

UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI

(UNITECH)

Faculté des Sciences de Génie et d'Architecture



Cours de Cybersécurité

TD No. 1- Systèmes

Nom & Prénom : Martchello Gaëthan Aimé

Niveau : II

Date : 16/01/2026

Plan

- | | |
|---|----------------|
| - Description des résultats de la tâche | page 3 |
| - Résultats de l'exécution des commandes | page 4 |
| - Conclusion | page 11 |

Description des résultats de la tâche

Titre : TD Cybersécurité - Prise en main de Kali Linux et commandes système

1. Objectif du TD

Ce TD avait pour objectif de me familiariser avec l'environnement Kali Linux, distribution spécialisée en cybersécurité, en réalisant plusieurs tâches pratiques :

- Installer et configurer une machine virtuelle Kali Linux
- Maîtriser les commandes fondamentales de gestion de fichiers et répertoires
- Explorer les commandes système pour la surveillance et l'administration
- Effectuer des analyses réseau de base

Comprendre la structure et le fonctionnement d'un système Linux dédié à la sécurité offensive

2. Démarche suivie

J'ai adopté une approche méthodique en suivant ces étapes :

Phase 1 : Installation et configuration

Création d'une machine virtuelle sous VirtualBox avec allocation de ressources adaptées (4GB RAM, 50GB stockage, 2 CPU)

Installation complète de Kali Linux via l'installateur graphique

Configuration des paramètres régionaux (langue française, fuseau horaire de Paris)

Création d'un utilisateur personnalisé avec mot de passe sécurisé

Mise à jour initiale du système via apt update && apt upgrade

Phase 2 : Manipulation du système de fichiers

- Création d'une arborescence structurée dans /home/martchellogaethanaime/cybersec/
- Utilisation des commandes « mkdir, tree, touch, echo » pour générer la structure demandée
- Pratique des opérations CRUD (Create, Read, Update, Delete) sur les fichiers
- Validation à chaque étape avec ls, cat, et vérification des chemins

Phase 3 : Exploration des commandes système

- Investigation réseau avec « ifconfig/ip a » pour identifier les interfaces
- Analyse des ressources système via « df -h, free -h, ps aux »

- Installation et utilisation d'outils de diagnostic réseau (traceroute)
- Consultation des journaux système avec « journalctl » et ses options
- Récupération d'informations système via « hostnamectl, cat /etc/os-release »

Phase 4 : Documentation et vérification

- Capture systématique des outputs des commandes
- Vérification de chaque opération avant passage à l'étape suivante
- Documentation des erreurs rencontrées et des solutions appliquées

3. Méthodologie de travail

J'ai travaillé selon le principe "test and learn" :

- Exécution de chaque commande demandée
- Analyse de la sortie produite
- Compréhension de l'utilité pratique en contexte cybersécurité
- Documentation des apprentissages pour référence future

Cette démarche progressive m'a permis de passer de la simple exécution de commandes à une compréhension de leur application réelle dans un contexte de sécurité informatique, tout en consolidant mes compétences en administration système Linux.

Résultats de l'exécution des commandes

```
martchelogaethanaime@kali-td:~$ sudo apt update
[sudo] Mot de passe de martchelogaethanaime :
Atteint : 1 http://http.kali.org/kali kali-rolling InRelease
Err : 1 http://http.kali.org/kali kali-rolling InRelease
  Sub-process /usr/bin/squ returned an error code (1), error message is: Verifying signature: Not live until 2026-01-16T11:34:38Z
980 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les détails
Attention : Une erreur s'est produite lors du contrôle de la signature. Le dépôt n'est pas mis à jour et les fichiers d'index précédents seront utilisés.
Échec de la vérification de signature OpenPGP : http://http.kali.org/kali kali-rolling InRelease : Sub-process /usr/bin/squ returned an error code (1), error message is: Verifying signature: Not live until 2026-01-16T11:34:38Z
Attention : Impossible de récupérer http://http.kali.org/kali/dists/kali-rolling/InRelease
Sub-process /usr/bin/squ returned an error code (1), error message is: Verifying signature: Not live until 2026-01-16T11:34:38Z
Attention : Le téléchargement de certains fichiers d'index a échoué, ils ont été ignorés, ou les anciens ont été utilisés à la place.

[martchelogaethanaime@kali-td:~]$ sudo apt upgrade -y
[sudo] Mot de passe de martchelogaethanaime :
Les packages suivants ont été installés automatiquement et ne sont plus nécessaires :
  aircrack
  bloodhound.py          libgav1-1           libspnbase3t64
  curlftpfs              libmpgutils-2.1-0t64   libswscale8
  libavfilter10           libmpeg2encpp-2.1-0t64  libvdpau-va-gli
```

I Mise à jour du système après installation sudo apt upgrade -y

```

Session Actions Éditer Vue Aide
Suppression de vpau-driver-all:amd64 (1.5-3+b1) ...
Suppression de libvpau-va-gl1:amd64 (0.4.2-2) ...
Suppression de mesa-vpau-drivers:amd64 (25.2.6-1) ...
Suppression de pocketphinx-en-us (0.8+5prealpha+1-15) ...
Traitement des actions différencées (« triggers ») pour libc-bin (2.42-5) ...
Traitement des actions différencées (« triggers ») pour man-db (2.13.1-1) ...
Traitement des actions différencées (« triggers ») pour kali-menu (2025.4.3) ...

(martchellogaethanaime㉿kali-td) [~]
$ sudo apt autoremove
(martchellogaethanaime㉿kali-td) [~]
$ cd ~
(martchellogaethanaime㉿kali-td) [~]
$ mkdir -p cybersec/{scan,logs,scripts}
(martchellogaethanaime㉿kali-td) [~]
$ tree cybersec
cybersec
├── logs
│   └── notes.txt
├── scan
│   └── notes.txt
└── scripts

4 directories, 0 files

(martchellogaethanaime㉿kali-td) [~]
$ echo "Logs d'analyse - $(date)" > cybersec/logs/notes.txt
(martchellogaethanaime㉿kali-td) [~]
$ echo "Notes de scan réseau - $(date)" > cybersec/scan/notes.txt
(martchellogaethanaime㉿kali-td) [~]
$ cat cybersec/logs/notes.txt
Logs d'analyse - Ven 16 jan 2026 13:40:21 EST
(martchellogaethanaime㉿kali-td) [~]
$ cat cybersec/scan/notes.txt
Notes de scan réseau - ven 16 jan 2026 13:41:06 EST
(martchellogaethanaime㉿kali-td) [~]
$ 

```

2 Création de fichiers notes et affichage de structure de dossiers avec tree

```

(martchellogaethanaime㉿kali-td) [~]
$ 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:a00:27ff:fe3c:4e97  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe3c:4e97  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:3c:4e:97  txqueuelen 1000  (Ethernet)
        RX packets 2101855  bytes 2800991277 (2.6 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 262995  bytes 16078710 (15.3 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  (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

```

3 Scan de réseau avec ifconfig

```
(martchellogaethanaime㉿kali-td)~]$ 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 08:00:27:3c:4e:97 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 81067sec preferred_lft 81067sec
    inet6 fd17:625c:f037:2:121:52be:a68f/64 scope global temporary dynamic
        valid_lft 86354sec preferred_lft 14354sec
    inet6 fd17:625c:f037:2:a00:27ff:fe3c:4e97/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86354sec preferred_lft 14354sec
    inet6 fe80::a00:27ff:fe3c:4e97/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

4 Scan de réseau avec ip a

```
(martchellogaethanaime㉿kali-td)~]$ df -h
Sys. de fichiers Taille Utilisé Dispo Utile Monté sur
udev          1,9G     0  1,9G   0% /dev
tmpfs         392M  1004K  391M   1% /run
/dev/sda1      28G   17G   11G  62% /
tmpfs         2,0G   4,0K   2,0G   1% /dev/shm
tmpfs         2,0G   6,4M   2,0G   1% /tmp
none          1,0M     0  1,0M   0% /run/credentials/getty@tty1.service
tmpfs         392M   108K  392M   1% /run/user/1000
none          1,0M     0  1,0M   0% /run/credentials/systemd-journald.service

(martchellogaethanaime㉿kali-td)~]$ du -sh
2,0M .

(martchellogaethanaime㉿kali-td)~]$ free -h
              total        utilisé        libre      partagé  tamp/cache  disponible
Mem:       3,8Gi        961Mi       425Mi       16Mi       2,8Gi       2,9Gi
Échange:  1,6Gi       700Ki       1,6Gi

(martchellogaethanaime㉿kali-td)~]$
```

5 Affichage des résultats de commandes pour Espace disque : df -h ; Taille du répertoire courant :du -sh ; Mémoire :free -h ;

```
(martchellogaethanaime㉿kali-td) [~]
$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1 0.2 0.3 25320 16036 ?        Ss  11:53 0:22 /usr/lib/systemd/systemd --system --deserialize=67 splash
root      2 0.0 0.0 0     0 ?        S   11:53 0:00 [kthreadd]
root      3 0.0 0.0 0     0 ?        S   11:53 0:00 [pool_workqueue_release]
root      4 0.0 0.0 0     0 ?        I<  11:53 0:00 [kworker/R-rcu_gp]
root      5 0.0 0.0 0     0 ?        I<  11:53 0:00 [kworker/R-sync_wq]
root      6 0.0 0.0 0     0 ?        I<  11:53 0:00 [kworker/R-kvfree_rcu_reclaim]
root      7 0.0 0.0 0     0 ?        I<  11:53 0:00 [kworker/R-slab_flushwq]
root      8 0.0 0.0 0     0 ?        I<  11:53 0:00 [kworker/R-netsns]
root      13 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-mg-percpu_wq]
root      14 0.0 0.0 0     0 ?       S   11:53 0:00 [ksoftirqd/0]
root      15 0.0 0.0 0     0 ?       I   11:53 0:00 [rcu_preempt]
root      16 0.0 0.0 0     0 ?       S   11:53 0:00 [rcu_exp_par_gp_kthread_worker/0]
root      17 0.0 0.0 0     0 ?       S   11:53 0:00 [rcu_exp_gp_kthread_worker]
root      18 0.0 0.0 0     0 ?       S   11:53 0:00 [migration/0]
root      19 0.0 0.0 0     0 ?       S   11:53 0:00 [idle_inject/0]
root      20 0.0 0.0 0     0 ?       S   11:53 0:00 [cpuhp/0]
root      22 0.0 0.0 0     0 ?       S   11:53 0:00 [kdevtmpfs]
root      23 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-inet_frag_wq]
root      24 0.0 0.0 0     0 ?       I   11:53 0:00 [rcu_tasks_kthread]
root      25 0.0 0.0 0     0 ?       I   11:53 0:00 [rcu_tasks_rude_kthread]
root      26 0.0 0.0 0     0 ?       I   11:53 0:00 [rcu_tasks_trace_kthread]
root      27 0.0 0.0 0     0 ?       S   11:53 0:00 [kaudittd]
root      28 0.0 0.0 0     0 ?       S   11:53 0:00 [hungtaskd]
root      29 0.0 0.0 0     0 ?       S   11:53 0:00 [oom_reaper]
root      32 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-writeback]
root      33 0.0 0.0 0     0 ?       S   11:53 0:01 [kcompactd0]
root      34 0.0 0.0 0     0 ?       SN  11:53 0:00 [ksmd]
root      35 0.0 0.0 0     0 ?       SN  11:53 0:00 [khugepaged]
root      36 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-kblockd]
root      37 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-blkcg_punt_bio]
root      38 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-kintegrityd]
root      39 0.0 0.0 0     0 ?       S   11:53 0:00 [irq/9-acpi]
root      40 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-tpm_dev_wq]
root      41 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-edac-poller]
root      42 0.0 0.0 0     0 ?       I<  11:53 0:00 [kworker/R-devfreq_wq]
```

6 La ligne de commande « ps aux » nous permet d'afficher tous les processus

```
(martchellogaethanaime㉿kali-td) [~]
$ 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/FBM/FR/FW/FRW (ICH6 Family) USB2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/BEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)

(martchellogaethanaime㉿kali-td) [~]
$ lspci -v
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
Flags: fast devsel

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 0170 [size=8]
I/O ports at 0374
I/O ports at d000 [size=16]
Kernel driver in use: ata_piix
```

7 "lspci" nous permet de voir tous les périphériques PCI

```

martchellogaethanaime@kali-td:~$ sudo apt install traceroute -y
[sudo] Mot de passe pour martchellogaethanaime :
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 : 8

(martchellogaethanaime@kali-td) ~]$ traceroute google.com
traceroute to google.com (142.250.217.174), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  1.693 ms  1.641 ms  78.636 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  * * *

(martchellogaethanaime@kali-td) ~]$ 

```

8 Cette ligne de commande permet d'installer la dernière version de traceroute et traceroute google.com trace la route vers google.com

```

(martchellogaethanaime@kali-td) ~]$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale           Adresse distante         Etat
udp    0      0 0.0.0.0:4500                0.0.0.0:*               ESTABLISHED
udp    0      0 0.0.0.0:500                 0.0.0.0:*
udp6   0      0 ::1:4500                  ::*:*
udp6   0      0 ::1:500                   ::*:*

(martchellogaethanaime@kali-td) ~]$ ss -tuln
Netid      State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
udp        UNCONN     0           0           0.0.0.0:4500            0.0.0.0:*
udp        UNCONN     0           0           0.0.0.0:500             0.0.0.0:*
udp        UNCONN     0           0           [::]:4500              [::]:*
udp        UNCONN     0           0           [::]:500               [::]:*

(martchellogaethanaime@kali-td) ~]$ 

```

9 netstat -tuln et ss -tuln font la même chose, à savoir ouvrir les ports

```

(martchellogaethanaime@kali-td) ~]$ journalctl
jan 16 11:53:13 kali-td kernel: Linux version 6.16.8+kali-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.3.0-8) 14.3.0, GNU ld (GNU Binutils fo
jan 16 11:53:13 kali-td kernel: Linux version 6.16.8+kali-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.3.0-8) 14.3.0, GNU ld (GNU Binutils fo
jan 16 11:53:13 kali-td kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.16.8+kali-amd64 root=UUID=9589eb4e-8cd6-42ab-b9e9-33f7bbbf3ff2 ro quiet splash
jan 16 11:53:13 kali-td kernel: BIOS-provided physical RAM map:
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000009fbfff] usable
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x000000000009fc00-0x00000000009ffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000ffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dfffffff] usable
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x000000000fec0000-0x00000000fec00fff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fffffc] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000010000000-0x000000011fffffff] usable
jan 16 11:53:13 kali-td kernel: NX (Execute Disable) protection: active
jan 16 11:53:13 kali-td kernel: APIC: Static calls initialized
jan 16 11:53:13 kali-td kernel: SMBIOS 2.5 present.
jan 16 11:53:13 kali-td kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006

```

10 journalctl affiche tous les journaux, il faut faire ctrl+c pour pouvoir recommencer à utiliser le terminal

```
(martchellogaethanaime㉿kali-td) [~]
└$ journalctl -f
jan 16 14:15:01 kali-td CRON[113800]: pam_unix(cron:session): session closed for user root
jan 16 14:17:01 kali-td CRON[114776]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
jan 16 14:17:01 kali-td CRON[114778]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
jan 16 14:17:01 kali-td CRON[114776]: pam_unix(cron:session): session closed for user root
jan 16 14:17:44 kali-td sudo[115115]: martchellogaethanaime : TTY pts/0 ; PWD=/home/martchellogaethanaime ; USER=root ; COMMAND=/usr/bin/apt install traceroute -y
jan 16 14:17:44 kali-td sudo[115115]: pam_unix(sudo:session): session opened for user root(uid=0) by martchellogaethanaime(uid=1000)
jan 16 14:17:45 kali-td sudo[115115]: pam_unix(sudo:session): session closed for user root
jan 16 14:25:01 kali-td CRON[118766]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
jan 16 14:25:01 kali-td CRON[118768]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
jan 16 14:25:01 kali-td CRON[118766]: pam_unix(cron:session): session closed for user root
```

11 journalctl -f permet de faire un suivi des journaux en temps réel

```
(martchellogaethanaime㉿kali-td) [~]
└$ journalctl -b
jan 16 11:53:13 kali-td kernel: Linux version 6.16.8+kali-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.3.0-8) 14.3.0, GNU ld (GNU Binutils for Debian) 2.40.1) #1 SMP PREEMPT_DYNAMIC Debian 6.16.8+kali-amd64 root=UUID=9589eb4e-8cd6-42ab-b9e9-33f7bbbf3ff2 ro quiet splash
jan 16 11:53:13 kali-td kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.16.8+kali-amd64 root=UUID=9589eb4e-8cd6-42ab-b9e9-33f7bbbf3ff2 ro quiet splash
jan 16 11:53:13 kali-td kernel: BIOS-provided physical RAM map:
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000009fbfff] usable
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000f0000-0x0000000000ffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000100000-0x000000000dfffffff] usable
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000fec0000-0x000000000fec00ffff] ACPI data
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000fe00000-0x000000000fe00ffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000fee0000-0x000000000fee00ffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000000fffc0000-0x000000000fffcffff] reserved
jan 16 11:53:13 kali-td kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011fffffff] usable
jan 16 11:53:13 kali-td kernel: NX (Execute Disable) protection: active
jan 16 11:53:13 kali-td kernel: APIC: Static calls initialized
jan 16 11:53:13 kali-td kernel: SMBIOS 2.5 present.
jan 16 11:53:13 kali-td kernel: DMI: innoteck GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
jan 16 11:53:13 kali-td kernel: DMI: Memory slots populated: 0/0
jan 16 11:53:13 kali-td kernel: Hypervisor detected: KVM
jan 16 11:53:13 kali-td kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
jan 16 11:53:13 kali-td kernel: kvm-clock: using sched offset of 15437803865 cycles
jan 16 11:53:13 kali-td kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dff, max_idle_ns: 881590591483 ns
jan 16 11:53:13 kali-td kernel: tsc: Detected 2400.002 MHz processor
```

12 journalctl -b permet d'afficher les journaux de démarrage actuel

```
(martchellogaethanaime㉿kali-td) [~]
└$ journalctl -n 10
jan 16 14:15:01 kali-td CRON[113800]: pam_unix(cron:session): session closed for user root
jan 16 14:17:01 kali-td CRON[114776]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
jan 16 14:17:01 kali-td CRON[114778]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
jan 16 14:17:01 kali-td CRON[114776]: pam_unix(cron:session): session closed for user root
jan 16 14:17:44 kali-td sudo[115115]: martchellogaethanaime : TTY pts/0 ; PWD=/home/martchellogaethanaime ; USER=root ; COMMAND=/usr/bin/apt install traceroute
jan 16 14:17:44 kali-td sudo[115115]: pam_unix(sudo:session): session opened for user root(uid=0) by martchellogaethanaime(uid=1000)
jan 16 14:17:45 kali-td sudo[115115]: pam_unix(sudo:session): session closed for user root
jan 16 14:25:01 kali-td CRON[118766]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
jan 16 14:25:01 kali-td CRON[118768]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
jan 16 14:25:01 kali-td CRON[118766]: pam_unix(cron:session): session closed for user root
lines 1-10/10 (END)
```

13 journalctl -n 10 permet d'afficher seulement les 10 dernières lignes du journal

```
(martchellogaethanaime㉿kali-td)~]
└─$ date
ven 16 jan 2026 14:32:30 EST

(martchellogaethanaime㉿kali-td)~]
└─$ timedatectl
    Local time: ven 2026-01-16 14:33:28 EST
    Universal time: ven 2026-01-16 19:33:28 UTC
        RTC time: ven 2026-01-16 19:33:28
       Time zone: America/Toronto (EST, -0500)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no

(martchellogaethanaime㉿kali-td)~]
└─$ hostnamectl
  Static hostname: kali-td
            Icon name: computer-vm
      Chassis: vm
   Machine ID: fefadd11af646eba93243a5dfa8c1e7
      Boot ID: 1274d62844e6451faf6c361b54f6eb0b
  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 2d

(martchellogaethanaime㉿kali-td)~]
└─$
```

14 "date" permet d'afficher la date et l'heure actuelle, "timedatectl" permet d'avoir un contrôle du temps, « hostnamectl » nous donne les informations du système

```
(martchellogaethanaime㉿kali-td)~]
└─$ sudo hostnamectl set-hostname itachi-Kali-TD
[sudo] Mot de passe de martchellogaethanaime :

(martchellogaethanaime㉿kali-td)~]
└─$
```

15 On peut changer les informations du système via la commande hostnamectl avec les attributs set-hostname

```
(martchellogaethanaime㉿kali-td)~]
└─$ 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"

(martchellogaethanaime㉿kali-td)~]
└─$
```

16 Cette commande permet de vérifier la version OS

Conclusion

Résultats obtenus et apprentissages

Cette séance de travaux pratiques a été entièrement réussie sur tous les plans. J'ai pu maîtriser les notions suivantes :

- Installation et configuration : Installation complète de Kali Linux dans un environnement virtualisé fonctionnel
- Maîtrise des commandes : Acquisition solide des commandes fondamentales de gestion de fichiers (mkdir, cp, mv, rm, tree)
- Surveillance système : Exploration approfondie des outils de diagnostic (df, free, ps, journalctl)
- Analyse réseau : Premiers pas en investigation réseau avec ifconfig, ip a, et traceroute

Compétences acquises

Administration système Linux : Gestion des utilisateurs, mise à jour via apt, consultation des journaux

Orientation cybersécurité : Compréhension de l'utilité pratique de chaque commande dans un contexte de sécurité

Méthodologie de travail : Approche structurée "test and learn" applicable à d'autres outils techniques

Dépannage autonome : Capacité à diagnostiquer et résoudre des problèmes courants

Difficultés rencontrées et solutions

Difficultés techniques :

- Virtualisation désactivée : Activation du VT-x dans le BIOS
- Installation longue de Kali : Patience et vérification des ressources allouées
- Liste interminable avec les commandes de journal : J'ai découvert qu'il fallait faire CTRL + c pour stopper le processus et pouvoir recommencer à passer des commandes dans le terminal.

Applications concrètes en cybersécurité

tree : Cartographie des structures de fichiers pour audits de sécurité

journalctl : Analyse des logs pour détection d'intrusions

ps aux : Surveillance des processus malveillants

ss -tuln : Identification des ports ouverts et services exposés

traceroute : Analyse du chemin réseau pour investigations

Perspectives d'amélioration

Pour approfondir ces compétences, je pourrais :

Automatiser les tâches répétitives avec des scripts Bash

Explorer les outils offensifs de Kali (Metasploit, nmap, Wireshark)

Mettre en pratique dans des scénarios de pentesting basiques

Documenter mes propres procédures pour référence future

Bilan final

Ce TD a constitué une excellente introduction pratique à Kali Linux et à l'administration système orientée sécurité. La transition réussie entre la théorie des commandes et leur application concrète valide l'acquisition de compétences fondamentales pour la suite du cursus en cybersécurité.

Taux de réussite : 100% des objectifs atteints

Niveau de maîtrise : Opérationnel sur les bases, prêt pour les sujets avancés

Principale réalisation : Installation autonome d'un environnement de travail complet pour la sécurité offensive