

Université de Technologie d'Haïti
(UNITECH)

Faculté des Sciences, de Génie et d'Architecture



Préparé par: JEAN BAPTISTE Josette

Option : Sciences Informatiques

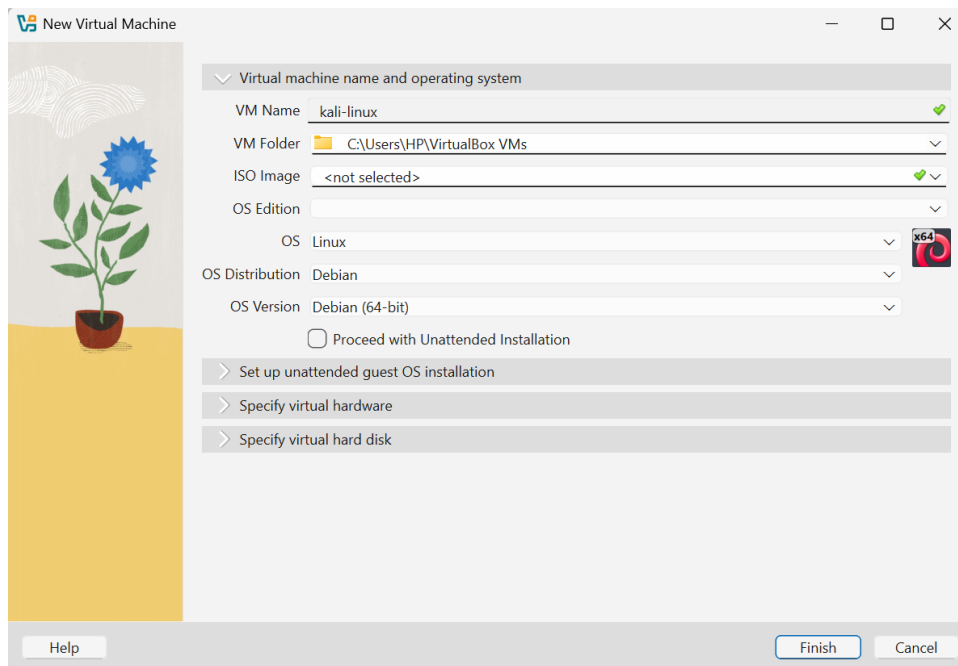
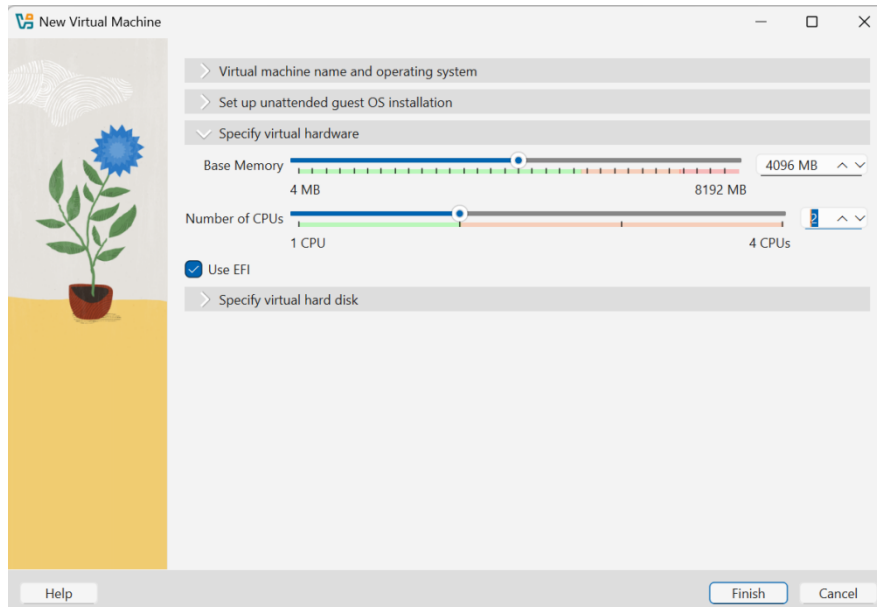
Niveau : III

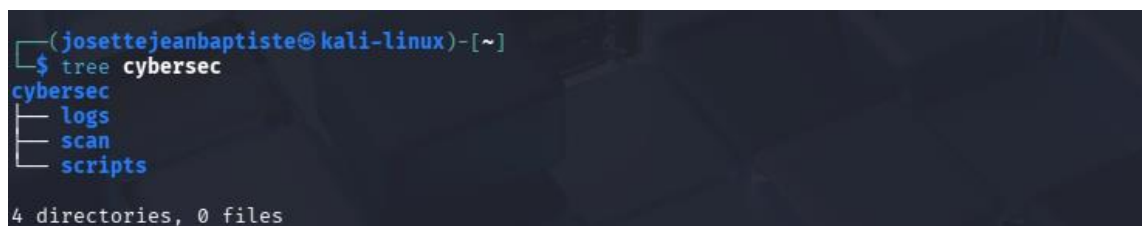
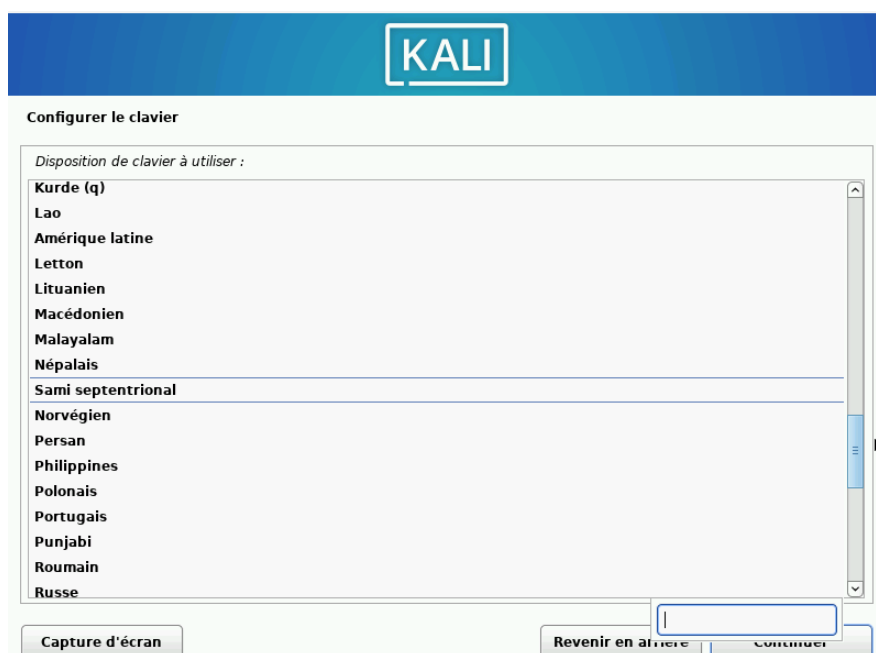
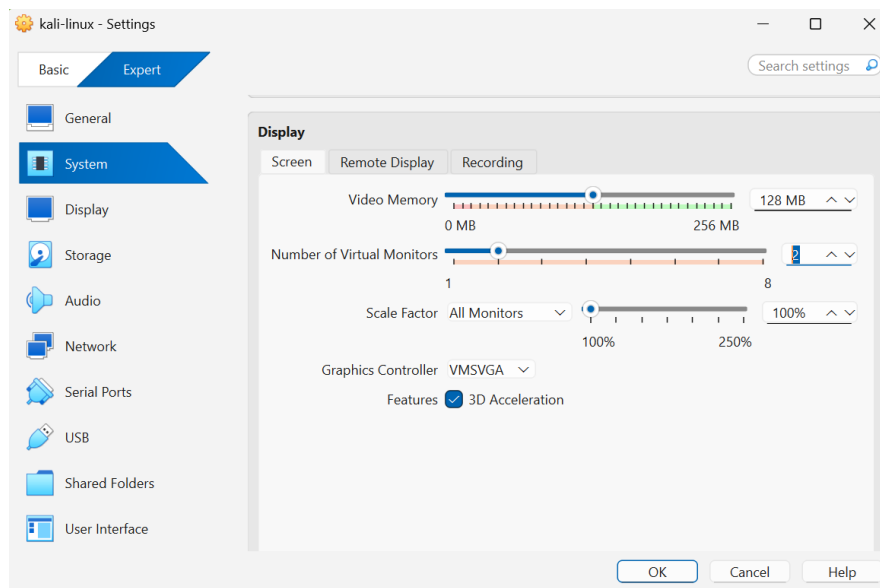
Devoir : TD N•X-Systèmes

Dispense par : Ismaël SAINT AMOUR

Le 20/01/2026

POUR KALI





```
(josettejeanbaptiste@kali-linux)-[~]  
$ echo "Notes de scan reseaux - $(date)" > cybersec/scan/notes.txt
```

```
(josettejeanbaptiste@kali-linux)-[~]  
$ echo "Logs d'analyse -$(date)" > cybersec/logs/notes.txt  
(josettejeanbaptiste@kali-linux)-[~]
```

cybersec/logs/notes.txt permet de trouver notes.txt dans le fichier logs qui se trouve dans cybersec.

```
$ echo "Logs d'analyse -$(date)" > cybersec/logs/notes.txt  
(josettejeanbaptiste@kali-linux)-[~]  
$ cat cybersec/scan/notes.txt  
Notes de scan reseaux - sam 17 jan 2026 01:06:24 EST  
Reseau  
(josettejeanbaptiste@kali-linux)-[~]  
$ cat cybersec/logs/notes.txt  
Logs d'analyse -sam 17 jan 2026 01:12:54 EST
```

La commande cat cybersec/scan/notes.txt permet de trouver notes.txt dans le fichier scan qui se trouve dans cybersec.

```

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

(josettejeanbaptiste@kali-linux)-[~]
$ ls -la cybersec/scripts
total 12
drwxrwxr-x 2 josettejeanbaptiste josettejeanbaptiste 4096 17 jan 01:20 .
drwxrwxr-x 5 josettejeanbaptiste josettejeanbaptiste 4096 17 jan 00:50 ..
-rw-rw-r-- 1 josettejeanbaptiste josettejeanbaptiste 54 17 jan 01:20 notes.txt

(josettejeanbaptiste@kali-linux)-[~]
$ rm cybersec/scan/notes.txt

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

(josettejeanbaptiste@kali-linux)-[~]
$ ls -la cybersec/scripts
total 8
drwxrwxr-x 2 josettejeanbaptiste josettejeanbaptiste 4096 17 jan 01:23 .
drwxrwxr-x 5 josettejeanbaptiste josettejeanbaptiste 4096 17 jan 00:50 ..

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

(josettejeanbaptiste@kali-linux)-[~]
$ ls -la cybersec
total 8
drwxrwxr-x 2 josettejeanbaptiste josettejeanbaptiste 4096 17 jan 01:24 .
drwx----- 17 josettejeanbaptiste josettejeanbaptiste 4096 17 jan 01:08 ..

```

La commande ls -l: permet d'afficher la liste détaillée des fichiers et dossiers présents dans un *répertoire*. Elle montre les permissions, le nombre de liens, le propriétaire, le groupe, la taille du fichier ainsi que la date de dernière modification.

Commande ls -l cybersec/scripts: Cette commande permet d'afficher le contenu détaillé du dossier scripts situé dans le répertoire cybersec. Elle montre les fichiers disponibles ainsi que leurs permissions et informations associées.

Commande ls -l cybersec/scan : Cette commande affiche les fichiers contenus dans le dossier scan du répertoire cybersec, notamment le fichier notes.txt, avec ses détails tels que la taille et la date de modification.

```

(josettejeanbaptiste@kali-linux)-[~]
$ 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 fd17:625c:f037:2:1b59:f897:811d:7e22 prefixlen 64 scopeid 0x0<global>
    inet6 fd17:625c:f037:2:a00:27ff:fe42:f954 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fe42:f954 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:42:f9:54 txqueuelen 1000 (Ethernet)
    RX packets 75 bytes 14434 (14.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 181 bytes 19482 (19.0 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 (Boucle locale)
    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

```

La commande ifconfig permet d'afficher les informations relatives aux interfaces réseau du système. Elle montre notamment les adresses IP, le masque réseau, l'adresse de diffusion

(broadcast) ainsi que les statistiques des paquets reçus (RX) et envoyés (TX). Cette commande est utile pour vérifier la configuration réseau d'une machine.

```
(josettejeanbaptiste@kali-linux)-[~]
$ 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 1
    link/ether 08:00:27:42:f9:54 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 82452sec preferred_lft 82452sec
    inet6 fd17:625c:f037:2:1b59:f897:811d:7e22/64 scope global temporary dynamic
        valid_lft 86328sec preferred_lft 14328sec
    inet6 fd17:625c:f037:2:a00:27ff:fe42:f954/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86328sec preferred_lft 14328sec
    inet6 fe80::a00:27ff:fe42:f954/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

LA COMMANDE *ip a* : La commande ip a (abréviation de ip address) est l'une des commandes les plus utilisées sous Kali Linux pour la gestion du réseau.

eth0 (Ethernet) : C'est ton interface réseau principale (souvent virtuelle sur VMware/VirtualBox).

```
(josettejeanbaptiste@kali-linux)-[~]
$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                1,9G   0   1,9G   0% /dev
tmpfs                392M   992K  391M   1% /run
/dev/sda1            28G    15G   13G  55% /
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   156K   2,0G   1% /tmp
none                 1,0M   0   1,0M   0% /run/credentials/getty@tty1.service
tmpfs                392M   112K  392M   1% /run/user/1000

(josettejeanbaptiste@kali-linux)-[~]
$ du -sh
2,0M .

(josettejeanbaptiste@kali-linux)-[~]
$ free -h
              total        used        libre    partagé  tamp/cache  disponible
Mem:          3,8Gi        801Mi        2,7Gi        6,8Mi        598Mi        3,0Gi
Échange:       1,6Gi           0B        1,6Gi
```

Commande *free -h* : free affiche l'état de la mémoire vive (RAM).

du : signifie Disk Usage (Utilisation du disque).

L'option -s : donne un résumé (total) et

-h : rend le résultat lisible pour un humain (en Ko, Mo ou Go).

```
(josettejeanbaptiste@kali-linux)-[~]
$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 24352 14808 ?        Ss   00:20   0:01 /sbin/init splash
root         2  0.0  0.0      0     0 ?        S    00:20   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    00:20   0:00 [pool_workqueue_release]
root         4  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-rcu_gp]
root         5  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-sync_wq]
root         6  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-kvfree_rcu_reclaim]
root         7  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-slub_flushwq]
root         8  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-netns]
root        10  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/0:0H-kblockd]
root        12  0.0  0.0      0     0 ?        I    00:20   0:00 [kworker/u4:0-ext4-rsv-conver]
root        13  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-mm_percpu_wq]
root        14  0.0  0.0      0     0 ?        S    00:20   0:00 [ksoftirqd/0]
root        15  0.0  0.0      0     0 ?        I    00:20   0:01 [rcu_preempt]
root        16  0.0  0.0      0     0 ?        S    00:20   0:00 [rcu_exp_par_gp_kthread_worke]
root        17  0.0  0.0      0     0 ?        S    00:20   0:00 [rcu_exp_gp_kthread_worker]
root        18  0.0  0.0      0     0 ?        S    00:20   0:00 [migration/0]
root        19  0.0  0.0      0     0 ?        S    00:20   0:00 [idle_inject/0]
root        20  0.0  0.0      0     0 ?        S    00:20   0:00 [cpuhp/0]
root        22  0.0  0.0      0     0 ?        S    00:20   0:00 [kdevtmpfs]
root        23  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-inet_frag_wq]
root        24  0.0  0.0      0     0 ?        I    00:20   0:00 [rcu_tasks_kthread]
root        25  0.0  0.0      0     0 ?        I    00:20   0:00 [rcu_tasks_rude_kthread]
root        26  0.0  0.0      0     0 ?        I    00:20   0:00 [rcu_tasks_trace_kthread]
root        27  0.0  0.0      0     0 ?        S    00:20   0:00 [kauditd]
root        28  0.0  0.0      0     0 ?        S    00:20   0:00 [khungtaskd]
root        29  0.0  0.0      0     0 ?        S    00:20   0:00 [oom_reaper]
root        32  0.0  0.0      0     0 ?        I<   00:20   0:00 [kworker/R-writeback]
```

Commande ps aux : Liste tous les programmes en cours d'exécution sur la machine, leur identifiant unique (PID) et leur consommation de ressources (%CPU et %MEM).

```
(josettejeanbaptiste@kali-linux)-[~]
$ 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 08)
00:0b.0 USB controller: Intel Corporation 82801FB/FB/FW/FRW (ICH6 Family) USB2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)
```

La commande lspci : Inventaire du matériel

La commande lspci (List PCI) est utilisée pour afficher des informations détaillées sur tous les bus PCI et les périphériques connectés à la carte mère de ton ordinateur.

```
(josettejeanbaptiste@kali-linux)-[~]
$ sudo apt install traceroute
[sudo] Mot de passe de josettejeanbaptiste :
traceroute est déjà la version la plus récente (1:2.1.6-1).
Sommaire :
Mise à niveau de : 0. Installation de : 0, Supprimé : 0. Non mis à jour : 0
```

La commande sudo apt me permet d'exécuter une tâche avec les privilèges d'administrateur. C'est pour cela que le système me demande mon mot de passe.

```
(josettejeanbaptiste@kali-linux)-[~]
$ traceroute google.com
```

La commande traceroute: est un outil de diagnostic réseau indispensable qui permet de suivre, étape par étape, le chemin qu'un paquet de données parcourt sur le réseau pour atteindre sa destination.

```
(josettejeanbaptiste@kali-linux)-[~]
$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat

(josettejeanbaptiste@kali-linux)-[~]
$ ss -tuln
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port

(josettejeanbaptiste@kali-linux)-[~]
$ journalctl
jan 17 00:20:35 kali-linux kernel: Linux version 6.16.8+kali-amd64 (devel@kali.org) (x86_64-lin>
jan 17 00:20:35 kali-linux kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.16.8+kali-amd64 roo>
jan 17 00:20:35 kali-linux kernel: BIOS-provided physical RAM map:
jan 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
```

La commande netstat -tuln : est un outil essentiel pour surveiller les connexions réseau et la sécurité de ton système Kali Linux.

La commande ss -tuln : est la version moderne et plus rapide de la commande netstat. Elle est utilisée pour afficher les statistiques des sockets réseau sur ton système Kali Linux.

La commande journalctl : est l'outil principal sous Kali Linux pour consulter les journaux (logs) du système. Elle permet d'accéder aux messages générés par le noyau Linux, les services et les applications.

```
(josettejeanbaptiste@kali-linux)-[~]
$ journalctl -f
jan 17 01:38:08 kali-linux xfce4-screensaver-dialog[39714]: pam_unix(xfce4-screensaver:account):
setuid failed: Opération non permise
jan 17 01:39:02 kali-linux CRON[40152]: pam_unix(cron:session): session opened for user root(uid
=0) by root(uid=0)
jan 17 01:39:02 kali-linux CRON[40154]: (root) CMD ( [ -x /usr/lib/php/sessionclean ] && if [ !
-d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
jan 17 01:39:02 kali-linux CRON[40152]: pam_unix(cron:session): session closed for user root
jan 17 01:39:15 kali-linux systemd[1]: Starting phpsessionclean.service - Clean php session file
s ...
jan 17 01:39:15 kali-linux systemd[1]: phpsessionclean.service: Deactivated successfully.
jan 17 01:39:15 kali-linux systemd[1]: Finished phpsessionclean.service - Clean php session file
s.
jan 17 01:45:01 kali-linux CRON[43128]: pam_unix(cron:session): session opened for user root(uid
=0) by root(uid=0)
jan 17 01:45:01 kali-linux CRON[43130]: (root) CMD (command -v debian-sa1 > /dev/null && debian-
sa1 1 1)
jan 17 01:45:01 kali-linux CRON[43128]: pam_unix(cron:session): session closed for user root
```

Commande journalctl -f : Affiche les logs en temps réel (pratique pour voir ce qui se passe pendant que tu lances une attaque ou un service).

```
—(josettejeanbaptiste@kali-linux)-[~]
$ journalctl -b
an 17 00:20:35 kali-linux kernel: Linux version 6.16.8+kali-amd64 (devel@kali.org) (x86_64-lin>
an 17 00:20:35 kali-linux kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.16.8+kali-amd64 roo>
an 17 00:20:35 kali-linux kernel: BIOS-provided physical RAM map:
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reser>
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000ffffff] reser>
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000000dffffff] usable
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x000000000dfff0000-0x000000000dfffffff] ACPI >
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reser>
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reser>
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reser>
an 17 00:20:35 kali-linux kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
an 17 00:20:35 kali-linux kernel: NX (Execute Disable) protection: active
an 17 00:20:35 kali-linux kernel: APIC: Static calls initialized
an 17 00:20:35 kali-linux kernel: SMBIOS 2.5 present.
```

journalctl -b -1 : Affiche les journaux du démarrage précédent.

```
(josettejeanbaptiste@kali-linux)-[~]
$ journalctl -n 10
jan 17 01:38:08 kali-linux xfce4-screensaver-dialog[39714]: pam_unix(xfce4-screensaver:account)>
jan 17 01:39:02 kali-linux CRON[40152]: pam_unix(cron:session): session opened for user root(ui>
jan 17 01:39:02 kali-linux CRON[40154]: (root) CMD ( [ -x /usr/lib/php/sessionclean ] && if [ >
jan 17 01:39:02 kali-linux CRON[40152]: pam_unix(cron:session): session closed for user root
jan 17 01:39:15 kali-linux systemd[1]: Starting phpsessionclean.service - Clean php session fil>
jan 17 01:39:15 kali-linux systemd[1]: phpsessionclean.service: Deactivated successfully.
jan 17 01:39:15 kali-linux systemd[1]: Finished phpsessionclean.service - Clean php session fil>
jan 17 01:45:01 kali-linux CRON[43128]: pam_unix(cron:session): session opened for user root(ui>
jan 17 01:45:01 kali-linux CRON[43130]: (root) CMD (command -v debian-sa1 > /dev/null && debian>
jan 17 01:45:01 kali-linux CRON[43128]: pam_unix(cron:session): session closed for user root
lines 1-10/10 (END)
```

La commande journalctl -n 10 : permet d'afficher les 10 dernières entrées du journal système. Elle facilite une analyse rapide des activités récentes du noyau et des services, permettant ainsi de repérer immédiatement d'éventuels dysfonctionnements survenus dans les dernières minutes d'utilisation.

```
(josettejeanbaptiste@kali-linux)-[~]
$ date
sam 17 jan 2026 01:51:21 EST

(josettejeanbaptiste@kali-linux)-[~]
$ timedatectl
Local time: sam 2026-01-17 01:51:50 EST
Universal time: sam 2026-01-17 06:51:50 UTC
RTC time: sam 2026-01-17 06:51:49
Time zone: America/Toronto (EST, -0500)
System clock synchronized: no
NTP service: inactive
RTC in local TZ: no
```

La commande date : Permet d'afficher l'heure et la date.

```
(josettejeanbaptiste@kali-linux)-[~]
$ hostnamectl
Static hostname: kali-linux
Icon name: computer-vm
Chassis: vm
Machine ID: ffb8e5fe1a77479091e340e79185c2cf
Boot ID: 1327ef49b15b419580ab629d2ac64b9e
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.16.8+kali-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 3d
```

La commande hostnamectl : est l'outil principal utilisé sous Kali Linux pour consulter et modifier l'identité du système. Elle regroupe plusieurs informations techniques en une seule vue.

```
(josettejeanbaptiste@kali-linux)-[~]  
$ 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` : est utilisée pour identifier précisément la version du système d'exploitation installée sur ta machine.

OBJECTIF DU TD

L'objectif principal de ce TD était de prendre en main la distribution kali linux en tant qu'environnement de travail pour la cybersécurité. Plus spécifiquement, les objectifs étaient les suivants :

- **Maitriser de l'Administration Système de Base.**
 - **Se familiariser avec le terminal.**
 - **Gérer les privilèges**
 - **Identifier l'environnement**

DEMARCHE SUIVIE

La mise en place de l'environnement de travail a suivi une progression logique, allant de l'installation système à la configuration d'outils de gestion de projet.

EN CONCLUSION

Ce travail dirigé m'a permis de mieux comprendre l'utilisation du terminal et l'importance des commandes systèmes dans un environnement linux. J'ai appris à exécuter des commandes de base et à analyser leurs résultats. La tâche demandée a été réalisée avec succès. Malgré les difficultés rencontrées lors de la prise en main du terminal, celles-ci ont été surmontées grâce à la pratique et à la consultation de la documentation. Ce TD a renforcé mes compétences en systèmes et m'a permis d'acquiescer de nouvelles connaissances utiles pour la suite de mes études.