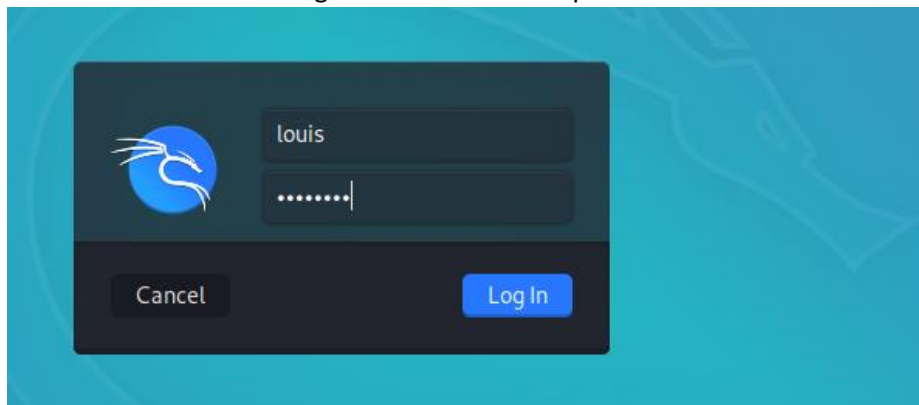
### 3.1 Démarrer et arrêter proprement sa machine

1. Sous VMware, démarrez la machine virtuelle si ce n'est déjà fait



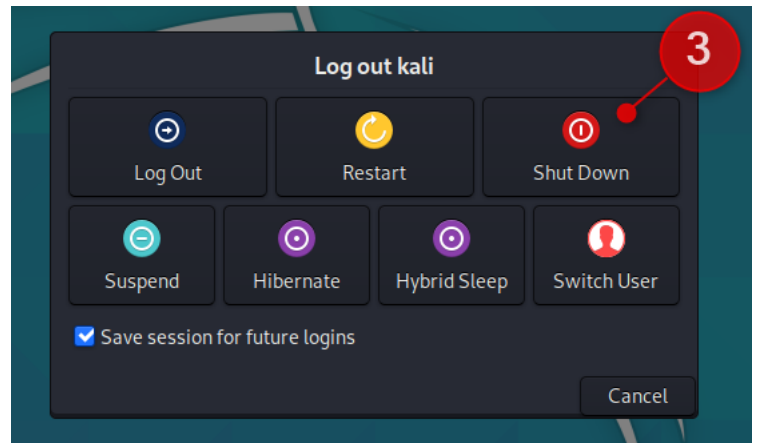
Attention, sous VMware n'arrêtez JAMAIS votre machine virtuelle sans réaliser un arrêt du système d'exploitation, sous peine de corrompre votre système, voire de ne plus pouvoir le démarrer !

2. Connectez-vous avec le login **louis** et le mot de passe **toorroot**



3. Pour stopper proprement votre machine virtuelle en fin de session.

- I. Cliquez sur le menu applications
- II. Cliquez sur le bouton **logout...**
- III. Et cliquez sur **Shutdown** pour un arrêt complet.



## 4 Exercice 2 - Trouver de l'aide

Sous Linux, il existe une très grande quantité de commandes. Il est donc impossible de connaître l'ensemble de celles-ci, ni de connaître leurs nombreux paramètres et possibilités. Toutefois, il faut connaître les commandes de base. Pour cela nous avons les pages de manuel accessible en ligne ou sur accessible directement sur le système.

4. Passons en ligne de commande pour la suite du labo. Ouvrez un terminal virtuel !



Pour ceux qui sont habitués à l'interface graphique, utiliser la ligne de commande peut constituer un problème : celui d'interagir avec l'ordinateur en utilisant de simples commandes textuelles. Les commandes présentées ici sont spécifiques à Linux et se comportent en général de manière similaire, quelle que soit la distribution.

5. Exécutez maintenant la commande `man ls`

La commande **man** est une interface de consultation des manuels de référence du système.

```

LS(1) User Commands LS(1)
NAME
  ls - list directory contents
SYNOPSIS
  ls [OPTION]... [FILE]...
DESCRIPTION
  List information about the FILES (the current directory by default). Sort entries alphabetically if none of -cftuvSUX
  nor --sort is specified.
  Mandatory arguments to long options are mandatory for short options too.
  -a, --all
    do not ignore entries starting with .
  -A, --almost-all
    do not list implied . and ..
  --author
    with -l, print the author of each file
  -b, --escape
    print C-style escapes for nongraphic characters
Manual page ls(1) line 1 (press h for help or q to quit)

```

Chaque page de manuel fait partie d'une section, d'une catégorie de manuels si vous préférez.

Sections	Types de sujets
<b>1</b>	Commandes utilisateur
<b>2</b>	Appels système
<b>3</b>	Fonctions de bibliothèque
<b>4</b>	Fichiers spéciaux
<b>5</b>	Formats de fichier
<b>6</b>	Jeux
<b>7</b>	Divers
<b>8</b>	Administration système

Chaque section possède une page d'introduction qui présente la section, disponible en tapant `man <section> intro`.

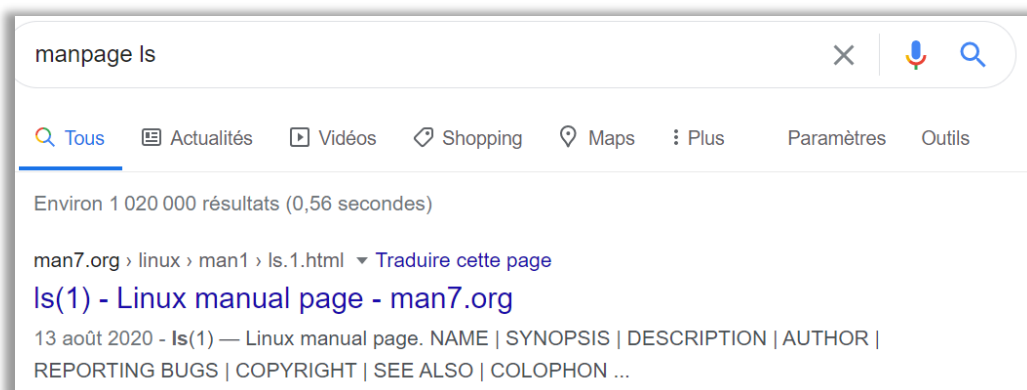
6. Pour apprendre comment naviguer dans les manpages, appuyez sur la touche h pour afficher une aide contextuelle.

Les commandes les plus utilisées sont :

- H → afficher l'aide contextuelle (q pour quitter l'aide)
- g → retour à la première ligne
- G → saut à la dernière ligne
- Barre d'espace → saut d'une page
- b → retour d'une page
- /texte → recherche texte dans le man page (/ pour continuer la recherche)
- q → pour quitter la manpage

7. Essayez de naviguer dans la manpage de la commande **ls** et essayez de trouver le paramètre de la commande **ls** pour obtenir un long listing (indice **/long listing**)

8. Recherchez sur internet dans votre moteur de recherche préféré « **manpage ls** » et cliquez sur le premier lien **man7.org**



Vous constatez que les manuels des commandes linux sont accessibles en ligne sur le web.

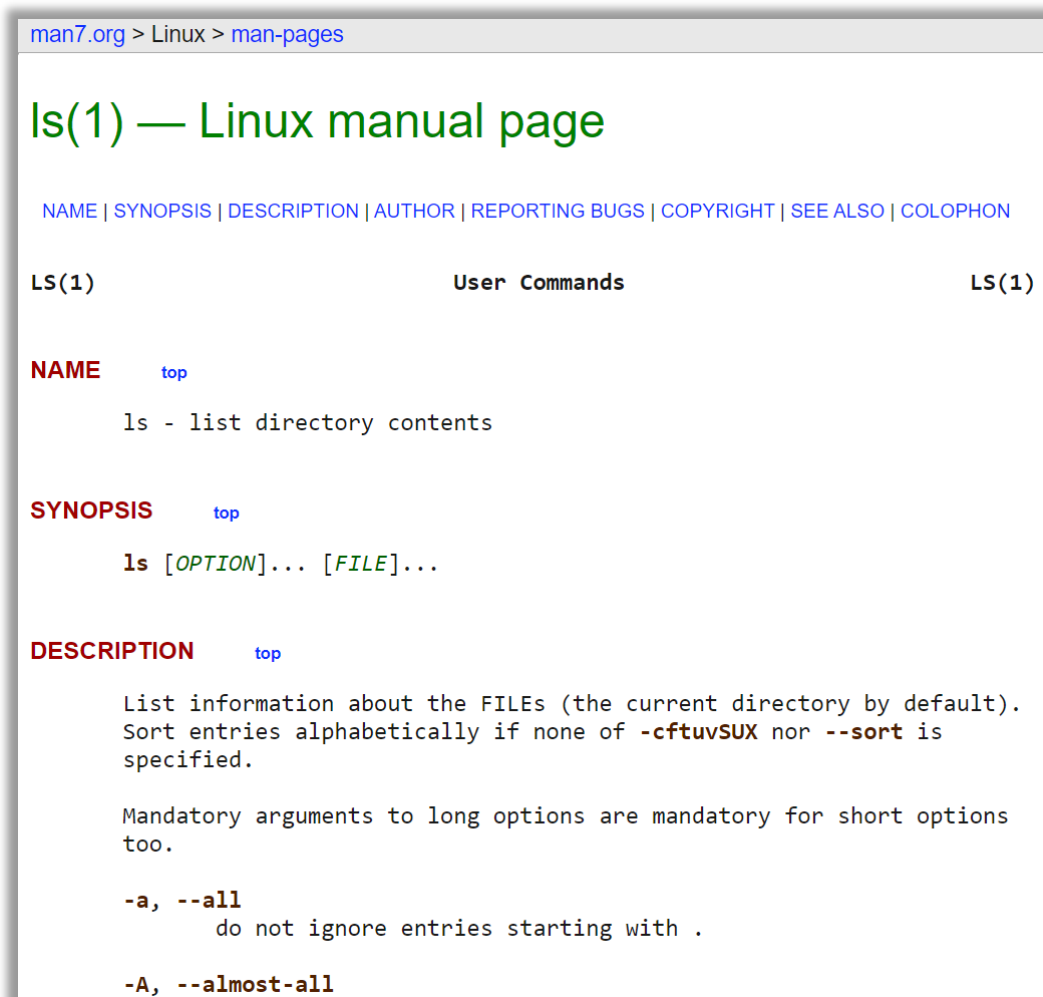


Figure 1 – Page de manuel en ligne de la commande ls

Maintenant que vous pouvez trouver de l'aide sur les commandes Linux, nous pouvons commencer à administrer le système Linux.

## 5 Exercice 3 - Gestion des logins

Vous êtes actuellement connecté sur la session de l'utilisateur **louis**.

- Pour pouvoir gérer les comptes d'un système Linux, il faut passer en mode **super admin**, c'est-à-dire utiliser le compte **root**. Exécuter la commande **sudo su -**, et entrez à nouveau le mot de passe de l'utilisateur **louis**. Le dernier caractère du prompt devrait avoir changé de \$ il est passé à #.

```
louis@kali-2020:~$ sudo su -  
[sudo] password for louis:  
root@kali-2020:~#
```

**Vous êtes maintenant en session root ou super utilisateur. Il faut être très prudent, vous disposez de tous les droits sur le système Linux.**

## 5.1 Enoncé des tâches à réaliser sur le système :

Au moyen de **la ligne de commande** :

- A. Créez deux groupes locaux **student** et **whitehat**.
- B. Créez un utilisateur local correspondant à votre login HELMo et placez-le dans le groupe principal **student**. Précisez également vos informations (nom, prénom, ...) et fixez le mot de passe.
- C. Créez un compte hacker dans le groupe principal **student** et dans le groupe secondaire **whitehat** et fixez-lui un mot de passe.
- D. Modifiez (usermod) votre compte pour qu'il appartienne également au groupe secondaire **whitehat** et **sudo**. (**Très important pour la suite du laboratoire**)
- E. Vérifiez avec les commandes et en consultant les fichiers adéquats que tout est correct.
- F. À partir de maintenant, connectez-vous avec votre nouveau login !

Voyons les quelques commandes de gestion des utilisateurs et groupes sur Linux afin de réaliser l'exercice.

Sous Linux (comme sous beaucoup d'autres Unix), les droits sont gérés au travers d'utilisateurs et de groupes. Chaque utilisateur appartient à un ou plusieurs groupe(s). S'il appartient à plusieurs groupes l'un d'entre eux sera son **groupe principal**.

## 5.2 Les commandes pour gérer les utilisateurs sont :

### useradd

Cette commande permet d'ajouter un utilisateur sur le système. Par défaut, cette commande crée un groupe du nom de l'utilisateur et intègre l'utilisateur dans ce groupe principal. Comme ce comportement n'est pas souhaité, il convient de préciser les arguments suivants :

Exemple :

```
$ useradd -g student superswila
```

Cette commande ajoute l'utilisateur (dont le login est superswila) dans la liste des utilisateurs locaux du système. Cet utilisateur est placé dans le groupe principal users. Par défaut, le système lui attribue le shell bash et détermine le chemin vers le dossier personnel dans /home/superswila. Consulter la page de manuel pour plus d'information<sup>5</sup>.

Le compte de l'utilisateur est désactivé tant qu'aucun mot de passe n'est précisé.

### usermod

Cette commande permet de modifier les paramètres d'un utilisateur local déjà créé (par exemple, l'ajouter dans un groupe secondaire, ...). Consulter la page de manuel pour plus d'information<sup>5</sup>.

### userdel

Cette commande permet de supprimer un utilisateur local existant. Sans option particulière, le dossier personnel de l'utilisateur est conservé. Consulter la page de manuel pour plus d'information<sup>5</sup>.

## chfn

Cette commande permet de changer le nom de l'utilisateur, préciser son bureau, et toutes les informations utilisateurs qui lui sont attachées. Consulter la page de manuel pour plus d'information5.

## passwd

Sans paramètre, cette commande permet de changer le mot de passe de l'utilisateur courant. L'administrateur peut préciser le login d'un utilisateur pour changer ou fixer le mot de passe de celui-ci. Quand le mot de passe est mentionné pour la 1ère fois, le compte est automatiquement activé.

## id

Sans paramètre, cette commande permet de connaître le nom d'utilisateur courant. Il précise également les groupes (principaux et secondaires) de cet utilisateur. Il est possible de préciser le login d'un utilisateur, la commande retourne alors les informations de cet utilisateur.

## chsh

Cette commande permet de changer le shell d'un utilisateur.

Le fichier **/etc/passwd** est un fichier texte de configuration essentiel sous Linux. Il contient la liste des utilisateurs du système ainsi que les informations sur chacun d'entre eux. Chaque ligne de ce fichier renseigne les informations d'un utilisateur :

```
louis:x:1000:1000:Louis SWINNEN,,,:/home/louis:/bin/bash
```

Champs	Significations
1	username
2	mot de passe
3	UID
4	GID
5	Information
6	Dossier personnel
7	Shell

### 5.3 Les commandes pour gérer les groupes sont :

#### groupadd

Cette commande permet d'ajouter un groupe sur le système. Consulter la page de manuel pour plus d'information.

#### groupmod

Cette commande permet de modifier un groupe déjà existant. Consulter la page de manuel pour plus d'information.

#### groupdel

Cette commande permet de supprimer un groupe existant. Consulter la page de manuel pour plus d'information.

#### groups

Cette commande permet de connaître les groupes auxquels l'utilisateur appartient. Consulter la page de manuel pour plus d'information.

Le fichier **/etc/group** contient la liste des groupes du système ainsi que les informations sur chacun d'entre eux et leur membres. Chaque ligne renseigne les informations d'un groupe :

```
sudo:x:27:louis
```

Champs		Significations
1	groupename	Nom du groupe
2	mot de passe	Le mot de passe du groupe n'est plus précisé dans ce fichier mais dans le fichier <b>/etc/gshadow</b> sous un format haché. C'est pourquoi celui-ci est remplacé par <b>x</b> .
3	GID	L'identifiant numérique du groupe principal de l'utilisateur. Précisons que le groupe <b>root</b> a le GID 0.
4	liste des utilisateurs séparés par « , »	Précise les utilisateurs ayant comme groupe secondaire le groupe en question. Ainsi, si l'utilisateur <b>louis</b> a comme groupe principal le groupe <b>louis</b> et comme groupe secondaire <b>sudo</b> , nous aurons : l'identifiant 1000 précisé comme GID dans le fichier <b>passwd</b> pour cet utilisateur et, dans les membres du groupe <b>sudo</b> , le login <b>louis</b> apparaîtra. Par contre, il n'apparaîtra pas pour le groupe <b>louis</b> (ce n'est pas un groupe secondaire).




Pour visualiser le contenu d'un fichier, utilisez la commande **less [options] <fichier>**  
 Pour naviguer dans le document, appuyez sur la **barre d'espace** pour descendre à la page suivante, la touche **b** pour remonter, la touche **q** pour quitter et **/« texte recherché »** pour effectuer une recherche dans le fichier.

10. Utilisez la commande **less** pour visualiser les fichiers suivants :

- a. /etc/passwd
- b. /etc/group
- c. /etc/shadow
- d. /etc/gshadow

### **Conseil général**

Rédigez une synthèse des commandes utilisées pour répondre aux exercices ou annotez et surlignez votre propre fichier PDF via Acrobat Reader  afin de pouvoir étudier les bonnes réponses pour l'examen.