

TD N°1 –Sécurité Informatique & Cybersécurité



Virtualisation de Kali Linux
et Commandes de base sous Kali Linux

Présenté Par :
OCCINE ODNEY.

Professeur :
ISMAEL SAINT AMOOUR

Option:
RESEAUX

Niveau :
2e année

Date : 4/1/2026

INTRODUCTION

Dans le cadre du module *Sécurité Informatique & Cybersécurité*, ce travail dirigé a pour objectif de se familiariser avec l'environnement **Kali Linux**, les commandes fondamentales du système Linux ainsi que la gestion des fichiers et dossiers.

Ce TD permet également de comprendre les bases de l'analyse système et réseau à travers l'exécution de différentes commandes.

OBJECTIF DU TRAVAIL DIRIGÉ

Les objectifs principaux de ce TD sont :

- Installer Kali Linux sur une machine virtuelle
- Mettre à jour le système Linux
- Manipuler les fichiers et dossiers via le terminal
- Exécuter des commandes système et réseau
- Observer et analyser les informations produites par ces commandes
- Documenter les résultats dans un rapport technique

ENVIRONNEMENT DE TRAVAIL

- **Système d'exploitation** : Kali Linux
- **Type d'installation** : Machine virtuelle
- **Logiciel de virtualisation** : VMware
- **Interface utilisée** : Terminal Linux

DÉMARCHE SUIVIE

1- Installation de Kali Linux

Kali Linux a été installé sur une machine virtuelle en utilisant l'installateur graphique. Les paramètres de base tels que la langue, le clavier, le réseau et l'utilisateur ont été configurés correctement.



2- Mise à jour du système

Après l'installation, le système a été mis à jour à l'aide des commandes suivantes :

```
sudo apt update
```

```
sudo apt upgrade -y
```

```
Session Actions Edit View Help
(oddyht@scorpion)-[~]
$ sudo apt update
sudo: unable to resolve host scorpion: Name or service not known
[sudo] password for oddyht:
Get:1 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling I
nRelease [34.0 kB]
Get:2 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling/m
ain amd64 Packages [20.9 MB]
Get:3 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling/m
ain amd64 Contents (deb) [52.6 MB]
Get:4 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling/c
ontrib amd64 Packages [115 kB]
Get:5 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling/c
ontrib amd64 Contents (deb) [256 kB]
Fetched 73.9 MB in 2min 34s (481 kB/s)
812 packages can be upgraded. Run 'apt list --upgradable' to see them.

(oddyht@scorpion)-[~]
$
::1          ip6-allnodes    ip6-loopback
ff02::1      ip6-allrouters  kali
ff02::2      ip6-localhost    localhost
(oddyht@scorpion)-[~]
$
```

Ces commandes permettent de récupérer les dernières versions des paquets et de corriger d'éventuelles failles de sécurité.

GESTION DES DOSSIERS ET FICHIERS

Création de la structure de dossiers

Un dossier principal nommé **cybersec** a été créé avec trois sous-dossiers :

- scan
- logs
- scripts

```
(odyht@scorpion)-[~]  
$  
::1          ip6-allnodes    ip6-loopback  
ff02::1      ip6-allrouters kali  
ff02::2      ip6-localhost  localhost  
(odyht@scorpion)-[~]  
$ mkdir cybersec  
  
(odyht@scorpion)-[~]  
$ cd cybersec  
  
(odyht@scorpion)-[~/cybersec]  
$ mkdir scan logs scripts
```

Affichage de la structure

tree cybersec

```
(odyht@scorpion)-[~/cybersec]  
$ tree  
.  
├── logs  
├── scan  
└── scripts
```

Cette commande

permet de visualiser l'arborescence des dossiers.

Création et manipulation des fichiers

Des fichiers notes.txt ont été créés dans les dossiers scan et logs, puis du contenu a été ajouté

```
touch scan/notes.txt logs/notes.txt  
echo "Notes de scan réseau" > scan/notes.txt  
echo "Fichier de logs système" > logs/notes.txt
```

```
(odyht@scorpion)-[~/cybersec]  
$ touch scan/notes.txt logs/notes.txt  
  
(odyht@scorpion)-[~/cybersec]  
$ echo "Notes de scan réseau" > scan/notes.txt  
echo "Fichier de logs système" > logs/notes.txt  
  
(odyht@scorpion)-[~/cybersec]  
$ cat scan/notes.txt  
cat logs/notes.txt  
Notes de scan réseau  
Fichier de logs système
```

Copie, déplacement et suppression

- Copie du fichier vers scripts
- Déplacement du fichier
- Suppression du fichier
- Vérification avec ls et find

```
Fichier de logs système

(od yht@scorpion)-[~/cybersec]
$ cp scan/notes.txt scripts/

(od yht@scorpion)-[~/cybersec]
$ ls scripts
notes.txt
```

```
(od yht@scorpion)-[~/cybersec]
$ mv scripts/notes.txt scan/

(od yht@scorpion)-[~/cybersec]
$ rm scripts/notes.txt
rm: cannot remove 'scripts/notes.txt': No such file or directory

(od yht@scorpion)-[~/cybersec]
$ ls scripts

(od yht@scorpion)-[~/cybersec]
$ rm -r scan logs scripts

(od yht@scorpion)-[~/cybersec]
$ ls cybersec
ls: cannot access 'cybersec': No such file or directory

(od yht@scorpion)-[~/cybersec]
$ ls
```

Ces opérations permettent de maîtriser les commandes cp, mv, rm et ls.

COMMANDES SYSTÈME ET RÉSEAU

Les commandes suivantes ont été exécutées afin d'analyser le système :

- df -h : espace disque
- du -sh : taille des dossiers
- free -h : mémoire RAM
- ps aux : processus en cours
- lspci : matériel PCI
- ip a : interfaces réseau
- traceroute google.com
- netstat -tuln
- ss -tuln
- journalctl
- date
- hostnamectl
- cat /etc/os-release

```
(od yht@scorpion)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.188.128 netmask 255.255.255.0 broadcast 192.168.188.255
    ether 00:0c:29:0a:7f:bb txqueuelen 1000 (Ethernet)
    RX packets 53465 bytes 76809498 (73.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20857 bytes 1259071 (1.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 88 bytes 6960 (6.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 88 bytes 6960 (6.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(odyht@scorpion)-[~]
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G   0% /dev
tmpfs           392M  1.2M  390M   1% /run
/dev/sda1       79G   16G   59G  21% /
tmpfs           2.0G  4.0K   2.0G   1% /dev/shm
none            1.0M   0    1.0M   0% /run/credentials/systemd-journald.servi
ce
tmpfs           2.0G  8.0K   2.0G   1% /tmp
none            1.0M   0    1.0M   0% /run/credentials/getty@tty1.service
tmpfs           392M 108K   391M   1% /run/user/1001

(odyht@scorpion)-[~]
$ du -sh
3.1M .

(odyht@scorpion)-[~]
$ free -h
              total        used        free      shared  buff/cache   availa
ble
Mem:           3.8Gi        887Mi        2.4Gi         8.8Mi         748Mi        3.
0Gi
Swap:          953Mi           0B         953Mi
```

```
(odyht@scorpion)-[~]
$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 24464 15124 ?        Ss   19:51   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S    19:51   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    19:51   0:00 [pool_work
root         4  0.0  0.0      0     0 ?        I<   19:51   0:00 [kworker/R
root         5  0.0  0.0      0     0 ?        I<   19:51   0:00 [kworker/R
root         6  0.0  0.0      0     0 ?        I<   19:51   0:00 [kworker/R
root         7  0.0  0.0      0     0 ?        I<   19:51   0:00 [kworker/R
root         8  0.0  0.0      0     0 ?        I<   19:51   0:00 [kworker/R
root        11  0.0  0.0      0     0 ?        I    19:51   0:03 [kworker/0
root        13  0.0  0.0      0     0 ?        I<   19:51   0:00 [kworker/R
root        14  0.0  0.0      0     0 ?        S    19:51   0:00 [ksoftirqd
root        15  0.0  0.0      0     0 ?        R    19:51   0:01 [rcu_preem
root        16  0.0  0.0      0     0 ?        S    19:51   0:00 [rcu_exp_p
root        17  0.0  0.0      0     0 ?        S    19:51   0:00 [rcu_exp_g
```

```
(odyht@scorpion)-[~]
$ sudo apt install traceroute
sudo: unable to resolve host scorpion: Name or service not known
[sudo] password for odyht:
traceroute is already the newest version (1:2.1.6-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 812
```

```
traceroute to google.com (142.250.217.206), 30 hops max, 60 byte packets
 1  192.168.188.2 (192.168.188.2)  4.916 ms  4.595 ms  0.743 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
```

```

(od yht@scorpi on)-[~]
$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

(od yht@scorpi on)-[~]
$ ss -tuln
Netid State  Recv-Q Send-Q Local Address:Port      Peer Address:Port

(od yht@scorpi on)-[~]
$ journalctl
Hint: You are currently not seeing messages from other users and the system.
Users in groups 'adm', 'systemd-journal' can see all messages.
Pass -q to turn off this notice.
Jan 03 12:34:19 kali sudo[11962]:      odyht : user NOT in sudoers ; TTY=pts/0
Jan 03 12:37:07 kali su[13367]: pam_unix(su-l:auth): authentication failure;
Jan 03 12:37:09 kali su[13367]: FAILED SU (to root) odyht on pts/0
Jan 03 12:37:36 kali su[13603]: pam_unix(su-l:auth): authentication failure;
Jan 03 12:37:38 kali su[13603]: FAILED SU (to root) odyht on pts/0
Jan 03 12:39:21 kali sudo[14439]:      odyht : user NOT in sudoers ; TTY=pts/0
-- Boot e9f5e2487e494866ae6266eeafb3417f --
Jan 03 12:45:54 kali systemd[885]: Queued start job for default target defau>
Jan 03 12:45:54 kali systemd[885]: Created slice app.slice - User Applicatio>
Jan 03 12:45:54 kali systemd[885]: Created slice session.slice - User Core S>
Jan 03 12:45:54 kali systemd[885]: Reached target paths.target - Paths.
Jan 03 12:45:54 kali systemd[885]: Reached target timers.target - Timers.
Jan 03 12:45:54 kali systemd[885]: Starting dbus.socket - D-Bus User Message>

```

```

(od yht@scorpi on)-[~]
$ journalctl -f
Hint: You are currently not seeing messages from other users and the system.
Users in groups 'adm', 'systemd-journal' can see all messages.
Pass -q to turn off this notice.
Jan 03 20:38:15 scorpi on systemd[1163]: Started xfconfd.service - Xfce confi
uration service.
Jan 03 20:38:30 scorpi on xfce4-screensaver-dialog[23984]: gkr-pam: unlocked l
ogin keyring
Jan 03 20:38:30 scorpi on xfce4-screensaver-dialog[24143]: pam_unix(xfce4-scre
ensaver:account): setuid failed: Operation not permitted
Jan 03 21:15:33 scorpi on sudo[39724]:      odyht : TTY=pts/0 ; PWD=/home/odyht
; USER=root ; COMMAND=/usr/bin/apt install traceroute
Jan 03 21:15:33 scorpi on sudo[39724]: pam_unix(sudo:session): session opened
for user root(uid=0) by odyht(uid=1001)
Jan 03 21:15:33 scorpi on sudo[39724]: pam_unix(sudo:session): session closed
for user root
Jan 03 21:16:32 scorpi on dbus-daemon[1185]: [session uid=1001 pid=1185 pidfd=
5] Activating via systemd: service name='org.xfce.Xfconf' unit='xfconfd.servi
ce' requested by ':1.39' (uid=1001 pid=1434 comm="/usr/lib/x86_64-linux-gnu/x
fce4/notifyd/xfce4-noti")
Jan 03 21:16:32 scorpi on systemd[1163]: Starting xfconfd.service - Xfce confi
guration service ...
Jan 03 21:16:32 scorpi on dbus-daemon[1185]: [session uid=1001 pid=1185 pidfd=
5] Successfully activated service 'org.xfce.Xfconf'
Jan 03 21:16:32 scorpi on systemd[1163]: Started xfconfd.service - Xfce confi
guration service.

```

```

(od yht@scorpi on)-[~]
$ journalctl -b
Hint: You are currently not seeing messages from other users and the system.
Users in groups 'adm', 'systemd-journal' can see all messages.
Pass -q to turn off this notice.
Jan 03 19:52:27 scorpi on systemd[1163]: Queued start job for default target >
Jan 03 19:52:27 scorpi on systemd[1163]: Created slice app.slice - User Appli>
Jan 03 19:52:27 scorpi on systemd[1163]: Created slice session.slice - User Co>
Jan 03 19:52:27 scorpi on systemd[1163]: Reached target paths.target - Paths.
Jan 03 19:52:27 scorpi on systemd[1163]: Reached target timers.target - Timer>
Jan 03 19:52:27 scorpi on systemd[1163]: Starting dbus.socket - D-Bus User Me>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on dirmgr.socket - GnuPG >
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on gnome-keyring-daemon.sock>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on gpg-agent-browser.socke>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on gpg-agent-extra.socket >
Jan 03 19:52:27 scorpi on systemd[1163]: Starting gpg-agent-ssh.socket - GnuP>
Jan 03 19:52:27 scorpi on systemd[1163]: Starting gpg-agent.socket - GnuPG cr>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on keyboard.socket - GnuPG>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on pipewire-pulse.socket ->
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on pipewire.socket - PipeW>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on speech-dispatcher.socke>
Jan 03 19:52:27 scorpi on systemd[1163]: Starting ssh-agent.socket - OpenSSH >
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on systemd-ask-password.sock>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on dbus.socket - D-Bus Use>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on gpg-agent-ssh.socket ->
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on gpg-agent.socket - GnuP>
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on ssh-agent.socket - Open>
Jan 03 19:52:27 scorpi on systemd[1163]: Starting gcr-ssh-agent.socket - GCR >
Jan 03 19:52:27 scorpi on systemd[1163]: Listening on gcr-ssh-agent.socket ->
Jan 03 19:52:27 scorpi on systemd[1163]: Started dbus.service - D-Bus User Me>
Jan 03 19:52:27 scorpi on systemd[1163]: Reached target sockets.target - Sock>
Jan 03 19:52:27 scorpi on systemd[1163]: Reached target basic.target - Basic>
Jan 03 19:52:27 scorpi on systemd[1163]: Starting dbus.service - D-Bus User M>
Jan 03 19:52:27 scorpi on systemd[1163]: Started pipewire.service - PipeWire>
Jan 03 19:52:27 scorpi on systemd[1163]: Started gnome-keyring-daemon.service>
Jan 03 19:52:27 scorpi on systemd[1163]: Started dbus.service - D-Bus User Me>
Jan 03 19:52:27 scorpi on systemd[1163]: Started mpri s-proxy.service - Blueto>
Jan 03 19:52:27 scorpi on systemd[1163]: Started wireplumber.service - Multime>
Jan 03 19:52:27 scorpi on systemd[1163]: Started filter-chain.service - PipeW>
Jan 03 19:52:27 scorpi on systemd[1163]: Started pipewire-pulse.service - Pip>
Jan 03 19:52:27 scorpi on systemd[1163]: Reached target default.target - Main>
Jan 03 19:52:27 scorpi on systemd[1163]: Startup finished in 260ms.
Jan 03 19:52:27 scorpi on gnome-keyring-daemon[1188]: GNOME KEYRING CONTROL-/>
Jan 03 19:52:27 scorpi on wireplumber[1198]: wp-event-dispatcher: wp_event_di>

```

```

(od yht@scorpi on)-[~]
$ journalctl -n 10
Hint: You are currently not seeing messages from other users and the system.
Users in groups 'adm', 'systemd-journal' can see all messages.
Pass -q to turn off this notice.
Jan 03 20:38:15 scorpi on systemd[1163]: Started xfconfd.service - Xfce confi>
Jan 03 20:38:30 scorpi on xfce4-screensaver-dialog[23984]: gkr-pam: unlocked >
Jan 03 20:38:30 scorpi on xfce4-screensaver-dialog[24143]: pam_unix(xfce4-scr>
Jan 03 21:15:33 scorpi on sudo[39724]:      odyht : TTY=pts/0 ; PWD=/home/odyht>
Jan 03 21:15:33 scorpi on sudo[39724]: pam_unix(sudo:session): session opened>
Jan 03 21:15:33 scorpi on sudo[39724]: pam_unix(sudo:session): session closed>
Jan 03 21:16:32 scorpi on dbus-daemon[1185]: [session uid=1001 pid=1185 pidfd>
Jan 03 21:16:32 scorpi on systemd[1163]: Starting xfconfd.service - Xfce conf>
Jan 03 21:16:32 scorpi on dbus-daemon[1185]: [session uid=1001 pid=1185 pidfd>
Jan 03 21:16:32 scorpi on systemd[1163]: Started xfconfd.service - Xfce confi>
lines 1-10/10 (END)

```

```

(od yht@scorpi on)-[~]
$ timedatectl

          Local time: Sat 2026-01-03 21:41:15 EST
          Universal time: Sun 2026-01-04 02:41:15 UTC
             RTC time: Sun 2026-01-04 02:41:14
            Time zone: America/New_York (EST, -0500)
system clock synchronized: yes
              NTP service: active
             RTC in local TZ: no

```

CONCLUSION

Ce travail dirigé a permis d'acquérir des compétences essentielles en environnement Linux, notamment l'utilisation de Kali Linux, la manipulation des fichiers et dossiers ainsi que l'analyse du système et du réseau.

Les objectifs fixés ont été atteints avec succès. Quelques difficultés mineures ont été rencontrées lors de la manipulation des fichiers, mais elles ont été résolues grâce à la vérification des chemins et des commandes utilisées.