



**Université Mohammed Premier  
Faculté des Sciences d'Oujda  
Département Informatique**



***Master M2I – M2***

***TP 2 : Sécurité sous Linux***

---

**Présenté par :**

**Mahroug Rachid**

**Encadré par :**

**Prof : Ouerdi Noura**

---

Introduction .....	3
Exercice 1 : Commandes de base pour la sécurité et l'audit du système .....	4
1. la description des commandes demandées et leurs fonctionnalités : .....	4
1.1 cat /etc/issue .....	4
1.2 uname -a .....	4
1.3 ps aux   grep ssh .....	4
1.4 Commandes top et htop .....	5
1.5 chkrootkit .....	5
1.6 rkhunter --check .....	6
1.7 sudo lynis audit system .....	7
2. Explication des résultats des commandes suivantes : .....	8
2.1 netstat -anpe   more : .....	8
2.2 sudo netstat -tuln .....	9
2.3 echo "TMOUT=20" >> ~/.bashrc (root) .....	10
2.4 ssh -l votreCompte localhost (on suppose que SSH est installé) : .....	10
Exercice 2 : Gestion des utilisateurs et des connexions .....	11
1. grep stagiaire /etc/shadow .....	11
2. Connexion en tant qu'administrateur et exécution de la commande .....	11
3. Changer la période de validité du mot de passe de stagiaire à 30 jours : .....	11
4. Changer le mot de passe de l'utilisateur à « stagiaire2 », tester la connexion, puis le remettre à « stagiaire » .....	12
5. Verrouiller et déverrouiller le mot de passe de l'utilisateur .....	12
5.1 sudo passwd -l stagiaire (Verrouiller le mot de passe) .....	12
5.2 sudo passwd -S stagiaire (Voir l'état du mot de passe ) .....	12
5.3 sudo passwd -u stagiaire (Déverrouiller le mot de passe) .....	13
6. Visualiser les dernières connexions réussies et échouées : .....	13
7. Lister les services actifs avec les fichiers associés .....	13
8. Désactiver les services inutiles : .....	14
9. Configurer une tâche cron : .....	14
Conclusion .....	16

---

## Introduction

Ce TP sur la **sécurité sous Linux** a pour objectif de familiariser les utilisateurs avec les outils et commandes essentiels à la gestion des utilisateurs, des droits et des services, ainsi qu'aux bonnes pratiques de sécurité. Dans un environnement multi-utilisateur comme Linux, il est crucial de contrôler les accès, de surveiller les activités, et d'automatiser certaines tâches afin de garantir l'intégrité du système.

À travers différents exercices, ce TP aborde les commandes fondamentales pour :

- Gérer les utilisateurs et leurs droits, comme la création de comptes, la gestion des mots de passe, et l'attribution de privilèges.
- Analyser les processus et services actifs à l'aide d'outils tels que ps, lsof, chkrootkit, et lynis, dans le but de détecter d'éventuelles failles de sécurité.
- Automatiser certaines actions via **cron**, permettant la gestion automatique des tâches système, telles que la réinitialisation des mots de passe.

Ce travail pratique vise à sensibiliser les administrateurs système et les utilisateurs avancés aux enjeux de la sécurité sur un système Linux, tout en fournissant des compétences pour identifier, prévenir et corriger les vulnérabilités.

---

## Exercice 1 : Commandes de base pour la sécurité et l'audit du système

### 1. la description des commandes demandées et leurs fonctionnalités :

#### 1.1 cat /etc/issue

- Cette commande affiche les informations sur la distribution Linux installée sur le système.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# cat /etc/issue
Kali GNU/Linux Rolling \n \l
```

#### 1.2 uname -a

- Affiche des informations détaillées sur le noyau Linux utilisé (version du noyau, architecture, nom de la machine, etc.).

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# uname -a
Linux DESKTOP-VH0G7EG 5.15.153.1-microsoft-standard-WSL2 #1 SMP Fri Mar 29 2
3:14:13 UTC 2024 x86_64 GNU/Linux
```

#### 1.3 ps aux | grep ssh

- Affiche la liste des processus en cours d'exécution, avec des informations sur le processus SSH. Cela permet de vérifier si le service SSH fonctionne.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2616   1748 hvc0    SL+   01:00    0:00 /init
root         5  0.0  0.0   2616   1100 hvc0    SL+   01:00    0:00 plan9 --con
root         8  0.0  0.0   2620    120 ?        Ss    01:00    0:00 /init
root         9  0.0  0.0   2620    124 ?        S     01:00    0:00 /init
kali        10  0.0  0.0   7320   4164 pts/0    Ss    01:00    0:00 -bash
root       521  0.0  0.0  17392   6548 pts/0    S+    01:12    0:00 sudo su
root       522  0.0  0.0  17392   1008 pts/1    Ss    01:12    0:00 sudo su
root       523  0.0  0.0   8768   3740 pts/1    S     01:12    0:00 su
root       524  0.0  0.0   7308   4056 pts/1    S     01:12    0:00 bash
root       540  0.0  0.0   8132   3524 pts/1    R+    01:25    0:00 ps aux

(root@DESKTOP-VH0G7EG)-[/home/kali]
# ps aux | grep ssh

(root@DESKTOP-VH0G7EG)-[/home/kali]
#
```

## 1.4 Commandes top et htop

- top : Affiche une vue en temps réel des processus en cours, triés par l'utilisation de la CPU. Permet de surveiller les performances du système.

```
top - 01:29:29 up 33 min, 0 user, load average: 0.00, 0.00, 0.00
Tasks: 10 total, 1 running, 9 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.1 sy, 0.0 ni, 99.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.
MiB Mem : 7748.0 total, 7314.6 free, 507.8 used, 109.5 buff/cache
MiB Swap: 2048.0 total, 2048.0 free, 0.0 used. 7240.2 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+
543 root        20   0   9164  4824 2740 R   0.3   0.1   0:00.02
  1 root        20   0   2616  1748 1636 S   0.0   0.0   0:00.01
  5 root        20   0   2616  1100 1060 S   0.0   0.0   0:00.00
  8 root        20   0   2620   120    0 S   0.0   0.0   0:00.00
  9 root        20   0   2620   124    0 S   0.0   0.0   0:00.47
 10 kali        20   0   7320  4164 3444 S   0.0   0.1   0:00.04
521 root        20   0  17392  6548 5584 S   0.0   0.1   0:00.37
522 root        20   0  17392  1008    0 S   0.0   0.0   0:00.00
523 root        20   0   8768  3740 3332 S   0.0   0.0   0:00.00
524 root        20   0   7308  4056 3344 S   0.0   0.1   0:00.03
```

- htop : Similaire à top, mais avec une interface interactive et plus conviviale pour surveiller l'utilisation des ressources système.

```
0[          0.0%] 4[          0.0%]
1[          0.0%] 5[          0.0%]
2[|         0.7%] 6[          0.0%]
3[          0.0%] 7[          0.0%]
Mem[|||||    324M/7.57G] Tasks: 10, 2 thr, 0 kthr; 1 running
Swp[          0K/2.00G] Load average: 0.00 0.00 0.00
                        Uptime: 00:51:52

Main I/O
PID USER      PRI  NI  VIRT  RES  SHR S CPU% MEM%   TIME+  Command
1 root        20   0   2616  1748 1636 S  0.0  0.0   0:00.01 /init
5 root        20   0   2616  1100 1060 S  0.0  0.0   0:00.00 plan9 --con
6 root        20   0   2616  1100 1060 S  0.0  0.0   0:00.00 plan9 --con
7 root        20   0   2616  1748 1636 S  0.0  0.0   0:00.00 /init
8 root        20   0   2620   120    0 S  0.0  0.0   0:00.00 /init
9 root        20   0   2620   124    0 S  0.0  0.0   0:00.51 /init
10 kali       20   0   7320  4164 3444 S  0.0  0.1   0:00.04 -bash
521 root       20   0  17392  6548 5584 S  0.0  0.1   0:00.46 sudo su
522 root       20   0  17392  1008    0 S  0.0  0.0   0:00.00 sudo su
523 root       20   0   8768  3740 3332 S  0.0  0.0   0:00.00 su
524 root       20   0   7308  4056 3344 S  0.0  0.1   0:00.02 bash
544 root       20   0   5288  3812 3032 R  0.0  0.0   0:00.03 htop
```

## 1.5 chkrootkit

- Un outil permettant de détecter des rootkits sur le système.

```

Searching for Kinsing.a backdoor rootkit...      not found
Searching for RotaJakiro backdoor rootkit...    not found
Searching for Syslogk LKM rootkit...            not found
Searching for Kovid LKM rootkit...              not tested
Searching for Tsunami DDoS Malware rootkit...  not found
Searching for Linux BPF Door...                 not found
Searching for suspect PHP files...              not found
Searching for zero-size shell history files...  not found
Searching for hardlinked shell history files... not found
Checking 'aliens'...                            finished
Checking 'asp'...                               not infected
Checking 'bindshell'...                         not found
Checking 'lkm'...                               started
Searching for Adore LKM...                      not tested
Searching for sebek LKM (Adore based)...        not tested
Searching for knark LKM rootkit...              not found
Searching for for hidden processes with chkproc... not found
Searching for for hidden directories using chkdirs... not found
Checking 'lkm'...                               finished
Checking 'rexedcs'...                           not found
Checking 'sniffer'...                           WARNING

WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
lo: not promisc and no packet sniffer sockets
eth0: not promisc and no packet sniffer sockets

Checking 'w55808'...                            not found
Checking 'wted'...                              not found
Checking 'scalper'...                           not found
Checking 'slapper'...                           not found
Checking 'z2'...                                not found
Checking 'chkutmp'...                            WARNING

WARNING: chkutmp output:
failed opening utmp !

Checking 'OSX_RSPLUG'...                         not tested

(root@DESKTOP-VH0G7EG)-[/home/kali]
#

```

## 1.6 rkhunter --check

- Un autre outil qui scanne le système à la recherche de rootkits, backdoors, et exploits.

```
Mokes backdoor [ Not found ]
Mood-MT Rootkit [ Not found ]
MRK Rootkit [ Not found ]
Ni0 Rootkit [ Not found ]
Ohhara Rootkit [ Not found ]
Optic Kit (Tux) Worm [ Not found ]
Oz Rootkit [ Not found ]
Phalanx Rootkit [ Not found ]
Phalanx2 Rootkit [ Not found ]
Phalanx2 Rootkit (extended tests) [ Not found ]
Portacelo Rootkit [ Not found ]
R3dstorm Toolkit [ Not found ]
RH-Sharpe's Rootkit [ Not found ]
RSA's Rootkit [ Not found ]
Scalper Worm [ Not found ]
Sebek LKM [ Not found ]
Shutdown Rootkit [ Not found ]
SHV4 Rootkit [ Not found ]
SHV5 Rootkit [ Not found ]
Sin Rootkit [ Not found ]
Slapper Worm [ Not found ]
Sneakin Rootkit [ Not found ]
'Spanish' Rootkit [ Not found ]
Suckit Rootkit [ Not found ]
Superkit Rootkit [ Not found ]
TBD (Telnet BackDoor) [ Not found ]
TeLeKiT Rootkit [ Not found ]
T0rn Rootkit [ Not found ]
trNkit Rootkit [ Not found ]
Trojanit Kit [ Not found ]
Tuxtendo Rootkit [ Not found ]
URK Rootkit [ Not found ]
Vampire Rootkit [ Not found ]
VcKit Rootkit [ Not found ]
Volc Rootkit [ Not found ]
Xzibit Rootkit [ Not found ]
zaRwT.KiT Rootkit [ Not found ]
ZK Rootkit [ Not found ]

[Press <ENTER> to continue]
```

### 1.7 sudo lynis audit system

- Lynis est un outil de sécurité pour auditer un système Linux, fournissant une analyse complète des vulnérabilités et des faiblesses potentielles.

```
- Firewall [V]
- Malware scanner [V]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====
====

Exceptions found
Some exceptional events or information was found!

What to do:
You can help by providing your log file (/var/log/lynis.log).
Go to https://cisofy.com/contact/ and send your file to the e-mail address
listed

=====
====

Lynis 3.1.1

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====
====

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /et
```

## 2. Explication des résultats des commandes suivantes :

### 2.1 netstat -anpe | more :

- Cette commande affiche toutes les connexions réseau actives, les ports ouverts et leur état (en écoute, établis, etc.), avec des informations supplémentaires comme le programme lié (option -p), les adresses réseau et les utilisateurs associés (-e). L'option | more permet de paginer la sortie pour en faciliter la lecture.



```

(root@DESKTOP-VH0G7EG)-[/home/kali]
# netstat -anpe | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
User      Inode   PID/Program name
tcp        0      0 10.255.255.254:53      0.0.0.0:*              LISTEN
0          20492   -
udp        0      0 10.255.255.254:53      0.0.0.0:*
0          20491   -
udp        0      0 127.0.0.1:323          0.0.0.0:*
0          18529   -
udp6       0      0 :::1:323               :::*
0          18530   -

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags               Type               State              I-Node   PID/Program name
Path
unix    2      [ ACC ]                STREAM             LISTENING          18311    1/init
/run/WSL/1_interop
unix    2      [ ACC ]                STREAM             LISTENING          21599    -
/run/WSL/1_interop
unix    2      [ ACC ]                STREAM             LISTENING          21610    9/init
/run/WSL/9_interop
unix    2      [ ACC ]                SEQPACKET          LISTENING          18291    -
/mnt/wslg/weston-notify.sock
unix    2      [ ACC ]                STREAM             LISTENING          18330    -
/var/run/dbus/system_bus_socket
unix    2      [ ACC ]                STREAM             LISTENING          22590    -
/mnt/wslg/runtime-dir/wayland-0
unix    2      [ ACC ]                STREAM             LISTENING          22591    -
/tmp/.X11-unix/X0
unix    2      [ ]                  DGRAM              -                  18532    -
/var/run/chrony/chronyd.sock
unix    2      [ ACC ]                STREAM             LISTENING          21660    -
/mnt/wslg/runtime-dir/pulse/native
unix    2      [ ACC ]                STREAM             LISTENING          222      -
/mnt/wslg/PulseServer
unix    2      [ ACC ]                STREAM             LISTENING          22652    -

```

## 2.2 sudo netstat -tuln

- Affiche les ports TCP et UDP ouverts (en écoute) ainsi que leurs adresses IP associées sans résolution de nom d'hôte (option -n).

```

(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.255.255.254:53      0.0.0.0:*              LISTEN
udp        0      0 10.255.255.254:53      0.0.0.0:*
udp        0      0 127.0.0.1:323          0.0.0.0:*
udp6       0      0 :::1:323               :::*

(root@DESKTOP-VH0G7EG)-[/home/kali]
#

```

### 2.3 echo "TMOUT=20" >> ~/.bashrc (root)

- Cette commande ajoute la ligne TMOUT=20 au fichier ~/.bashrc. La variable TMOUT détermine la durée d'inactivité (en secondes) après laquelle la session se déconnecte automatiquement. Ici, elle est définie à 20 secondes.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
timed out waiting for input: auto-logout

(kali@DESKTOP-VH0G7EG)-[~]
```

### 2.4 ssh -l votreCompte localhost (on suppose que SSH est installé) :

- Cette commande permet de se connecter à son propre système (localhost) via SSH avec un compte spécifique (-l spécifie le nom d'utilisateur). SSH doit être installé et configuré pour que cette commande fonctionne.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# ssh -l kali localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:0ELZbPZXzJ9noiRY73sATJcY8aDPwrp4NBm8OG8Qty
o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
kali@localhost's password:
Linux DESKTOP-VH0G7EG 5.15.153.1-microsoft-standard-WSL2 #1 SMP Fri Mar 29 2
3:14:13 UTC 2024 x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
=> https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
(kali@DESKTOP-VH0G7EG)-[~]
$
```

## Exercice 2 : Gestion des utilisateurs et des connexions

1. grep stagiaire /etc/shadow

En tant qu'utilisateur normal (kali), cette commande ne retournera aucun résultat car le fichier /etc/shadow (qui contient les mots de passe chiffrés) n'est lisible que par l'administrateur(root).

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# grep stagiaire /etc/shadow
stagiaire:$y$j9T$bNmXHpNIeIRwIaLgQiP1N1$hsVcDqBg8eD9sg1fAK11LWuJC/VYSLiHaXC
G8pSl3/:20003:0:99999:7:::

(root@DESKTOP-VH0G7EG)-[/home/kali]
# cat /etc/shadow
root:*:19966:0:99999:7:::
daemon:*:19966:0:99999:7:::
bin:*:19966:0:99999:7:::
sys:*:19966:0:99999:7:::
sync:*:19966:0:99999:7:::
games:*:19966:0:99999:7:::
man:*:19966:0:99999:7:::
lp:*:19966:0:99999:7:::
mail:*:19966:0:99999:7:::
news:*:19966:0:99999:7:::
uucp:*:19966:0:99999:7:::
proxy:*:19966:0:99999:7:::
www-data:*:19966:0:99999:7:::
backup:*:19966:0:99999:7:::
list:*:19966:0:99999:7:::
irc:*:19966:0:99999:7:::
_apt:*:19966:0:99999:7:::
nobody:*:19966:0:99999:7:::
systemd-network:!:19966:~::~:
```

## 2. Connexion en tant qu'administrateur et exécution de la commande

En tant qu'administrateur(root), cette commande permettra de vérifier la présence de l'utilisateur stagiaire dans le fichier /etc/shadow.

3. Changer la période de validité du mot de passe de stagiaire à 30 jours :

- Commandes :  
`sudo chage -M 30 stagiaire`  
`sudo chage -l stagiaire`

La première commande modifie la durée de validité du mot de passe à 30 jours, et la deuxième affiche les informations sur la politique de mot de passe de l'utilisateur stagiaire.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo chage -M 30 stagiaire

(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo chage -l stagiaire
Last password change           : Oct 07, 2024
Password expires                : Nov 06, 2024
Password inactive               : never
Account expires                 : never
Minimum number of days between password change : 0
Maximum number of days between password change : 30
Number of days of warning before password expires : 7

(root@DESKTOP-VH0G7EG)-[/home/kali]
#
```

4. Changer le mot de passe de l'utilisateur à « stagiaire2 », tester la connexion, puis le remettre à « stagiaire »

- Commandes : `sudo passwd stagiaire`

Cela permet de modifier le mot de passe de stagiaire puis de le remettre à l'original après test.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo passwd stagiaire
New password:
Retype new password:
passwd: password updated successfully

(root@DESKTOP-VH0G7EG)-[/home/kali]
#
```

5. Verrouiller et déverrouiller le mot de passe de l'utilisateur

5.1 Commandes : `sudo passwd -l stagiaire` (Verrouiller le mot de passe)

Cette commande verrouille le mot de passe de l'utilisateur stagiaire, empêchant toute connexion avec ce compte tant qu'il est verrouillé. Cela ne supprime pas l'utilisateur ni ses données, mais désactive temporairement l'accès en modifiant la chaîne du mot de passe dans le fichier `/etc/shadow`.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo passwd -l stagiaire
passwd: password changed.
```

5.2 `sudo passwd -S stagiaire` (Voir l'état du mot de passe )

Cette commande affiche l'état du mot de passe de l'utilisateur stagiaire. Elle montre si le compte est verrouillé ou non, ainsi que d'autres informations telles que la date de dernière modification du mot de passe et les règles de mot de passe appliquées.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo passwd -S stagiaire
stagiaire L 2024-10-15 0 30 7 -1
```

### 5.3 sudo passwd -u stagiaire (Déverrouiller le mot de passe)

Cette commande déverrouille le compte stagiaire, réactivant ainsi son accès par mot de passe. Elle retire le verrouillage précédemment appliqué avec passwd -l.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo passwd -u stagiaire
passwd: password changed.

(root@DESKTOP-VH0G7EG)-[/home/kali]
```

### 6. Visualiser les dernières connexions réussies et échouées :

- Commandes `last` | `head -5`

`lastb` | `head -5`

`last` affiche les connexions réussies, et `lastb` montre les tentatives de connexion échouées (si le fichier `/var/log/btmp` existe).

```
root@DESKTOP-VH0G7EG: /home/kali

(root@DESKTOP-VH0G7EG)-[/home/kali]
# last | head -5
root      pts/1                Tue Oct 15 12:40 - still logged in

/var/lib/wtmpdb/wtmp.db begins Tue Oct 15 12:40:51 2024

(root@DESKTOP-VH0G7EG)-[/home/kali]
# lastb | head -5
Command 'lastb' not found, did you mean:
  command 'last' from deb wtmpdb
  command 'lasts' from deb multicat
  command 'lastdb' from deb last-align
  command 'lastz' from deb lastz
Try: apt install <deb name>

(root@DESKTOP-VH0G7EG)-[/home/kali]
#
```

### 7. Lister les services actifs avec les fichiers associés

- Commande `lsof -i`

Cette commande affiche les connexions réseau actives et les fichiers ouverts associés.

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo lsof -i
COMMAND  PID USER  FD   TYPE DEVICE SIZE/OFF  NODE NAME
firefox-e 1099 kali   78u  IPv4  22259      0t0  TCP 172.23.105.29:55846->166.188.117.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox-e 1099 kali   96u  IPv4  25977      0t0  TCP 172.23.105.29:43554->191.144.160.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox-e 1099 kali  100u  IPv4  23487      0t0  TCP 172.23.105.29:54526->adsl-201-28-192-81.adsl.iam.net.ma:http (ESTABLISHED)
firefox-e 1099 kali  109u  IPv4  24242      0t0  TCP 172.23.105.29:47186->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox-e 1099 kali  110u  IPv4  24243      0t0  TCP 172.23.105.29:43426->mrs08s17-in-f3.1e100.net:http (ESTABLISHED)
firefox-e 1099 kali  112u  IPv4  25987      0t0  TCP 172.23.105.29:43692->209.100.149.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox-e 1099 kali  113u  IPv4  24244      0t0  TCP 172.23.105.29:47194->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)
firefox-e 1099 kali  122u  IPv4  27845      0t0  TCP 172.23.105.29:59628->adsl-235-28-192-81.adsl.iam.net.ma:http (ESTABLISHED)

(root@DESKTOP-VH0G7EG)-[/home/kali]
```

## 8. Désactiver les services inutiles :

- Commande `sudo apt-get remove nom-service`

Utilisez la commande suivante pour supprimer un service inutile .

```
(root@DESKTOP-VH0G7EG)-[/home/kali]
# service --status-all
[ - ] bluetooth
[ - ] cron
[ - ] dbus
[ - ] exim4
[ - ] haveged
[ - ] ipsec
[ ? ] kmod
[ - ] lightdm
[ - ] lm-sensors
[ ? ] networking
[ - ] openvpn
[ ? ] plymouth
[ ? ] plymouth-log
[ - ] procs
[ - ] pulseaudio-enable-autospawn
[ - ] saned
[ ? ] speech-dispatcher
[ - ] ssh
[ - ] sudo
[ - ] tor
[ - ] ufw
[ - ] x11-common
[ - ] xrdp

(root@DESKTOP-VH0G7EG)-[/home/kali]
#

(root@DESKTOP-VH0G7EG)-[/home/kali]
# sudo apt-get remove tor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  torsocks
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
  tor tor-geoipdb
0 upgraded, 0 newly installed, 2 to remove and 1 not upgraded.
After this operation, 23.9 MB disk space will be freed.
Do you want to continue? [Y/n] y
Reading database ... 162341 files and directories currently installed.)
Removing tor-geoipdb (0.4.8.12-1) ...
Removing tor (0.4.8.12-1) ...
invoke-rc.d: could not determine current runlevel
Stopping tor daemon...done (not running - there is no /run/tor/tor.pid).
Processing triggers for man-db (2.12.1-2) ...
```

## 9. Configurer une tâche cron :

- Commandes

`crontab -l > /tmp/crontab`

**Description :** Cette commande liste les tâches cron actuellement configurées pour l'utilisateur courant et redirige cette sortie vers un fichier nommé **crontab** dans le répertoire /tmp.

```
echo '0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire' >> /tmp/crontab
```

**Description :** Cette commande ajoute une nouvelle ligne à la fin du fichier **/tmp/crontab**. La ligne spécifie une tâche cron qui sera exécutée tous les jours à minuit (0 minutes, 0 heures).

- 0 0 \* \* \* : indique que la tâche doit être exécutée à 00h00 chaque jour.
- echo "stagiaire2" | passwd --stdin stagiaire : cette commande change le mot de passe de l'utilisateur stagiaire pour stagiaire2 en utilisant une entrée standard (stdin).

```
crontab /tmp/crontab
```

**Description :** Cette commande ajoute une nouvelle ligne à la fin du fichier /tmp/crontab. La ligne spécifie une tâche cron qui sera exécutée tous les jours à minuit (0 minutes, 0 heures).

```
crontab -l | tail -1
```

**Description :** Cette commande liste les tâches cron actuelles de l'utilisateur et affiche uniquement la dernière ligne de cette liste.

```
(root@DESKTOP-VH0G7EG)~/home/kali
# crontab -l > /tmp/crontab
0 0 * * * echo "stagiaire2" | passwd --st
(root@DESKTOP-VH0G7EG)~/home/kali
# echo '0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire' >> /tmp/crontab

ab /tmp (root@DESKTOP-VH0G7EG)~/home/kali
# crontab /tmp/crontab
b -1 | tail -1

(root@DESKTOP-VH0G7EG)~/home/kali
# crontab -l | tail -1
0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire
0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire
0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire
0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire
0 0 * * * echo "stagiaire2" | passwd --stdin stagiaire

(root@DESKTOP-VH0G7EG)~/home/kali
#
```

## Conclusion

Ce TP vous permet de vous familiariser avec les commandes essentielles de sécurité sur Linux, ainsi que la gestion des utilisateurs, des connexions et des services. Avec l'utilisation des capteurs appropriés pour surveiller les activités du système, vous pouvez renforcer la sécurité de votre environnement Linux contre les menaces internes et externes.