UNIVERSITÉ DE TÉCHNOLOGIE D'HAITI (UNITECH)

Faculté des Sciences de Génie,et d'Architecture

TD NoX-Sécurité informatique&Cybersécurité

NOM……..MAITRE

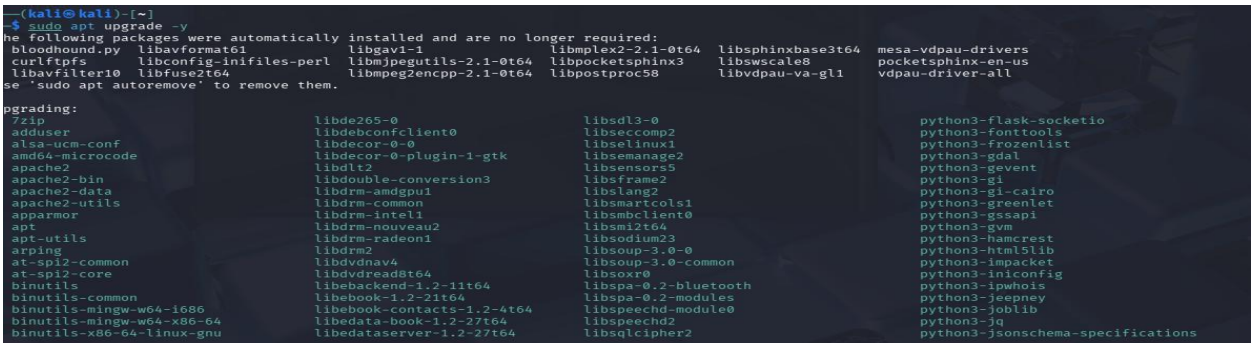
PRÉNOM…….Amourana

NIVEAU……2

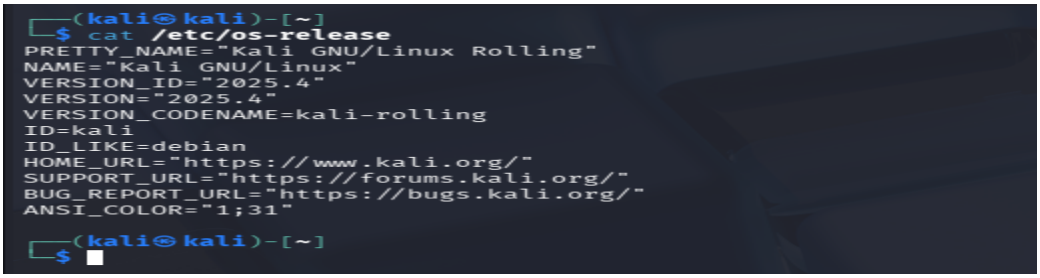
DATE…….le/20/01/25

Obdjectif du TD:

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



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



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 closed 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)-[~]
└─$
```

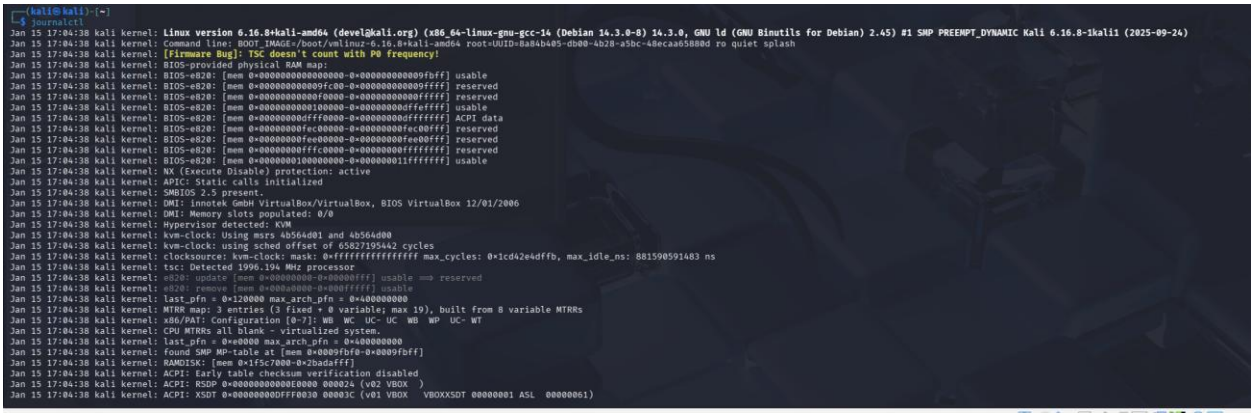
La commande jounalctl -n 10 permet d’afficher les 10 derniers messages des journaux systems.

```
┌──(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)-[~]
└─$
```

Date: Affiche la date et l’heur actuelles du système.

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

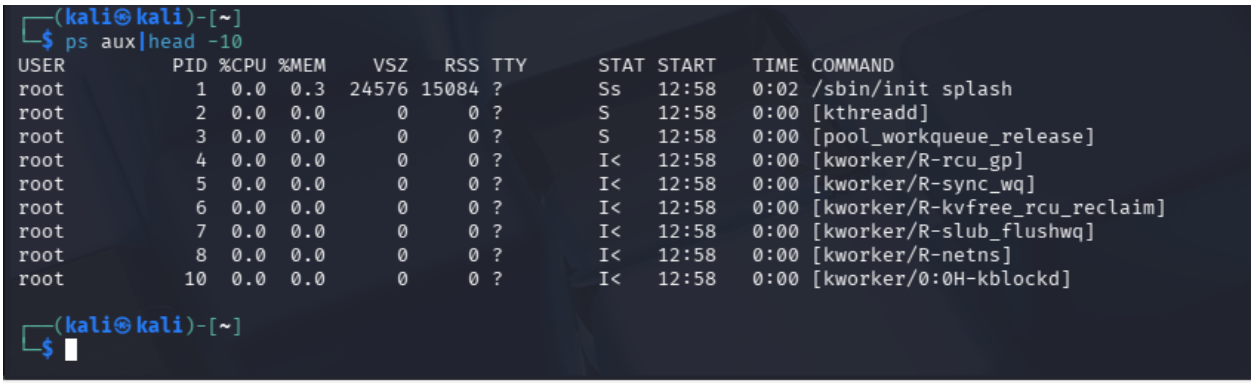
La commande jornalctl -b permet d’afficher les journaux du système depuis le dernier démarrage.



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

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

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

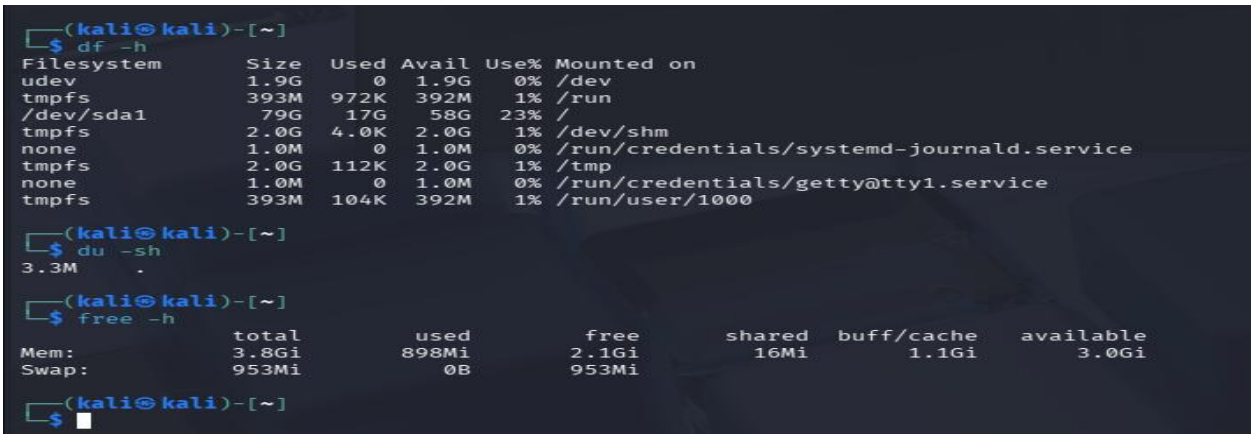


La command eps aux |head -10 permet d’afficher les 10 premiers processus enc ours d’exécution sur le système.

Lspci: liste tous les périphériques PCI de l’ordinateur

.

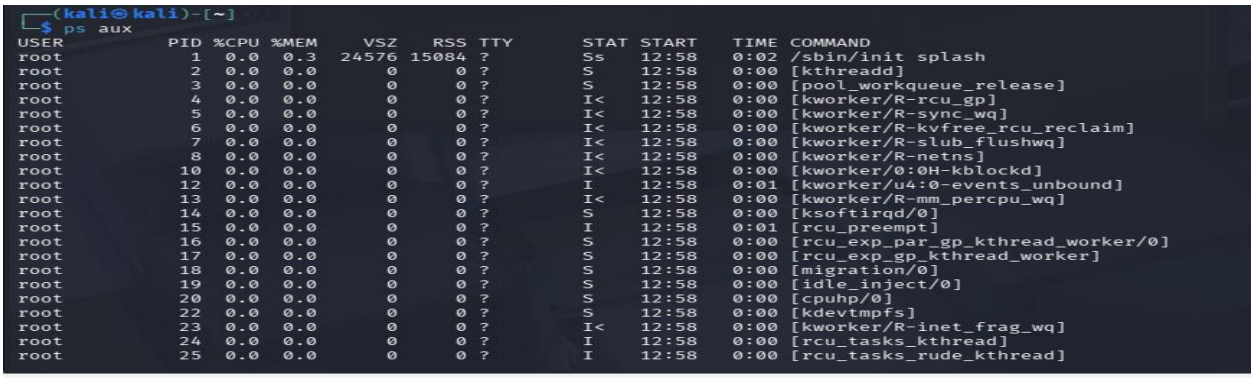
Lspci -v: Affiche les périphériques PCI avec plus de details.



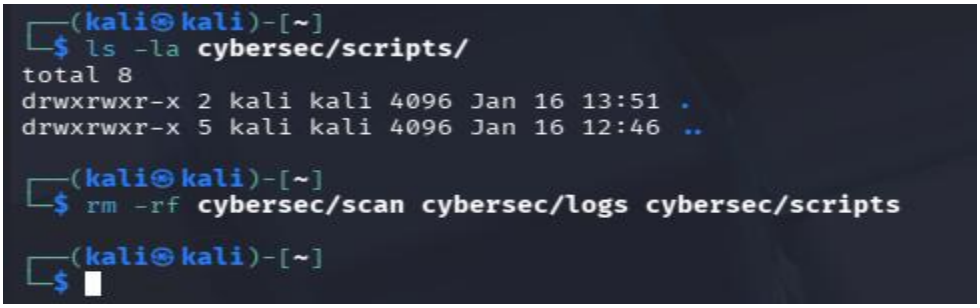
Df -h: Affiche l’espace disque disponible et utilize pour chaque partion, en format lisible.

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.



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



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)-[~]
└─$
```

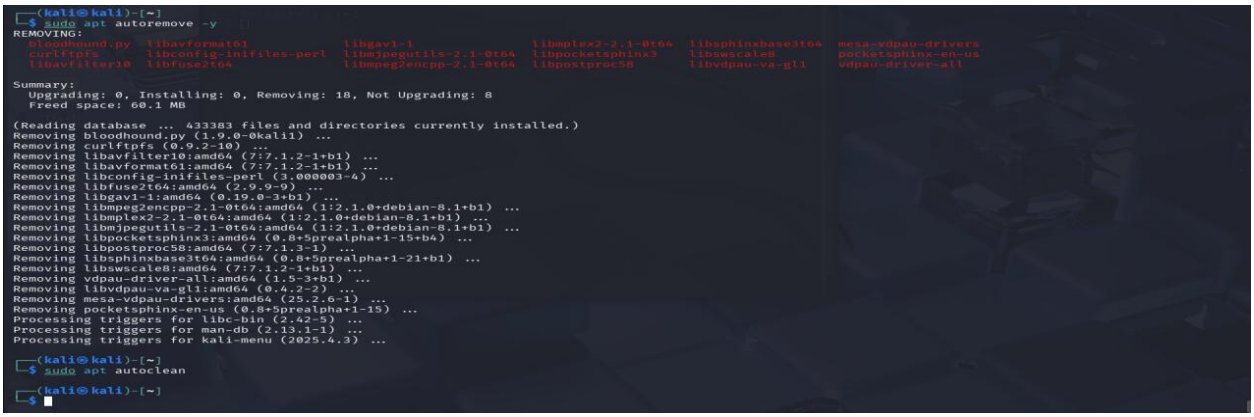
La commande ifconfig permet d’afficher et de configure les interfaces reseau sur le système linux.

```
┌──(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 sybersec/scan/notes.txt cybersec/scripts/
cp: cannot stat 'sybersec/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 ves le dossier cybersec/script.

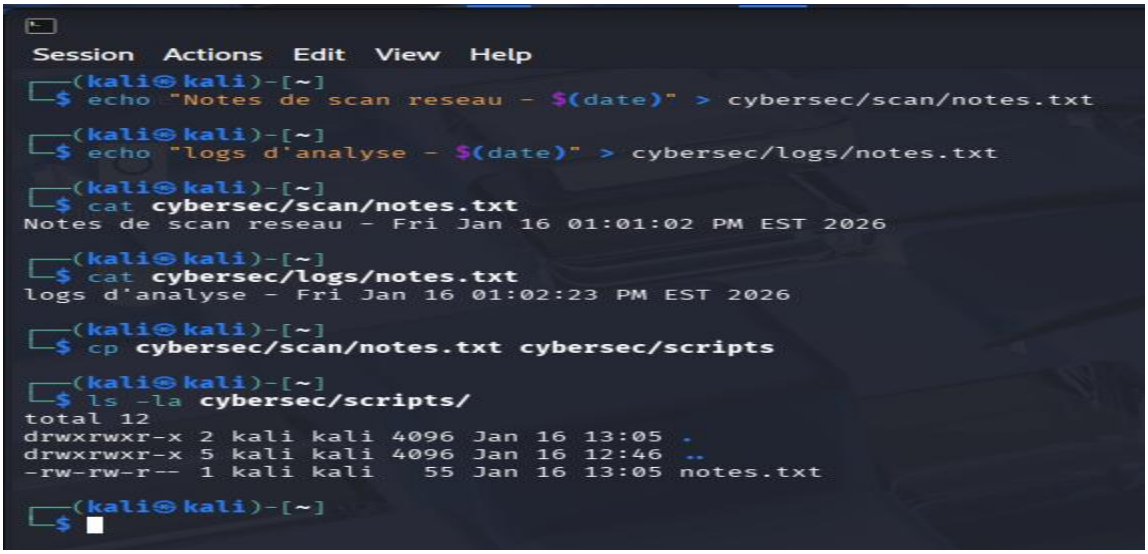
Ls -la cybersec/script/: Affiche tous les fichiers du dossier script,y compris les fichiers caches, avec leurs d”etails comples.

Cp: Premet de copier un fichier ou un dossier d’un emplacement vers un autre.

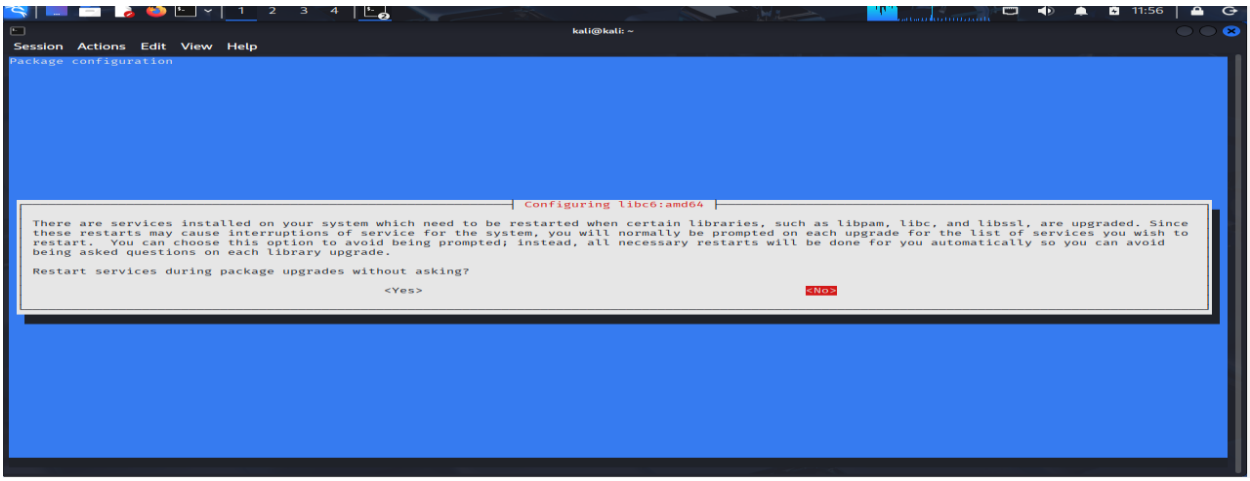


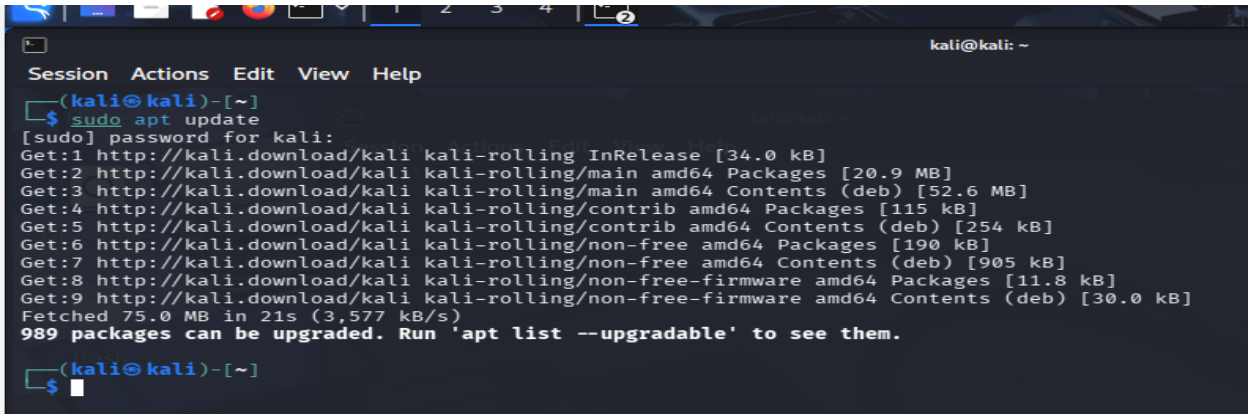
Sudo apt autoremove -y: Suprime automatiquement lrs paquets et dépendances inutilisés qui ne sont plus nécessaires sur le système.

Sudo apt autoclean: Suprime les fichiers de paquets téléchargés et obsolères pour libérer de l’espace disque.

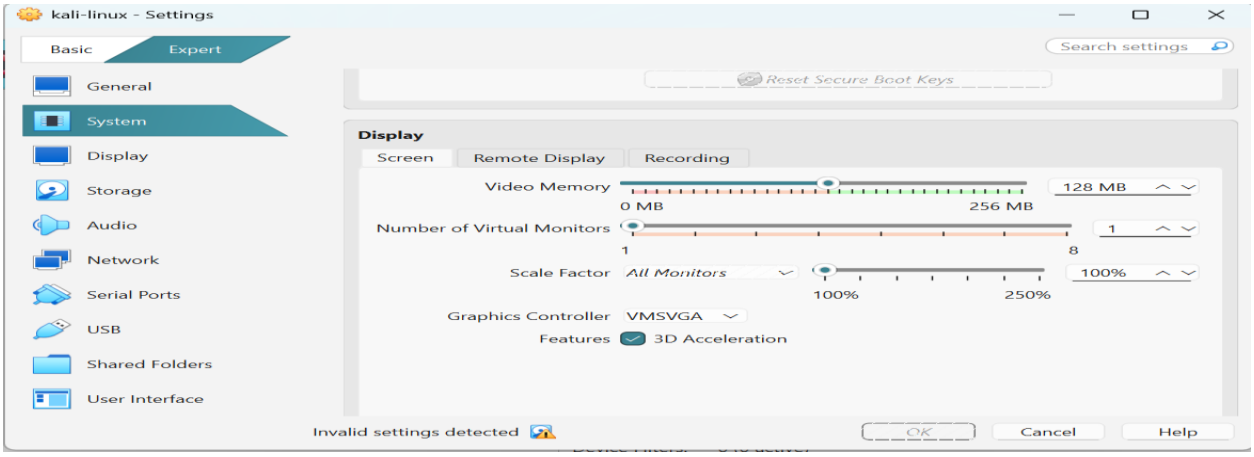


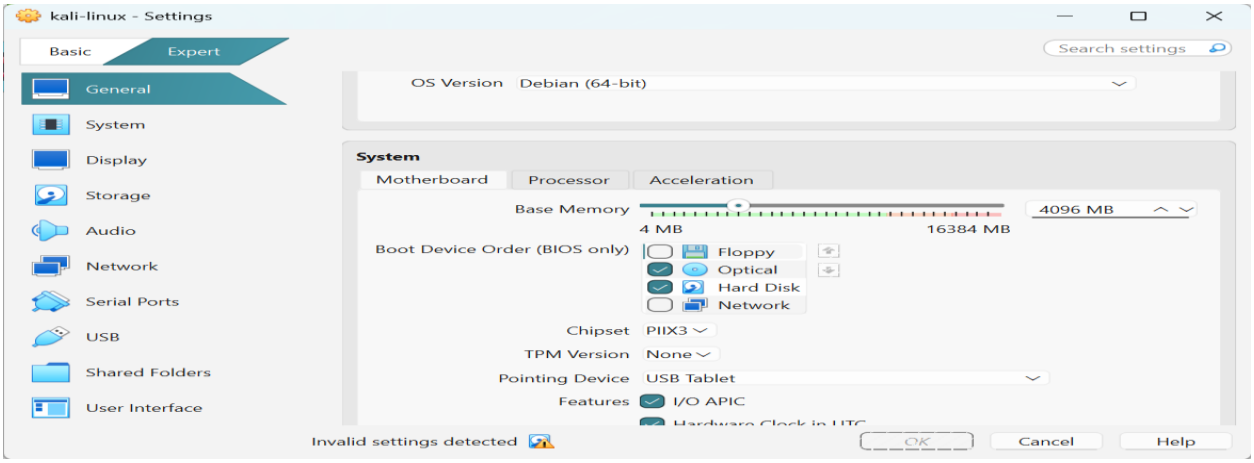
La commande echo permet d’afficher du texte ou des variables dans le terminal.

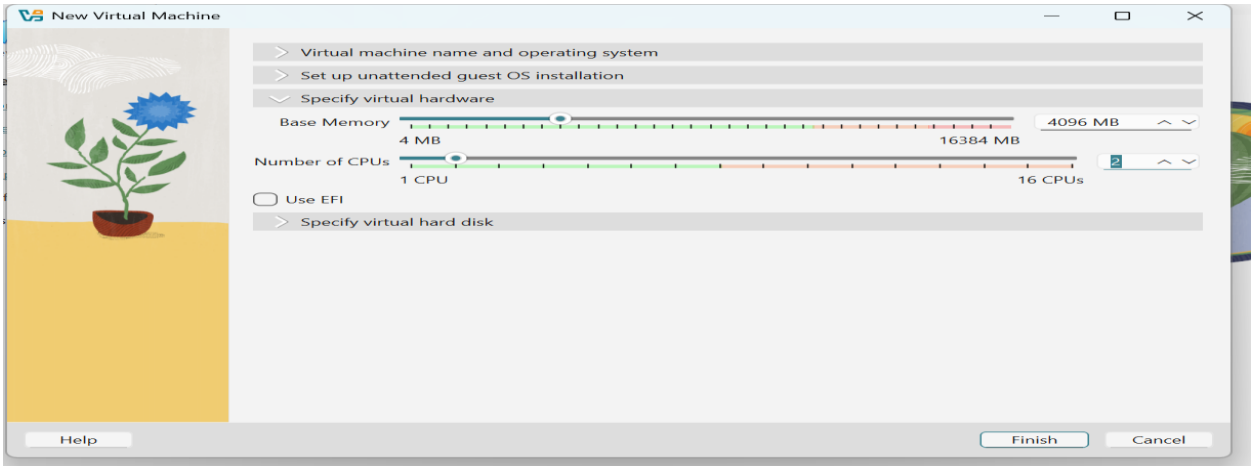


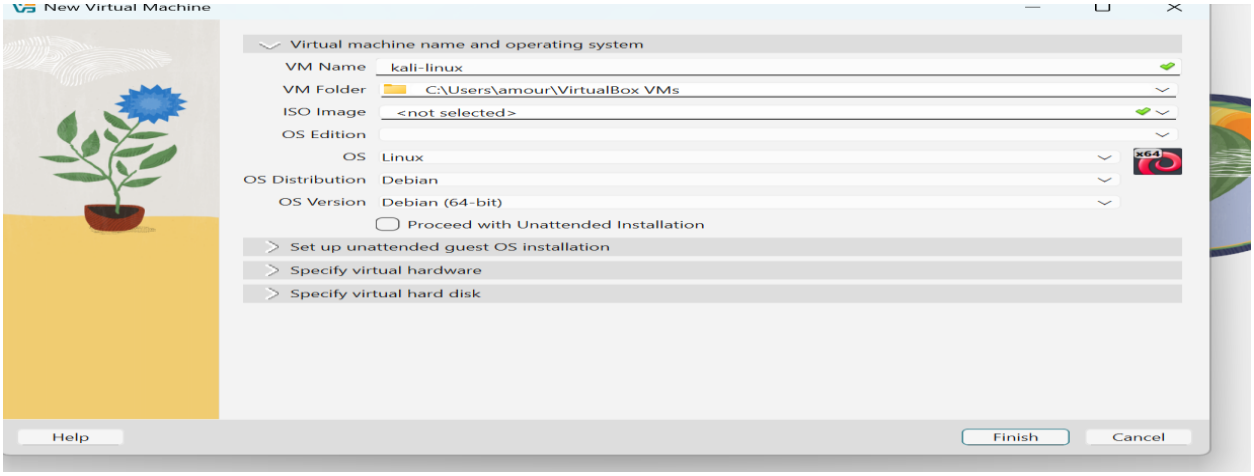


La commande sudo apt update permet de mettre à jour la liste des paquets disponibles sur le système linux.


kali-linux - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Reset Secure Boot Keys
Display
Screen
Remote Display
Recording
Video Memory
128 MB
0 MB
256 MB
Number of Virtual Monitors
1
1
8
Scale Factor
All Monitors
100%
100%
250%
Graphics Controller
VMSVGA
Features
3D Acceleration
Invalid settings detected
OK
Cancel
Help


kali-linux - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
OS Version
Debian (64-bit)
System
Motherboard
Processor
Acceleration
Base Memory
4096 MB
4 MB
16384 MB
Boot Device Order (BIOS only)
Floppy
Optical
Hard Disk
Network
Chipset
PIIX3
TPM Version
None
Pointing Device
USB Tablet
Features
I/O APIC
Invalid settings detected
OK
Cancel
Help


New Virtual Machine
Virtual machine name and operating system
Set up unattended guest OS installation
Specify virtual hardware
Base Memory
4096 MB
4 MB
16384 MB
Number of CPUs
2
1 CPU
16 CPUs
Use EFI
Specify virtual hard disk
Help
Finish
Cancel



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 principals dificultés 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 Lunix
- Choisir Graphical Install.