

# UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI (UNITECH)

Faculté des Sciences de Génie,et d'Architecture



TD NoX-Sécurité informatique&Cybersécurité

NOM.....MAITRE

PRÉNOM.....Amourana

NIVEAU.....2

DATE.....le/20/01/25

## Objectif du TD:

- Installer kali Linux
- Manipuler les commandes Linux de base
- Gérer les fichiers et dossier
- Observer l'état du système et du reseau.

```
(kali@kali)-[~]
$ sudo apt upgrade -y
The following packages were automatically installed and are no longer required:
bloodhound.py libavformat61 libgavl-1 libmplex2-2.1-0t64 libsphinxbase3t64 mesa-vaapi-drivers
curlftpfs libconfig-inifiles-perl libmjpegutils-2.1-0t64 libpocketsphinx3 libswscale8 pocketsphinx-en-us
libavfilter10 libfuse2t64 libmpeg2encpp-2.1-0t64 libpostproc58 libvdpau-va-gl1 vdpau-driver-all
Use 'sudo apt autoremove' to remove them.

Upgrading:
7zip                               libde265-0                               libstdc++-10-0
adduser                           libdebconfclient0                       libsystemd0
alsa-ucm-conf                     libdecor-0-0                             libsystemd-journald
amd64-microcode                  libdecor-0-plugin-1-gtk                 libsystemd-resolved
apache2                           libelt2                                  libsystemd-sysd
apache2-bin                       libdouble-conversion3                   libsystemd-timesyncd
apache2-data                      libdrm-amdgpu1                           libsystemd-userdb
apache2-utils                     libdrm-common                           libsystemd-xattr
apparmor                          libdrm-intel1                            libsystemd0
apt                                libdrm-nouveau2                         libsystemd2
apt-utils                         libdrm-radeon1                           libsystemd23
arping                            libdrm2                                  libsystemd23
at-spi2-common                    libdvdnav4                               libsystemd23
at-spi2-core                       libdvdread8t64                           libsystemd23
binutils                          libebackend-1.2-11t64                    libsystemd23
binutils-common                   libebook-1.2-21t64                       libsystemd23
binutils-mingw-w64-x86_64         libebook-contacts-1.2-4t64               libsystemd23
binutils-mingw-w64-x86_64         libedata-book-1.2-27t64                  libsystemd23
binutils-x86-64-linux-gnu         libedata-server-1.2-27t64                 libsystemd23
python3-flask-socketio            python3-fonttools                        python3-frozenset
python3-gdal                      python3-gevent                           python3-gi
python3-gi-cairo                  python3-greenlet                          python3-gssapi
python3-gssapi                     python3-gvm                               python3-hamcrest
python3-html5lib                  python3-impacket                          python3-iniconfig
python3-ipwhois                    python3-jeepney                           python3-joblib
python3-jq                          python3-jsonschema-specifications
```

La commande `sudo apt upgrade -Y` permet de mettre à jour tous les logiciels installés sur le système.

```
(kali@kali)-[~]
$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2025.4"
VERSION="2025.4"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

La commande `cat /etc/os-release` permet d'afficher les informations sur le système d'exploitation.

```
(kali@kali)-[~]
$ hostnamectl
Static hostname: kali
Icon name: computer-vm
Chassis: vm
Machine ID: b69758c0cad3481e967dcad827001d56
Boot ID: 5617726203ba4216b7d3b59d70f3cfe7
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.18.3+kali+1-amd64
Architecture: x86_64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Hardware Version: 1.2
Firmware Version: VirtualBox
Firmware Date: Fri 2006-12-01
Firmware Age: 19y 1month 2w 2d

(kali@kali)-[~]
$ sudo hostnamectl set-hostname Amourana
[sudo] password for kali:

(kali@kali)-[~]
$
```

Hostnamectl: Affiche les informations liées au nom de la machine(hostname)

Sudo hostnamectl: permet de modifier ou gérer le nom de la machine avec les droits administrateur.

```
(kali@kali)-[~]
$ journalctl -n 10
Jan 16 14:15:01 kali CRON[38895]: pam_unix(cron:session): session opened for user root
Jan 16 14:17:01 kali CRON[39907]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 16 14:17:01 kali CRON[39909]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
Jan 16 14:17:01 kali CRON[39907]: pam_unix(cron:session): session closed for user root
Jan 16 14:17:55 kali sudo[39864]: kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/apt install traceroute -y
Jan 16 14:17:55 kali sudo[39864]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Jan 16 14:17:56 kali sudo[39864]: pam_unix(sudo:session): session closed for user root
Jan 16 14:25:01 kali CRON[43894]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 16 14:25:01 kali CRON[43896]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 16 14:25:01 kali CRON[43894]: pam_unix(cron:session): session closed for user root

(kali@kali)-[~]
$
```

La commande journalctl -n 10 permet d'afficher les 10 derniers messages des journaux systems.

```
(kali@kali)-[~]
$ date
Fri Jan 16 02:32:32 PM EST 2026

(kali@kali)-[~]
$ timedatectl
Local time: Fri 2026-01-16 14:33:19 EST
Universal time: Fri 2026-01-16 19:33:19 UTC
RTC time: Fri 2026-01-16 19:33:19
Time zone: America/New_York (EST, -0500)
System clock synchronized: no
NTP service: inactive
RTC in local TZ: no

(kali@kali)-[~]
$ hostnamectl
Static hostname: kali
Icon name: computer-vm
Chassis: vm
Machine ID: b69758c0cad3481e967dcad827001d56
Boot ID: 5617726203ba4216b7d3b59d70f3cfe7
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.18.3+kali+1-amd64
Architecture: x86_64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Hardware Version: 1.2
Firmware Version: VirtualBox
Firmware Date: Fri 2006-12-01
Firmware Age: 19y 1month 2w 2d

(kali@kali)-[~]
$
```

Timedatectl: Affiche et permet de gérer les paramètres de date du système(fuseau horaire,synchronization).

La commande `journctl -b` permet d'afficher les journaux du système depuis le dernier démarrage.

Journalctl montre les messages enregistrés par le système et les services.

```
(kali@kali)-[~]
└─$ sudo apt install traceroute -y
[sudo] password for kali:
traceroute is already the newest version (1:2.1.6-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 8
└─$ traceroot google.com
traceroot: command not found
└─$ traceroute google.com
traceroute to google.com (172.217.165.206), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.752 ms  0.639 ms  0.573 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  * * *
```

Sudo apt install traceroute -y installe l'outil traceroute automatiquement, sans demander de confirmation.

Traceroute google.com affiche le chemin reseau emprunté par les paquets pour atteindre le serveur google.com.

```
(kali@kali)-[~]
└─$ ps aux|head -10
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 24576 15084 ?        Ss   12:58   0:02 /sbin/init splash
root         2  0.0  0.0      0     0 ?        S    12:58   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    12:58   0:00 [pool_workqueue_release]
root         4  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-rcu_gp]
root         5  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-sync_wq]
root         6  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-kvfree_rcu_reclaim]
root         7  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-slub_flushwq]
root         8  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-netns]
root        10  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/0:0H-kblockd]
```



La commande `lspci | head -10` permet d'afficher les 10 premiers processus en cours d'exécution sur le système.

```
(kali@kali)~$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:02.0 VGA compatible controller: VMware SVGA II Adapter
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Controller (rev 01)
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 00)
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW (ICH6 Family) USB2 EHCI Controller (rev 02)
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)

(kali@kali)~$ lspci -v
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
    Flags: fast devsel
    Kernel modules: intel_agp

00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
    Flags: bus master, medium devsel, latency 0

00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01) (prog-if 8a [ISA Compatibility mode controller, supports both channels switched to PCI native mode, supports bus mastering])
    Flags: bus master, fast devsel, latency 64
    I/O ports at 01f0 [size=8]
    I/O ports at 03f4
    I/O ports at 0270 [size=8]
    I/O ports at 0374
    I/O ports at d000 [size=16]
    Kernel driver in use: ata_piix
    Kernel modules: ata_piix, ata_generic
```

`Lspci`: liste tous les périphériques PCI de l'ordinateur

`Lspci -v`: Affiche les périphériques PCI avec plus de détails.

```
(kali@kali)~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G   0% /dev
tmpfs           393M  972K  392M   1% /run
/dev/sda1       79G   17G   58G  23% /
tmpfs           2.0G   4.0K  2.0G   1% /dev/shm
none            1.0M   0    1.0M   0% /run/credentials/systemd-journald.service
tmpfs           2.0G  112K  2.0G   1% /tmp
none            1.0M   0    1.0M   0% /run/credentials/getty@tty1.service
tmpfs           393M  104K  392M   1% /run/user/1000

(kali@kali)~$ du -sh
3.3M .

(kali@kali)~$ free -h
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi         898Mi       2.1Gi         16Mi         1.1Gi         3.0Gi
Swap:          953Mi           0B          953Mi
```

`Df -h`: Affiche l'espace disque disponible et utilise pour chaque partition, en format lisible.

`Du -sh`: Affiche la liste totale d'un dossier ou fichier.

Free -h: Affiche la quantité de mémoire RAM utilisée et disponible, en format lisible.

```
(kali@kali)-[~]
$ ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root            1  0.0  0.3 24576 15084 ?        Ss   12:58   0:02 /sbin/init splash
root            2  0.0  0.0      0     0 ?        S    12:58   0:00 [kthreadd]
root            3  0.0  0.0      0     0 ?        S    12:58   0:00 [pool_workqueue_release]
root            4  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-rcu_gp]
root            5  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-sync_wq]
root            6  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-kvfree_rcu_reclaim]
root            7  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-slub_flushwq]
root            8  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-netns]
root           10  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/0:0H-kblockd]
root           12  0.0  0.0      0     0 ?        I    12:58   0:01 [kworker/u4:0-events_unbound]
root           13  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-mm_percpu_wq]
root           14  0.0  0.0      0     0 ?        S    12:58   0:00 [ksoftirqd/0]
root           15  0.0  0.0      0     0 ?        I    12:58   0:01 [rcu_preempt]
root           16  0.0  0.0      0     0 ?        S    12:58   0:00 [rcu_exp_par_gp_kthread_worker/0]
root           17  0.0  0.0      0     0 ?        S    12:58   0:00 [rcu_exp_gp_kthread_worker]
root           18  0.0  0.0      0     0 ?        S    12:58   0:00 [migration/0]
root           19  0.0  0.0      0     0 ?        S    12:58   0:00 [idle_inject/0]
root           20  0.0  0.0      0     0 ?        S    12:58   0:00 [cpuhp/0]
root           22  0.0  0.0      0     0 ?        S    12:58   0:00 [kdevtmpfs]
root           23  0.0  0.0      0     0 ?        I<   12:58   0:00 [kworker/R-inet_frag_wq]
root           24  0.0  0.0      0     0 ?        I    12:58   0:00 [rcu_tasks_kthread]
root           25  0.0  0.0      0     0 ?        I    12:58   0:00 [rcu_tasks_rude_kthread]
```

La command eps aux: permet d'afficher tous les processus enc ours d'exécution sur le système.

```
(kali@kali)-[~]
$ ls -la cybersec/scripts/
total 8
drwxrwxr-x 2 kali kali 4096 Jan 16 13:51 .
drwxrwxr-x 5 kali kali 4096 Jan 16 12:46 ..

(kali@kali)-[~]
$ rm -rf cybersec/scan cybersec/logs cybersec/scripts

(kali@kali)-[~]
$
```

Ls -la:Affiche tous les fichiers et dossiers, y compris les fichiers caches, avrc details complets.

Rm -rf:Suprime un dossiee et tout son contenu de manière force,sans demande de confirmation.

```

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::1aeb:ad26:8895:2d84 prefixlen 64 scopeid 0x20<link>
    inet6 fd17:625c:f037:2:8a34:dcea:7b49:666b prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:42:2f:9c txqueuelen 1000 (Ethernet)
    RX packets 16 bytes 4222 (4.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 6443 (6.2 KiB)
    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 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$

```

La commande ifconfig permet d'afficher et de configure les interfaces reseau sur le système linux.

```

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

(kali@kali)-[~]
$ ls -la cybersec/scripts/
total 12
drwxrwxr-x 2 kali kali 4096 Jan 16 13:05 .
drwxrwxr-x 5 kali kali 4096 Jan 16 12:46 ..
-rw-rw-r-- 1 kali kali 55 Jan 16 13:05 notes.txt

(kali@kali)-[~]
$ cp cybersec/scan/notes.txt cybersec/scripts/
cp: cannot stat 'cybersec/scan/notes.txt': No such file or directory

(kali@kali)-[~]
$ ls -la cybersec/scripts/
total 12
drwxrwxr-x 2 kali kali 4096 Jan 16 13:05 .
drwxrwxr-x 5 kali kali 4096 Jan 16 12:46 ..
-rw-rw-r-- 1 kali kali 55 Jan 16 13:05 notes.txt

(kali@kali)-[~]
$

```

Cp cybersec/scan/notes.txt cybersec/script/: Copie le fichier notes.txt depuis le dossier cybersec/scan vers le dossier cybersec/script.

Ls -la cybersec/script/: Affiche tous les fichiers du dossier script, y compris les fichiers caches, avec leurs d'etails complexes.

Cp: Permet de copier un fichier ou un dossier d'un emplacement vers un autre.



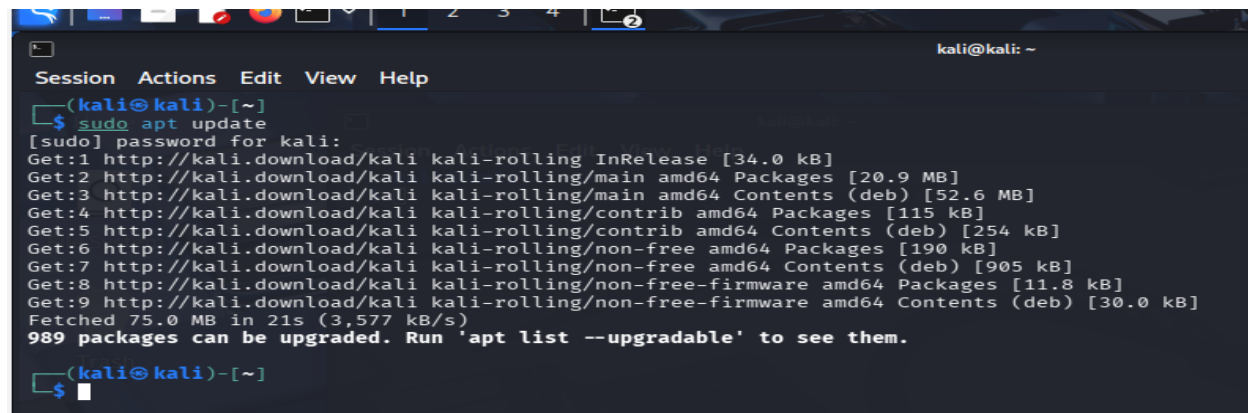
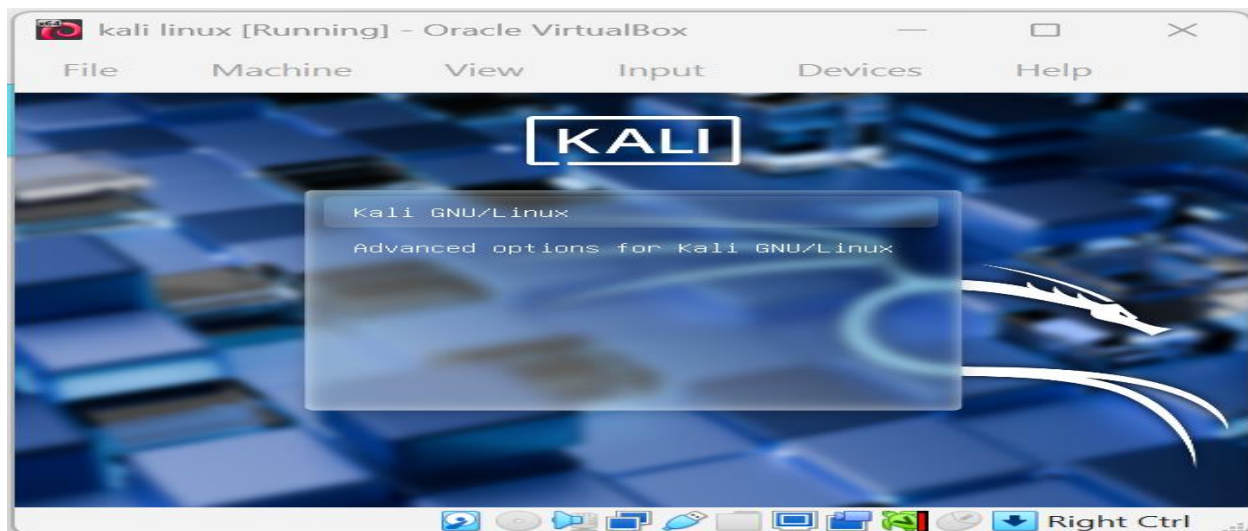
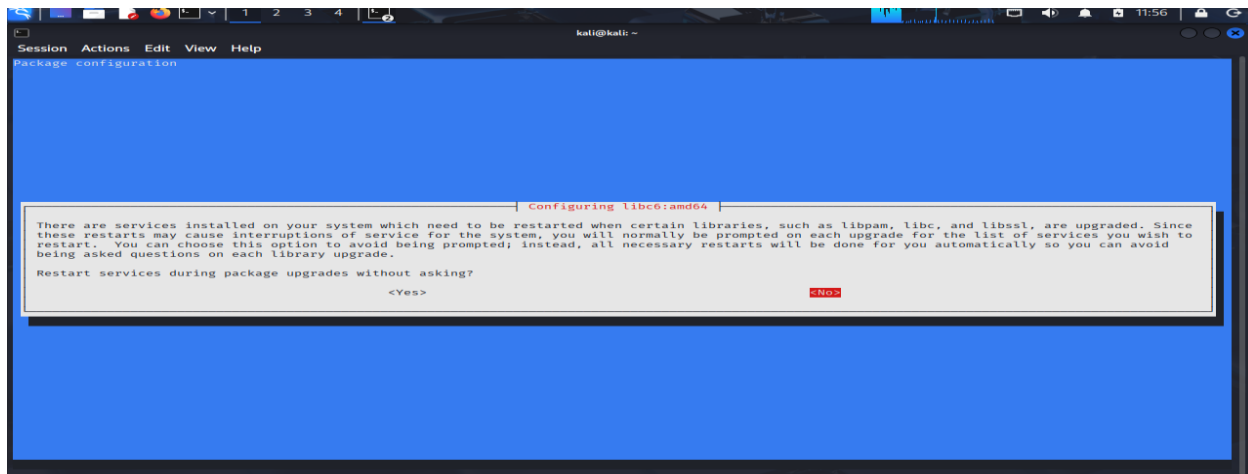
```
(kali@kali)-[~]
└─$ sudo apt autoremove -y
REMOVING:
  bloodhound.py  libavformat61  libgavi1-1  libmpeg2-2.1-0t64  libpocketsphinx3  libpocketsphinx3t64  mesa-vaapi-drivers
  curlftpfs  libconfig-inifiles-perl  libmpeg2encpp-2.1-0t64  libpostproc54  libpocketsphinx3  libpocketsphinx3t64  mesa-vaapi-drivers
  libavfilter10  libfuse2t64  libmpeg2encpp-2.1-0t64  libpostproc54  libpocketsphinx3  libpocketsphinx3t64  mesa-vaapi-drivers
Summary:
  Upgrading: 0, Installing: 0, Removing: 10, Not Upgrading: 8
  Freed space: 60.1 MB
(Reading database ... 433383 files and directories currently installed.)
Removing bloodhound.py (1.9.0-0kali1) ...
Removing curlftpfs (0.9.2-10) ...
Removing libavfilter10:amd64 (7:7.1.2-1+b1) ...
Removing libavformat61:amd64 (7:7.1.2-1+b1) ...
Removing libconfig-inifiles-perl (3.000003-4) ...
Removing libfuse2t64:amd64 (2.9.9-9) ...
Removing libgavi1-1:amd64 (0.10.0-3+b1) ...
Removing libmpeg2encpp-2.1-0t64:amd64 (1:2.1.0+debian-8.1+b1) ...
Removing libmpeg2-2.1-0t64:amd64 (1:2.1.0+debian-8.1+b1) ...
Removing libmpeg2t64:amd64 (2.1.0+debian-8.1+b1) ...
Removing libpocketsphinx3:amd64 (0.8.5+prealpha1-15+b4) ...
Removing libpostproc54:amd64 (7:7.1.3-1) ...
Removing libpocketsphinx3t64:amd64 (0.8.5+prealpha1-15+b1) ...
Removing libswscale8:amd64 (7:7.1.2-1+b1) ...
Removing vdpau-driver-all:amd64 (1.5-3+b1) ...
Removing libvdpau-va-gl1:amd64 (0.4.2-2) ...
Removing mesa-vaapi-drivers:amd64 (25.2.6-1) ...
Removing pocketsphinx-en-us (0.8.5+prealpha1-15) ...
Processing triggers for libc-bin (2.42-5) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.3) ...
(kali@kali)-[~]
└─$ sudo apt autoclean
(kali@kali)-[~]
```

Sudo apt autoremove -y: Supprime automatiquement les paquets et dépendances inutilisés qui ne sont plus nécessaires sur le système.

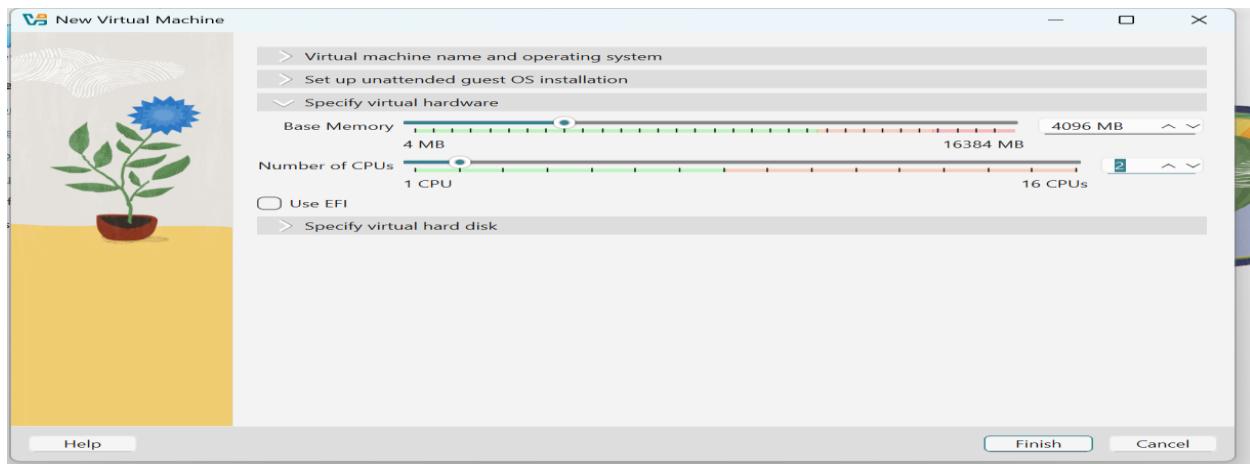
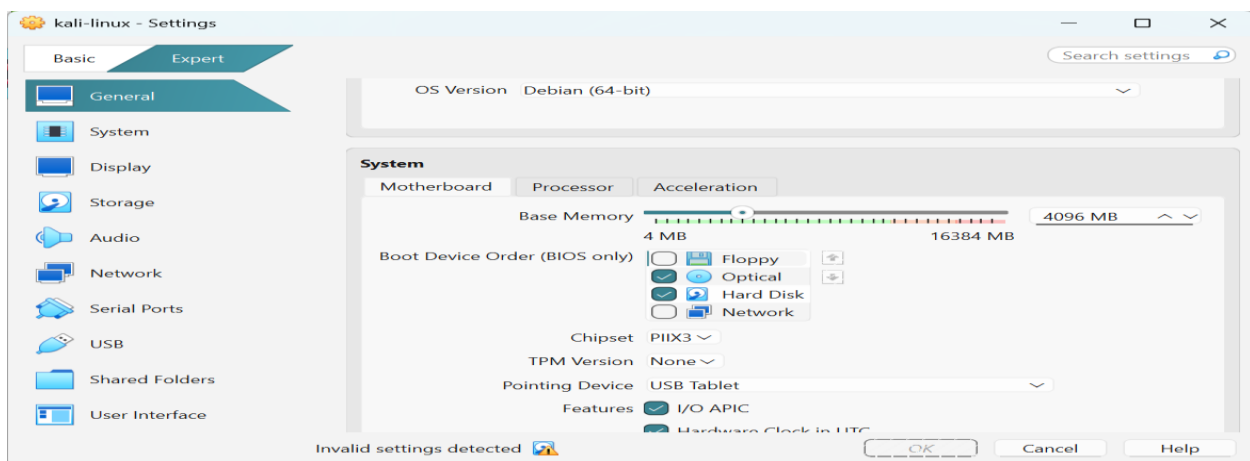
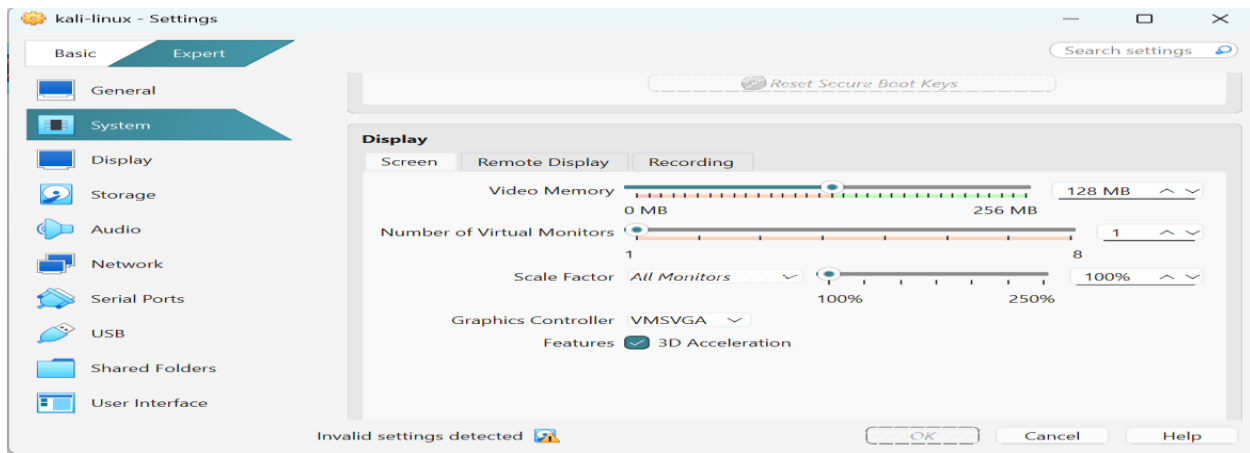
Sudo apt autoclean: Supprime les fichiers de paquets téléchargés et obsolètes pour libérer de l'espace disque.

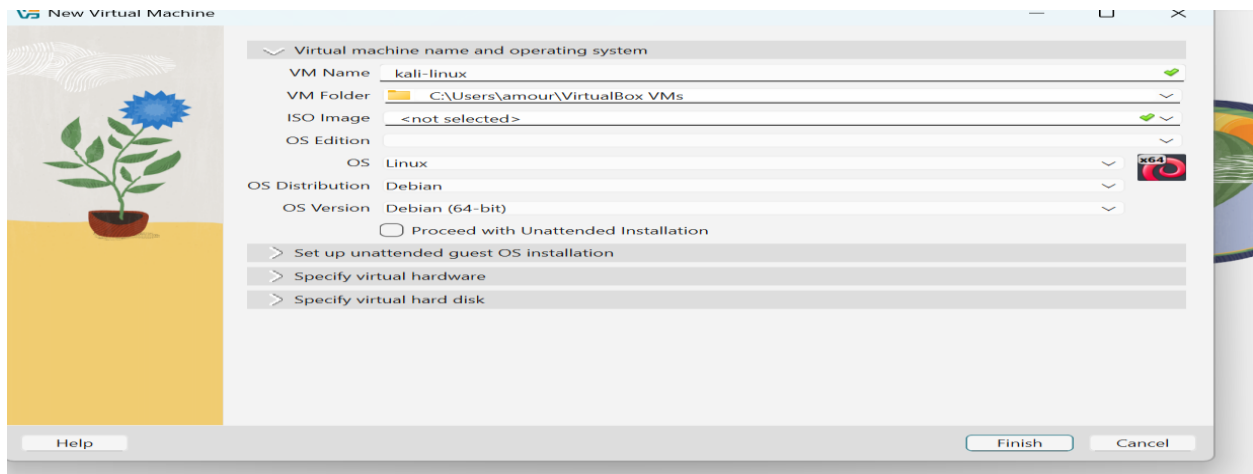
```
Session Actions Edit View Help
(kali@kali)-[~]
└─$ echo "Notes de scan reseau - $(date)" > cybersec/scan/notes.txt
(kali@kali)-[~]
└─$ echo "logs d'analyse - $(date)" > cybersec/logs/notes.txt
(kali@kali)-[~]
└─$ cat cybersec/scan/notes.txt
Notes de scan reseau - Fri Jan 16 01:01:02 PM EST 2026
(kali@kali)-[~]
└─$ cat cybersec/logs/notes.txt
logs d'analyse - Fri Jan 16 01:02:23 PM EST 2026
(kali@kali)-[~]
└─$ cp cybersec/scan/notes.txt cybersec/scripts
(kali@kali)-[~]
└─$ ls -la cybersec/scripts/
total 12
drwxrwxr-x 2 kali kali 4096 Jan 16 13:05 .
drwxrwxr-x 5 kali kali 4096 Jan 16 12:46 ..
-rw-rw-r-- 1 kali kali 55 Jan 16 13:05 notes.txt
(kali@kali)-[~]
└─$
```

La commande echo permet d'afficher du texte ou des variables dans le terminal.



La commande `sudo apt update` permet de mettre à jour la liste des paquets disponibles sur le système linux.





Résumé: J'ai appris à naviguer dans le système linux gérer les fichiers et dossiers avec les commandes de base. Utiliser les commande reseau et consulter les journaux système.

La tache a été réussie toutes les commandes pnt été executes correctement et les résultats attendus obtenus et les principaux difficultés concernaient la saisie correcte des commandes et l'utilisation des droits administrateur(sudo).

Les problems ont été résolus en vérifiant la syntaxe des commandes et en utilisant sudo lorsque necessaire.

## Démarche suivi: Créer une nouvelle VM

- Type : Linux
- Version :Debian 64 bits
- RAM :minimum 2 go
- Disque : minimum 20 go
- Démarrer avec l'ISO Kali Linux
- Choisir Graphical Install.