

Université de Technologie d'Haïti

Unitech

Sciences Informatiques

TD : Sécurité informatique et cybersécurité

Nom : AUGUSTE

Prénom : Melandecia

Niveau : IV

17/01/2026

1. CREEZ UNE NOUVELLE MACHINE VIRTUELLE DANS VIRTUALBOX OU VMWARE.

1. Guide de création (avec VMware)

1. **Lancer l'assistant** : Clique sur "Create a New Virtual Machine".
2. **Source d'installation** : Sélectionnez "Installer disc image file (iso)" et parcourez vos fichiers pour sélectionner l'image du système (Kali).
3. **Nom et Emplacement** : Donnez un nom à votre VM (Kali-pentest1) et choisissez le dossier de stockage.
4. **Configuration du disque** : Allouez une taille (minimum 20 Go recommandés). Sélectionnez "Split virtual disk into multiple files" pour de meilleures performances.
5. **Personnalisation matérielle** : Cliquez sur "Customize Hardware".
 - o **RAM** : Allouez au moins 4 Go.
 - o **Processeur** : Allouez 2 cœurs pour une navigation fluide.

2. RAPPORT DE CONFIGURATION VM

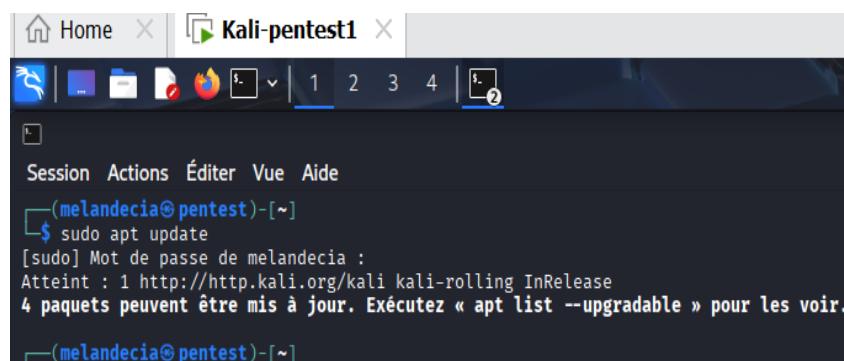
- Nom du projet : projet cybersec
- Date : 18 Janvier 2026
- Logiciel utilisé : VMware Workstation
- Composant Détails de la configuration

2.1 RAPPORT D'INSTALLATION (MODELE)

- ✓ Système Invité : Kali Linux / Windows 11
- ✓ Mémoire (RAM) : 4096 Mo]
- ✓ Processeurs : 2 cœurs]
- ✓ Disque Dur : 30 Go, Dynamique
- ✓ Réseau : NAT

3. METTEZ À JOUR LE SYSTÈME APRÈS L'INSTALLATION.

- sudo apt update
- sudo apt upgrade -y
- sudo apt dist-upgrade -y



```
Home X | Kali-pentest1 X | 
Session Actions Éditer Vue Aide
(melandecia@pentest)-[~]
$ sudo apt update
[sudo] Mot de passe de melandecia :
Atteint : 1 http://http.kali.org/kali kali-rolling InRelease
4 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.

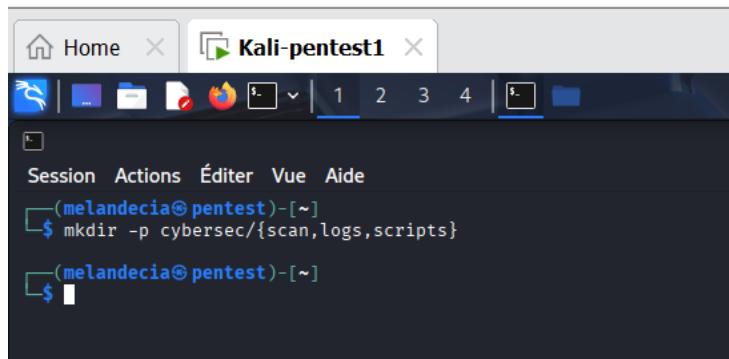
(melandecia@pentest)-[~]
```

- Ces commandes permettent de faire la mise à jour du système après l'installation

4. CREER UNE STRUCTURE DE DOSSIERS :

- CREEZ UN DOSSIER CYBERSEC AVEC TROIS SOUS-DOSSIERS : SCAN, LOGS, SCRIPTS

4.1- mkdir -p cybersec/{scan,logs,scripts}

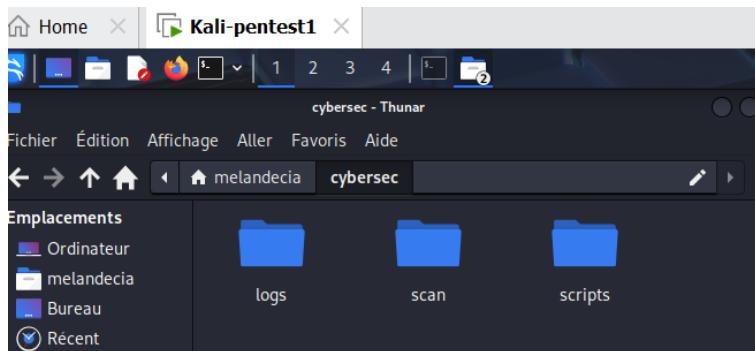


```
(melandecia㉿pentest)-[~]
$ mkdir -p cybersec/{scan,logs,scripts}

(melandecia㉿pentest)-[~]
```

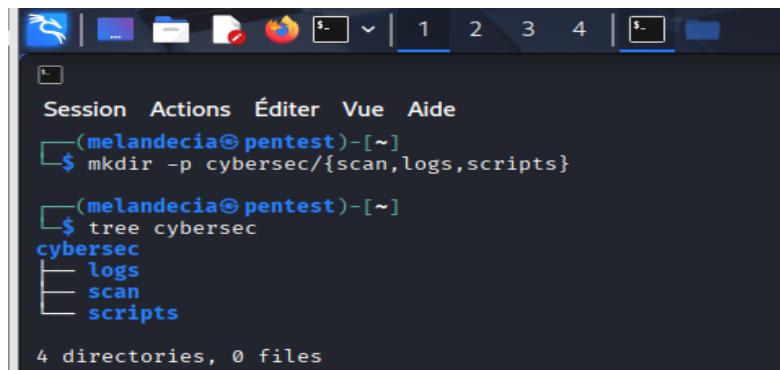
- Cette commande permet de créer un dossier avec des sous-dossiers.

4.2- Voici les dossiers et les sous-dossier qu'on a créé



5. AFFICHER LA STRUCTURE DU REPERTOIRE CYBERSEC AVEC TREE

- tree cybersec



```
(melandecia㉿pentest)-[~]
$ mkdir -p cybersec/{scan,logs,scripts}

(melandecia㉿pentest)-[~]
$ tree cybersec
cybersec
├── logs
└── scan
└── scripts

4 directories, 0 files
```

- Cette commande permet d'afficher la structure du répertoire sous forme d'un arbre.

6. AJOUTEZ UN FICHIER NOTES.TXT DANS SCAN ET LOGS

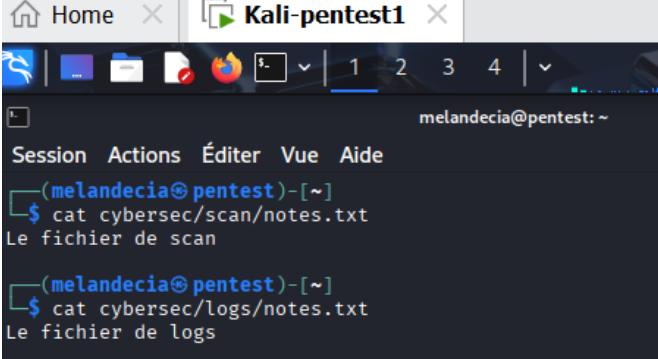
- echo "le fichier de scan " > cybersec/scan/notes.txt
- echo "Logs de sécurité" > cybersec/logs/notes.txt

```
4 directories, 0 files
└─(melandecia㉿pentest)-[~]
    $ echo "Le fichier de scan " > cybersec/scan/notes.txt
    └─(melandecia㉿pentest)-[~]
        $ echo "Le fichier de logs " > cybersec/logs/notes.txt
    └─(melandecia㉿pentest)-[~]
        └─█
```

- Ces commandes permettent d'ajouter un fichier dans SCAN et LOGS.

6.1 AFFICHEZ LE CONTENU DES FICHIERS.

- cat cybersec/scan/notes.txt
- cat cybersec/logs/notes.txt



```
Home | Kali-pentest1 | 1 2 3 4 | melandecia@pentest: ~
Session Actions Éditer Vue Aide
└─(melandecia㉿pentest)-[~]
    $ cat cybersec/scan/notes.txt
Le fichier de scan
└─(melandecia㉿pentest)-[~]
    $ cat cybersec/logs/notes.txt
Le fichier de logs
```

- Cela permet d'afficher le contenu des fichiers qu'on a déjà créé.

7. COPIEZ LE FICHIER (NOTES.TXT) DANS LE SOUS-DOSSIER SCRIPTS .

VERIFIER SI LE FICHIERS A ETE COPIE.

-cp cybersec/scan/notes.txt cybersec/scripts/

-VERIFICATION

- ls cybersec/scripts/
- cat cybersec/scripts/notes.txt

- Ces commandes permettent de copier le fichier dans le sous-dossier SCRIPTS et de vérifier si ce fichier a été copier

```
└─(melandecia㉿pentest)-[~]
$ cp cybersec/scan/notes.txt cybersec/scripts/
└─(melandecia㉿pentest)-[~]
$ ls cybersec/scripts/
notes.txt
└─(melandecia㉿pentest)-[~]
$ cat cybersec/scripts/notes.txt
Le fichier de scan
```

8. DEPLACEZ LE FICHIER (NOTES.TXT) DANS LE SOUS-DOSSIER SCAN, VERIFIER SI LE FICHIERS A ETE SUPPRIMER

-mv cybersec/scripts/notes.txt cybersec/scan/
-ls cybersec/scripts/

```
└─$ cat cybersec/scripts/notes.txt
Le fichier de scan

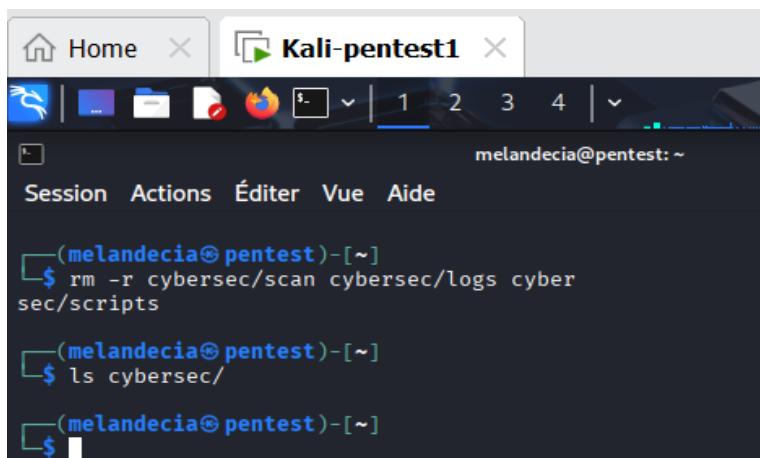
└─(melandecia㉿pentest)-[~]
$ mv cybersec/scripts/notes.txt cybersec/
scan/

└─(melandecia㉿pentest)-[~]
$ ls cybersec/scripts/
└─(melandecia㉿pentest)-[~]
```

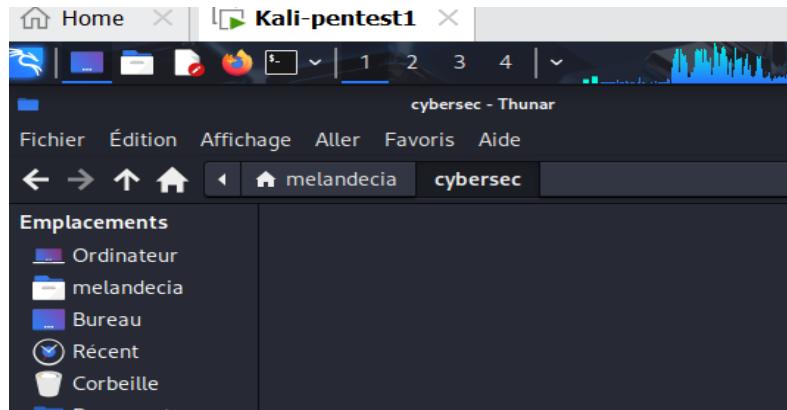
- Ces commandes permettent de déplacer le fichier qu'on avait créé et vérifier si le fichier a été supprimer.

9. SUPPRIMEZ LES SOUS-DOSSIERS : SCAN, LOGS, SCRIPTS. VERIFIER SI LES SOUS-DOSSIERS ONT ETE SUPPRIMES.

- rm -r cybersec/scan cybersec/logs cybersec/scripts
-ls cybersec/



- Ces commandes permettent de supprimer tous les sous dossiers qu'on avait créée, et de vérifier s'ils ont été supprimés.



- Cela nous montre que tous les fichiers ont été supprimés.

10. SCANNER UN RESEAU

- ifconfig ou ip a : affiche les informations réseau.

```

Session Actions Éditer Vue Aide
(melandecia㉿pentest)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5f:a7:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.176.132/24 brd 192.168.176.255 scope global dynamic noprefixroute eth0
        valid_lft 1673sec preferred_lft 1673sec
        inet6 fe80::20c:29ff:fe5f:a713/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

```

- Cette commande permet d'afficher tous les informations de ce réseau.

11. EXECUTER CES COMMANDES

- df -h : Affiche l'espace disque utilisé et disponible sur les systèmes de fichiers (format lisible)
- du -sh : Montre la taille totale d'un répertoire (-s pour sommaire, -h pour format lisible)
- free -h : Affiche la quantité de mémoire RAM utilisée et disponible (format lisible)
- ps aux : Liste tous les processus en cours d'exécution avec détails complets
- lspci : Liste tous les périphériques PCI (cartes réseau, graphiques, etc.)
- sudo apt install traceroute : Installe l'outil traceroute
- traceroute google.com : Trace le chemin des paquets vers une destination
- netstat -tuln : Affiche les connexions réseau et ports en écoute
- ss -tuln : Version moderne de netstat (plus rapide)
- journalctl : Affiche tous les journaux système (logs)
- journalctl -f : Affiche les logs en temps réel (follow)
- journalctl -b : Affiche les logs depuis le dernier démarrage
- journalctl -n 10 : Affiche les 10 dernières entrées de log
- date : Affiche la date et l'heure actuelles
- timedatectl : Affiche et permet de configurer le système de date/heure
- hostnamectl : Affiche le nom d'hôte et informations système
- sudo hostnamectl set-hostname [nouveau nom] : Modifie le nom d'hôte
- cat /etc/os-release : Affiche les informations sur la distribution Linux

- VOICI QUELQUES SCRENN DES COMMANDES QU'ON A DETAILLEE AU-DESSUS DU DOCUMENT.

```
(melandecia@pentest) ~]$ df -h
Sys. de fichiers Taille Utilisé Disp% Utile% Monté sur
udev          1,9G     0   1,9G   0% /dev
tmpfs        389M    1,2M  388M   1% /run
/dev/sda1      30G    18G   11G  62% /
tmpfs         1,9G   8,0K   1,9G   1% /dev/shm
none          1,0M     0   1,0M   0% /run/credentials/systemd-journald.service
tmpfs         1,9G   8,0K   1,9G   1% /tmp
none          1,0M     0   1,0M   0% /run/credentials/getty@tty1.service
tmpfs        389M   2,8M  386M   1% /run/user/1000

(melandecia@pentest) ~]$ du -sh
22M .

(melandecia@pentest) ~]$ free -h
              total        utilisé        libre      partagé  t/mpt/cache  disponible
Mem:       3,8Gi        991Mi       2,16i        15Mi      1,0Gi       2,8Gi
Échange:  1,7Gi          0B       1,7Gi

(melandecia@pentest) ~]$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  1,0  0,3 24876 15704 ?      Ss 19:50  0:05 /sbin/init splash
root        2  0,0  0,0     0     0 ?      S 19:50  0:00 [kthreadd]
root        3  0,0  0,0     0     0 ?      S 19:50  0:00 [pool_workqueue_release]
root        4  0,0  0,0     0     0 ?      I< 19:50  0:00 [kworker/R-rcu_gpl]
root        5  0,0  0,0     0     0 ?      I< 19:50  0:00 [kworker/R-sync_wq]
root        6  0,0  0,0     0     0 ?      I< 19:50  0:00 [kworker/R-kvfree_rcu_r
root        7  0,0  0,0     0     0 ?      I< 19:50  0:00 [kworker/R-slub_flushwa
```

```
File Edit View VM Tabs Help || Home Kali-pentest1 | 1 2 3 4 | melandecia@pentest: ~ Session Actions Éditer Vue Aide

└─(melandecia@pentest)-[~]
$ lspci
00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (rev 01)
00:01.0 PCI bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX AGP bridge (rev 01)
00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIx4 ISA (rev 08)
00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIx4 IDE (rev 01)
00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIx4 ACPI (rev 08)
00:07.7 System peripheral: VMware Virtual Machine Communication Interface (rev 10)
00:0f.0 VGA compatible controller: VMware SVGA II Adapter
00:10.0 SCSI storage controller: Broadcom / LSI 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI (rev 01)
00:11.0 PCI bridge: VMware PCI bridge (rev 02)
00:15.0 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.1 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.2 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.3 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.4 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.5 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.6 PCI bridge: VMware PCI Express Root Port (rev 01)
00:15.7 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.0 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.1 PCI bridge: VMware PCI Express Root Port (rev 01)
00:16.2 PCI bridge: VMware PCI Express Root Port (rev 01)
```

```
└─(melandecia@pentest)-[~]
$ traceroute google.com
traceroute to google.com (142.251.35.110), 30 hops max, 60 byte packets
 1  192.168.176.2 (192.168.176.2)  2.115 ms  1.979 ms  1.821 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  * * *
```

```
melandecia@pentest:~  
Session Actions Éditer Vue Aide  
[melandecia@pentest) ~]  
$ netstat -tuln  
Connexions Internet actives (seulement serveurs)  
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat  
tcp 0 0 0.0.0.0:41418 0.0.0.0:*  
[melandecia@pentest) ~]  
$ ss -tuln  
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port  
udp UNCONN 0 0 0.0.0.0:51518 0.0.0.0:  
[melandecia@pentest) ~]  
$ 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 13 09:47:55 pentest systemd[1227]: Queued start job for default target default.target.  
jan 13 09:47:56 pentest systemd[1227]: Created slice app.slice - User Application Slice.  
jan 13 09:47:56 pentest systemd[1227]: Created slice session.slice - User Core Session Slice.  
jan 13 09:47:56 pentest systemd[1227]: Reached target paths.target - Paths.  
jan 13 09:47:56 pentest systemd[1227]: Reached target timers.target - Timers.  
jan 13 09:47:56 pentest systemd[1227]: Starting dbus.socket - D-Bus User Message Bus Socket ...  
jan 13 09:47:56 pentest systemd[1227]: Listening on dimngr.socket - GnuPG network certificate management daemon.  
jan 13 09:47:56 pentest systemd[1227]: Starting gcr-ssh-agent.socket - GCR ssh-agent wrapper ...  
jan 13 09:47:56 pentest systemd[1227]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.  
jan 13 09:47:56 pentest systemd[1227]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers)  
jan 13 09:47:56 pentest systemd[1227]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).  
jan 13 09:47:56 pentest systemd[1227]: Starting gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation) ...  
jan 13 09:47:56 pentest systemd[1227]: Starting gpg-agent.socket - GnuPG cryptographic agent and passphrase cache ...
```

```
melandecia@pentest:~  
Session Actions Éditer Vue Aide  
[melandecia@pentest) ~]  
$ 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 19 14:35:58 pentest dbus-daemon[1231]: [session uid=1000 pid=1231 pidfd=5] Successfully activated service 'org.freedesktop.portal.  
jan 19 14:35:58 pentest systemd[1188]: Started xdg-desktop-portal.service - Portal service.  
jan 19 14:38:25 pentest systemd[1188]: tumblerd.service: Consumed 1.329s CPU time over 5min 9.051s wall clock time, 26.1M memory pe  
jan 19 14:46:56 pentest sudo[2182]: melandecia : TTY pts/0 ; PWD=/home/melandecia ; USER=root ; COMMAND=/usr/bin/apt install tracer  
jan 19 14:46:56 pentest sudo[2182]: pam_unix(sudo:session): session opened for user root(uid=0) by melandecia(uid=1000)  
jan 19 14:46:58 pentest sudo[2182]: pam_unix(sudo:session): session closed for user root  
jan 19 14:48:36 pentest dbus-daemon[1231]: [session uid=1000 pid=1231 pidfd=5] Activating via systemd: service name='org.xfce.Xfconf  
' requested by ':1.40' (uid=1000 pid=1490 comm="/usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-noti" label="unconfined")  
jan 19 14:48:36 pentest systemd[1188]: Starting xfconfd.service - Xfce configuration service ...  
jan 19 14:48:36 pentest dbus-daemon[1231]: [session uid=1000 pid=1231 pidfd=5] Successfully activated service 'org.xfce.Xfconf'  
jan 19 14:48:36 pentest systemd[1188]: Started xfconfd.service - Xfce configuration service.
```

```
[melandecia@pentest) ~]  
$ 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 19 14:35:58 pentest dbus-daemon[1231]: [session uid=1000 pid=1231 pidfd=5] Successfully activated service 'org.freedesktop.portal.  
jan 19 14:35:58 pentest systemd[1188]: Started xdg-desktop-portal.service - Portal service.  
jan 19 14:38:25 pentest systemd[1188]: tumblerd.service: Consumed 1.329s CPU time over 5min 9.051s wall clock time, 26.1M memory pe  
jan 19 14:46:56 pentest sudo[2182]: melandecia : TTY pts/0 ; PWD=/home/melandecia ; USER=root ; COMMAND=/usr/bin/apt install tracer  
jan 19 14:46:56 pentest sudo[2182]: pam_unix(sudo:session): session opened for user root(uid=0) by melandecia(uid=1000)  
jan 19 14:46:58 pentest sudo[2182]: pam_unix(sudo:session): session closed for user root  
jan 19 14:48:36 pentest dbus-daemon[1231]: [session uid=1000 pid=1231 pidfd=5] Activating via systemd: service name='org.xfce.Xfconf  
' requested by ':1.40' (uid=1000 pid=1490 comm="/usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-noti" label="unconfined")  
jan 19 14:48:36 pentest systemd[1188]: Starting xfconfd.service - Xfce configuration service ...  
jan 19 14:48:36 pentest dbus-daemon[1231]: [session uid=1000 pid=1231 pidfd=5] Successfully activated service 'org.xfce.Xfconf'  
jan 19 14:48:36 pentest systemd[1188]: Started xfconfd.service - Xfce configuration service.  
lines 1-10/10 (END)
```

```
(melandecia@pentest)@[~]
└─$ date
lun 19 jan 2026 15:00:03 EST

(melandecia@pentest)@[~]
└─$ timedatectl
      Local time: lun 2026-01-19 15:00:19 EST
      Universal time: lun 2026-01-19 20:00:19 UTC
            RTC time: lun 2026-01-19 20:00:17
        Time zone: America/Toronto (EST, -0500)
System clock synchronized: no
          NTP service: active
    RTC in local TZ: no

(melandecia@pentest)@[~]
└─$ hostnamectl
  Static hostname: pentest
            Icon name: computer-vm
           Chassis: vm ┌─
Chassis Asset Tag: No Asset Tag
      Machine ID: b0c1a6e128684c4cbb689a3efc107461
        Boot ID: 4f7a3891e15d4a93a11eae56aa67f6a6
      AF_VSOCK CID: 3378489107
Virtualization: vmware
Operating System: Kali GNU/Linux Rolling
      Kernel: Linux 6.18.3+kali+1-amd64
  Architecture: x86-64
Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
Hardware Version: None
```

CONCLUSION

Ce projet m'a permis de maîtriser les bases de l'administration système sous Kali Linux. J'ai surmonté des difficultés techniques significatives, notamment la configuration des dépôts APT qui était initialement défectueuse. Grâce à une méthodologie structurée et à la résolution de problèmes étape par étape, j'ai rétabli le fonctionnement du gestionnaire de paquets et pu exécuter l'ensemble des commandes demandées.

J'ai acquis des compétences pratiques en :

- Gestion des dépôts logiciels sous Kali Linux
- Manipulation de l'arborescence des fichiers et répertoires
- Utilisation des commandes système essentielles pour la cybersécurité
- Diagnostic et résolution de problèmes d'installation

Le système est maintenant opérationnel et prêt pour des exercices plus avancés en sécurité informatique. Cette expérience a renforcé ma capacité à travailler en environnement Linux, une compétence fondamentale dans le domaine de la cybersécurité.