Universite De Technologie D'haiti

(UNITECH)

Faculte des sciences et Genies d'architectures

Matiere : Cybersecurite

Nom : EXILIEN

Prenom : Wedson

Professeur : Ismael SAINT AMOUR

Objectif :

Ce TD est conçu pour permettre la virtualisation de Kali Linux et l'apprentissage des premières commandes est de vous familiariser avec l'environnement Kali Linux, de comprendre les bases de la virtualisation, et de maîtriser les commandes essentielles pour naviguer et interagir avec un système Linux.

Description des résultats de la tâche :

Création de la machine virtuelle et installation de Kali Linux :

Une nouvelle machine virtuelle a été configurée et Kali Linux a été installé avec succès via l'interface graphique.

Le système est pleinement fonctionnel après un redémarrage, prêt pour l'exécution des tâches.

Mise à jour du système :

La commande sudo apt update && sudo apt upgrade -y a permis de mettre à jour les paquets du système vers leurs dernières versions, garantissant ainsi la sécurité et la stabilité.

Création de la structure de dossiers :

Le dossier principal cybersec a été créé avec trois sous-dossiers : scan, logs, et scripts.

Deux fichiers notes.txt ont été créés dans les sous-dossiers scan et logs avec du contenu spécifique ajouté.

Le contenu des fichiers a été affiché avec succès, confirmant l'exactitude des informations.

Le fichier notes.txt a été copié correctement du dossier scan vers scripts, puis déplacé dans scan après vérification.

La suppression du fichier notes.txt dans scripts a été validée, montrant qu'il n'existe plus.

Enfin, les trois sous-dossiers ont été supprimés avec succès, confirmant un nettoyage complet de la structure.

Scan du réseau :

Les informations réseau locales ont été récupérées via ifconfig ou ip a, fournissant les adresses IP et les interfaces réseau.

Le scan du réseau local à l’aide de nmap a permis d’identifier les appareils connectés et d’afficher leurs adresses IP, les ports ouverts, et d'autres informations utiles.

Manipulation de fichiers et gestion des processus :

Les commandes grep, cat et echo ont permis de manipuler et d’afficher le contenu des fichiers.

La liste des processus en cours a été affichée avec ps aux, et un processus spécifique a pu être terminé à l’aide de la commande kill.

Gestion des permissions :

Un fichier secret.txt a été créé et ses permissions ont été modifiées pour être uniquement lisibles par le propriétaire (chmod 400).

Créez un dossier cybersec avec trois sous-dossiers : scan , logs , scripts

Ajoutez un fichier notes.txt dans scan et logs .

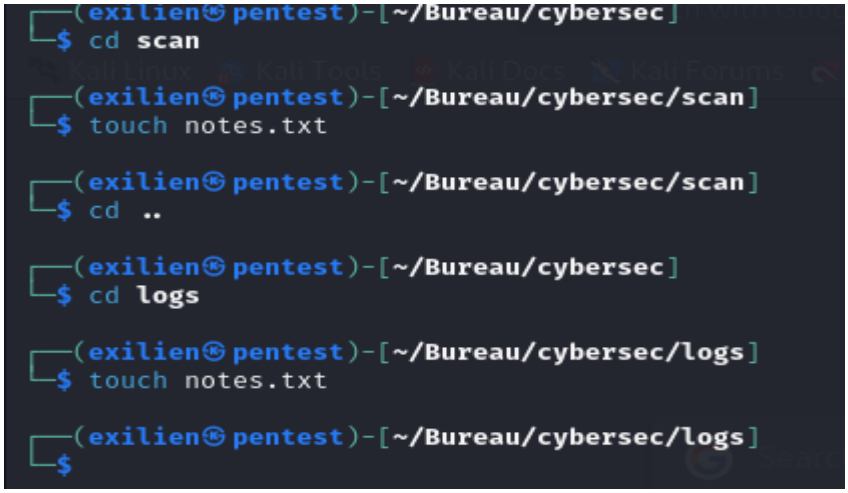
```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ git clone https://github.com/Exilien10/cybersec.git
Clonage dans 'cybersec' ...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Réception d'objets: 100% (3/3), fait.
```

```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ mkdir -p cybersec/scan

┌──(exilien㉿pentest)-[~/Bureau]
└─$ mkdir -p cybersec/logs

┌──(exilien㉿pentest)-[~/Bureau]
└─$ mkdir -p cybersec/scripts

┌──(exilien㉿pentest)-[~/Bureau]
└─$ ls -l ~/Bureau/cybersec/
total 16
drwxrwxr-x 2 exilien exilien 4096 16 fév 12:35 logs
-rw-rw-r-- 1 exilien exilien   39 16 fév 12:31 README.md
drwxrwxr-x 2 exilien exilien 4096 16 fév 12:35 scan
drwxrwxr-x 2 exilien exilien 4096 16 fév 12:36 scripts

┌──(exilien㉿pentest)-[~/Bureau]
└─$
```

Ajoutez du contenu dans les fichiers textes (notes.txt), puis affichez le contenu des fichiers.

Copiez le fichier (notes.txt) dans le sous-dossier scripts .

vérifier si le fichiers a été copié.



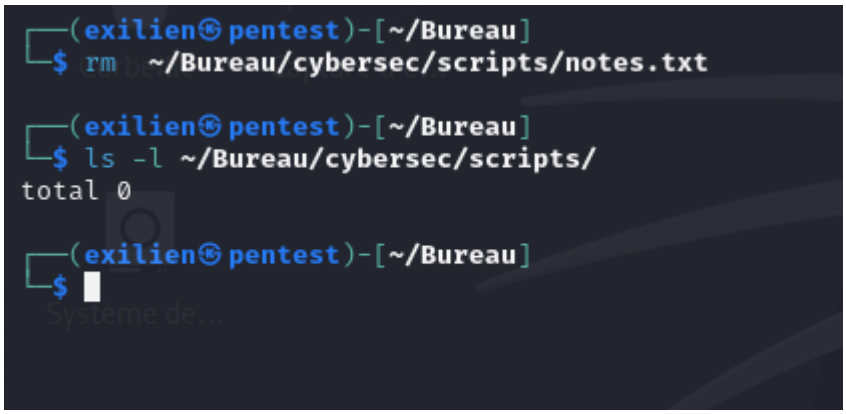
Déplacez le fichier (notes.txt) dans le sous-dossier scan .

```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ echo "ceci est un document ."> ~/Bureau/cybersec/scan/notes.txt

┌──(exilien㉿pentest)-[~/Bureau]
└─$ echo "voici mon dossier ."> ~/Bureau/cybersec/logs/notes.txt

┌──(exilien㉿pentest)-[~/Bureau]
└─$ cat ~/Bureau/cybersec/scan/
cat: /home/exilien/Bureau/cybersec/scan/: est un dossier

┌──(exilien㉿pentest)-[~/Bureau]
└─$ cat ~/Bureau/cybersec/scan/notes.txt
ceci est un document .

┌──(exilien㉿pentest)-[~/Bureau]
└─$ cat ~/Bureau/cybersec/logs/notes.txt
voici mon dossier .

┌──(exilien㉿pentest)-[~/Bureau]
└─$
```

```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ cp ~/Bureau/cybersec/scan/notes.txt ~/Bureau/cybersec/scripts/

┌──(exilien㉿pentest)-[~/Bureau]
└─$ ls -l ~/Bureau/cybersec/scripts/
total 4
-rw-rw-r-- 1 exilien exilien 23 16 fév 13:07 notes.txt

┌──(exilien㉿pentest)-[~/Bureau]
└─$
```

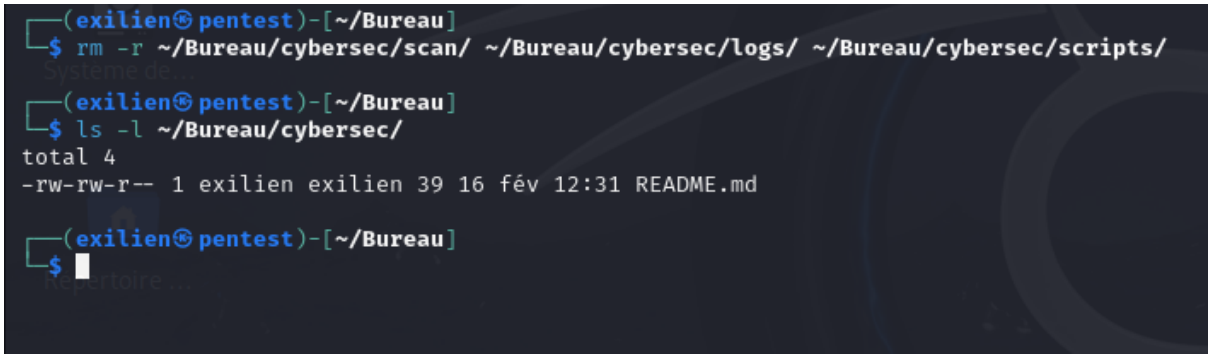
Supprimez le fichier (notes.txt)dans le sous-dossier scripts .

vérifier si le fichiers a été supprimé.



Supprimez les sous-dossiers : scan , logs , scripts.

vérifier si les sous-dossiers ont été supprimés.



ifconfig ou ip a : Affiche les informations réseau.

```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ 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:e2:29:5f 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 81986sec preferred_lft 81986sec
    inet6 fe80::a00:27ff:fee2:295f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(exilien㉿pentest)-[~/Bureau]
└─$
```

Utilisez nmap pour scanner votre réseau local et identifier les appareils connectés.

```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ nmap 10.0.2.15/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 13:33 EST
Nmap scan report for 10.0.2.2
Host is up (0.021s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
5357/tcp open  wsdapi
5560/tcp open  isqlplus
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.016s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
5357/tcp open  wsdapi
5560/tcp open  isqlplus
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.020s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
```

```
Nmap scan report for 10.0.2.4
Host is up (0.020s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
5357/tcp open  wsdapi
5560/tcp open  isqlplus
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.000085s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 12.06 seconds

┌──(exilien㉿pentest)-[~/Bureau]
└─$
```

Créez un fichier secret.txt et changez ses permissions pour qu'il ne soit accessible qu'en lecture par le propriétaire.

```
┌──(exilien㉿pentest)-[~/Bureau]
└─$ cd cybersec

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ touch secret.txt

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ chmod 400 ~/bureau/cybersec/secret.txt
chmod: impossible d'accéder à '/home/exilien/bureau/cybersec/secret.txt': Aucun fichier ou dossier de ce nom

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ chmod 400 ~/Bureau/cybersec/secret.txt

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ ls -l ~/Bureau/cybersec/secret.txt
-r-------- 1 exilien exilien 0 16 fév 13:41 /home/exilien/Bureau/cybersec/secret.txt

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

Créez un fichier log.txt avec des lignes de texte, puis utilisez grep pour rechercher un mot spécifique.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ touch logs.txt

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ echo "utilisation d'un mot ."> ~/Bureau/cybersec/logs.txt

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ echo "voila le mot qu'on a cherchar .">> ~/Bureau/cybersec/logs.txt

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ grep "mot" ~/Bureau/cybersec/logs.txt
utilisation d'un mot .
voila le mot qu'on a cherchar .

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

`df` : Affiche l'utilisation de l'espace disque.

`-h` : Affiche les informations dans un format lisible par l'humain (**h** pour "human-readable"), c'est-à-dire en Go, Mo, etc., au lieu de blocs en octets.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                926M       0  926M   0% /dev
tmpfs               198M   1008K  197M   1% /run
/dev/sda1            30G     14G   15G  49% /
tmpfs               988M    4,0K  988M   1% /dev/shm
tmpfs               5,0M       0  5,0M   0% /run/lock
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-journald.service
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-sysctl.service
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs               988M    8,0K  988M   1% /tmp
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs               1,0M       0  1,0M   0% /run/credentials/getty@tty1.service
tmpfs               198M    116K  198M   1% /run/user/1000

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

`du` : Signifie Disk Usage (utilisation du disque).
`-s` : Résumé (summary) – Affiche uniquement le total, sans détailler les sous-dossiers.

`-h` : Format lisible par l'humain (**h** pour "human-readable"), comme Ko, Mo, Go, etc.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ du -sh
200K    .

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ free -h
               total        utilisé      libre     partagé tamp/cache   disponible
Mem:           1,9Gi       714Mi       751Mi        12Mi       662Mi       1,2Gi
Échange:       1,7Gi          0B       1,7Gi
```

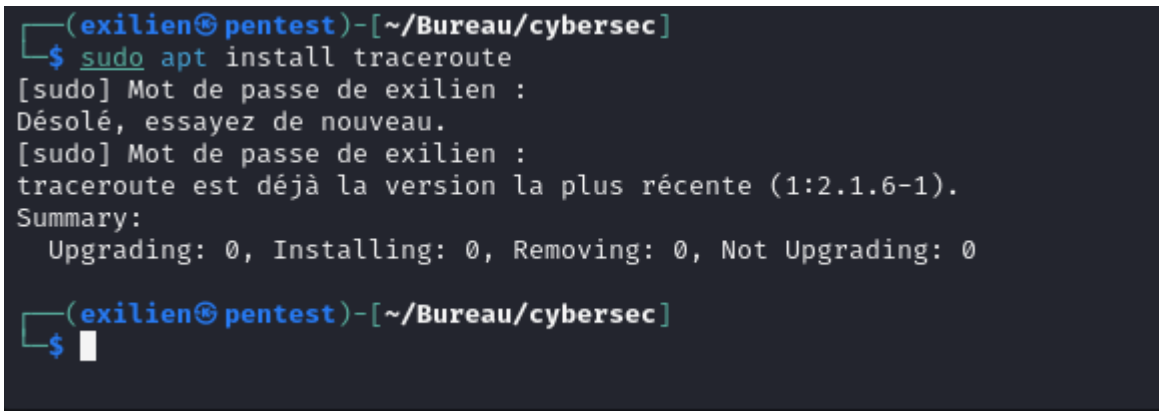
La commande **`ps aux`** sous Linux est utilisée pour afficher la liste des processus en cours d'exécution sur le système.

La commande **`lspci`** est utilisée pour lister les périphériques connectés au bus PCI de votre système (cartes graphiques, cartes réseau, contrôleurs USB, etc.).

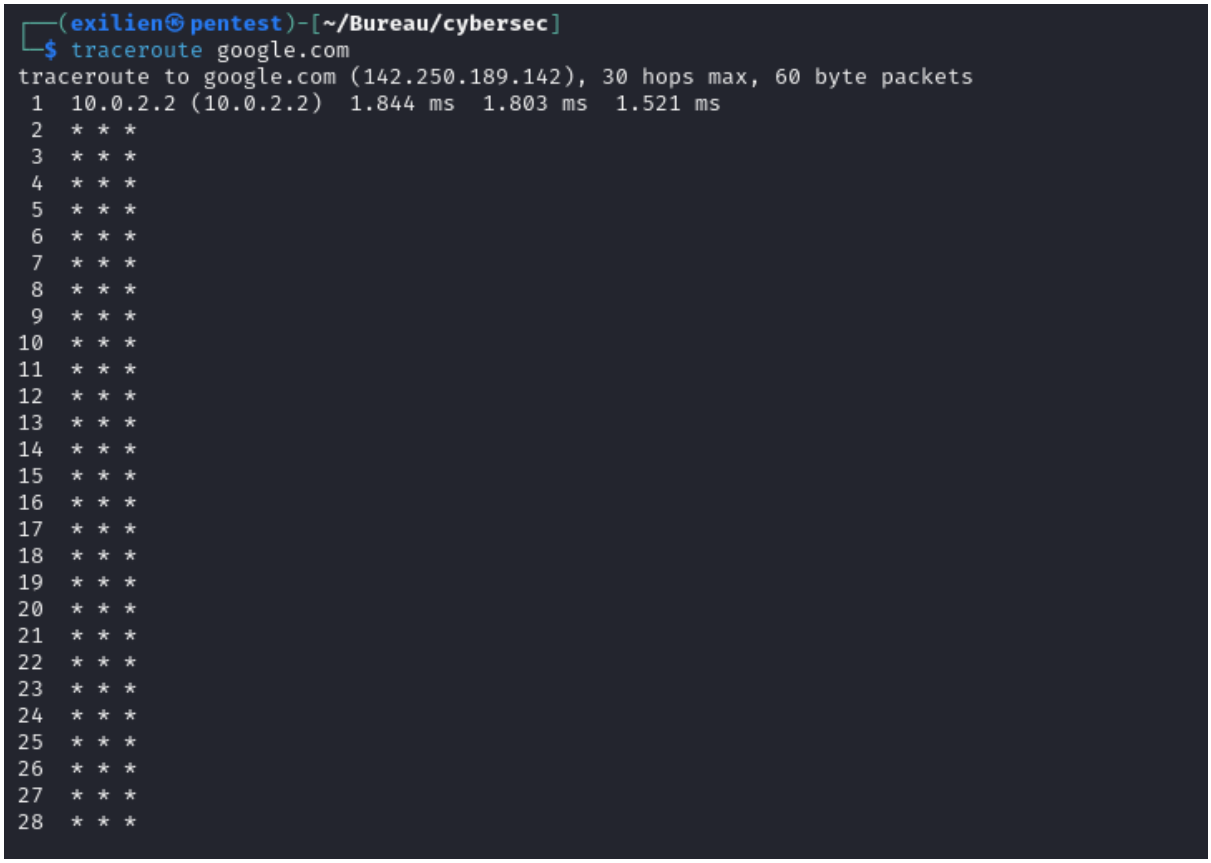
```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.3  0.6  22588 14016 ?        Ss   14:27   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    14:27   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    14:27   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-netns]
root           8  0.0  0.0      0     0 ?        R    14:27   0:00 [kworker/0:0-events]
root          11  0.0  0.0      0     0 ?        I    14:27   0:00 [kworker/u4:0-events_unbound]
root          12  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    14:27   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    14:27   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    14:27   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    14:27   0:00 [ksoftirqd/0]
root          17  0.1  0.0      0     0 ?        I    14:27   0:01 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    14:27   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          19  0.0  0.0      0     0 ?        S    14:27   0:00 [rcu_exp_gp_kthread_worker]
root          20  0.0  0.0      0     0 ?        S    14:27   0:00 [migration/0]
root          21  0.0  0.0      0     0 ?        S    14:27   0:00 [idle_inject/0]
root          22  0.0  0.0      0     0 ?        S    14:27   0:00 [cpuhp/0]
root          24  0.0  0.0      0     0 ?        S    14:27   0:00 [kdevtmpfs]
root          25  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-inet_frag_wq]
root          26  0.6  0.0      0     0 ?        I    14:27   0:05 [kworker/u4:1-events_unbound]
root          27  0.0  0.0      0     0 ?        S    14:27   0:00 [kauditd]
root          28  0.0  0.0      0     0 ?        S    14:27   0:00 [khungtaskd]
root          29  0.0  0.0      0     0 ?        S    14:27   0:00 [oom_reaper]
root          31  0.0  0.0      0     0 ?        I<   14:27   0:00 [kworker/R-writeback]
root          32  0.0  0.0      0     0 ?        S    14:27   0:00 [kcompactd0]
root          33  0.0  0.0      0     0 ?        SN   14:27   0:00 [ksmd]
```

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ 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]
00:02.0 VGA compatible controller: InnoTek Systemberatung GmbH VirtualBox Graphics 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 Audio device: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) High Definition 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)
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

La commande **`sudo apt install traceroute`** installe **l'outil `traceroute`** sur votre machine pour vous permettre de diagnostiquer et visualiser les routes réseau suivies par vos paquets de données.



La commande **`traceroute google.com`** est utilisée pour suivre le chemin emprunté par les paquets de données depuis votre ordinateur jusqu'à **google.com** (ou n'importe quel autre domaine) sur Internet.



La commande **`netstat -tuln`** est utilisée pour afficher les **connexions réseau** et les **ports d'écoute** actifs sur votre machine.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
udp        0      0 0.0.0.0:55404           0.0.0.0:*
udp        0      0 10.0.2.15:3702          0.0.0.0:*
udp        0      0 239.255.255.250:3702    0.0.0.0:*
udp6       0      0 :::60263                :::*
udp6       0      0 fe80::a00:27ff:fee:3702 :::*
udp6       0      0 ff02::c:3702            :::*

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

La commande **`ss -tuln`** est utilisée pour afficher des informations sur les **connexions réseau** actives, de manière similaire à **`netstat`**, mais elle est plus rapide et plus moderne. **`ss`** (Socket Stat) est l'outil recommandé pour examiner les sockets réseau dans les systèmes modernes.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ ss -tuln
Netid          State           Recv-Q          Send-Q                                  Local Address:Port                      Peer Address:Port
udp            UNCONN          0               0                                            0.0.0.0:55404                          0.0.0.0:*
udp            UNCONN          0               0                                          10.0.2.15:3702                           0.0.0.0:*
udp            UNCONN          0               0                                  239.255.255.250:3702                           0.0.0.0:*
udp            UNCONN          0               0                                               *:60263                                 *:*
udp            UNCONN          0               0                  [fe80::a00:27ff:fee2:295f]%eth0:3702                            [::]:*
udp            UNCONN          0               0                              [ff02::c]%eth0:3702                                 [::]:*

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

La commande **`journalctl`** est utilisée pour **afficher les journaux système** sur des systèmes utilisant **systemd**. Elle permet d'accéder aux logs générés par **systemd** (le gestionnaire de services du système), qui comprend des informations sur les services, les erreurs, les avertissements, etc.

La commande **`journalctl -f`** est utilisée pour afficher les journaux **en temps réel** (comme la commande `tail -f` pour les fichiers). Cela permet de **suivre l'activité** des services système pendant leur exécution.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl
fév 13 08:54:24 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-6) 14.2.0, GNU ld (GNU Binutils for Debian) 2.43.>
fév 13 08:54:24 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=24845ec1-ae10-48e3-9c22-b8254044bc0d ro quiet splash
fév 13 08:54:24 pentest kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
fév 13 08:54:24 pentest kernel: BIOS-provided physical RAM map:
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x00000007ffefffff] usable
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x00000007fff0000-0x00000007ffffffff] ACPI data
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
fév 13 08:54:24 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
fév 13 08:54:24 pentest kernel: NX (Execute Disable) protection: active
fév 13 08:54:24 pentest kernel: APIC: Static calls initialized
fév 13 08:54:24 pentest kernel: SMBIOS 2.5 present.
fév 13 08:54:24 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
fév 13 08:54:24 pentest kernel: DMI: Memory slots populated: 0/0
fév 13 08:54:24 pentest kernel: tsc: Fast TSC calibration using PIT
fév 13 08:54:24 pentest kernel: tsc: Detected 2195.799 MHz processor
fév 13 08:54:24 pentest kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
fév 13 08:54:24 pentest kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
fév 13 08:54:24 pentest kernel: last_pfn = 0x80000 max_arch_pfn = 0x400000000
fév 13 08:54:24 pentest kernel: MTRRs disabled by BIOS
fév 13 08:54:24 pentest kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
fév 13 08:54:24 pentest kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
fév 13 08:54:24 pentest kernel: RAMDISK: [mem 0x29633000-0x30b10fff]
fév 13 08:54:24 pentest kernel: ACPI: Early table checksum verification disabled
fév 13 08:54:24 pentest kernel: ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX  )
fév 13 08:54:24 pentest kernel: ACPI: XSDT 0x00000007FFF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
fév 13 08:54:24 pentest kernel: ACPI: FACP 0x00000007FFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001 ASL  00000061)
fév 13 08:54:24 pentest kernel: ACPI: DSDT 0x00000007FFF0470 002325 (v02 VBOX   VBOXBIOS 00000002 INTL 20100528)
```

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -f
fév 16 14:55:35 pentest dbus-daemon[566]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requ
ested by ':1.94' (uid=1000 pid=14598 comm="xfce4-screenshooter --region")
fév 16 14:55:35 pentest systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 16 14:55:35 pentest systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 16 14:55:35 pentest dbus-daemon[566]: [system] Successfully activated service 'org.freedesktop.hostname1'
fév 16 14:56:06 pentest systemd[1]: systemd-hostnamed.service: Deactivated successfully.
fév 16 14:57:12 pentest dbus-daemon[566]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requ
ested by ':1.96' (uid=1000 pid=15390 comm="xfce4-screenshooter --region")
fév 16 14:57:12 pentest systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 16 14:57:13 pentest systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 16 14:57:13 pentest dbus-daemon[566]: [system] Successfully activated service 'org.freedesktop.hostname1'
fév 16 14:57:43 pentest systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

La commande **`journalctl -b`** est utilisée pour afficher les journaux **du dernier démarrage** du système. Cela permet de visualiser les événements enregistrés depuis que votre machine a été démarrée, y compris les messages du noyau, les services système et d'autres informations pertinentes.

La commande **`journalctl -n 10`** est utilisée pour afficher les **dernières 10 lignes** du journal. C'est un moyen rapide de voir les **derniers événements** enregistrés dans le journal sans avoir à parcourir l'ensemble du fichier.

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -b
fév 16 09:28:10 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-6) 14.2.0, GNU ld (GNU Binutils for Debian) 2.43.>
fév 16 09:28:10 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=24845ec1-ae10-48e3-9c22-b8254044bc0d ro quiet splash
fév 16 09:28:10 pentest kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
fév 16 09:28:10 pentest kernel: BIOS-provided physical RAM map:
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000 7fefffff] usable
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x00000000 7fff0000-0x00000000 7fffffff] ACPI data
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
fév 16 09:28:10 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
fév 16 09:28:10 pentest kernel: NX (Execute Disable) protection: active
fév 16 09:28:10 pentest kernel: APIC: Static calls initialized
fév 16 09:28:10 pentest kernel: SMBIOS 2.5 present.
fév 16 09:28:10 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
fév 16 09:28:10 pentest kernel: DMI: Memory slots populated: 0/0
fév 16 09:28:10 pentest kernel: tsc: Fast TSC calibration failed
fév 16 09:28:10 pentest kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
fév 16 09:28:10 pentest kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
fév 16 09:28:10 pentest kernel: last_pfn = 0x80000 max_arch_pfn = 0x400000000
fév 16 09:28:10 pentest kernel: MTRRs disabled by BIOS
fév 16 09:28:10 pentest kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
fév 16 09:28:10 pentest kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
fév 16 09:28:10 pentest kernel: RAMDISK: [mem 0x29633000-0x30b10fff]
fév 16 09:28:10 pentest kernel: ACPI: Early table checksum verification disabled
fév 16 09:28:10 pentest kernel: ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX  )
fév 16 09:28:10 pentest kernel: ACPI: XSDT 0x000000007FFF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
```

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -n 10
fév 16 14:57:43 pentest systemd[1]: systemd-hostnamed.service: Deactivated successfully.
fév 16 14:58:57 pentest dbus-daemon[566]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' req>
fév 16 14:58:57 pentest systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 16 14:58:57 pentest systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 16 14:58:57 pentest dbus-daemon[566]: [system] Successfully activated service 'org.freedesktop.hostname1'
fév 16 14:59:27 pentest systemd[1]: systemd-hostnamed.service: Deactivated successfully.
fév 16 14:59:58 pentest dbus-daemon[566]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' req>
fév 16 14:59:58 pentest systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 16 14:59:59 pentest systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 16 14:59:59 pentest dbus-daemon[566]: [system] Successfully activated service 'org.freedesktop.hostname1'
lines 1-10/10 (END)
```

La commande **`date`** est utilisée pour afficher la **date et l'heure actuelles** du système dans un format lisible.

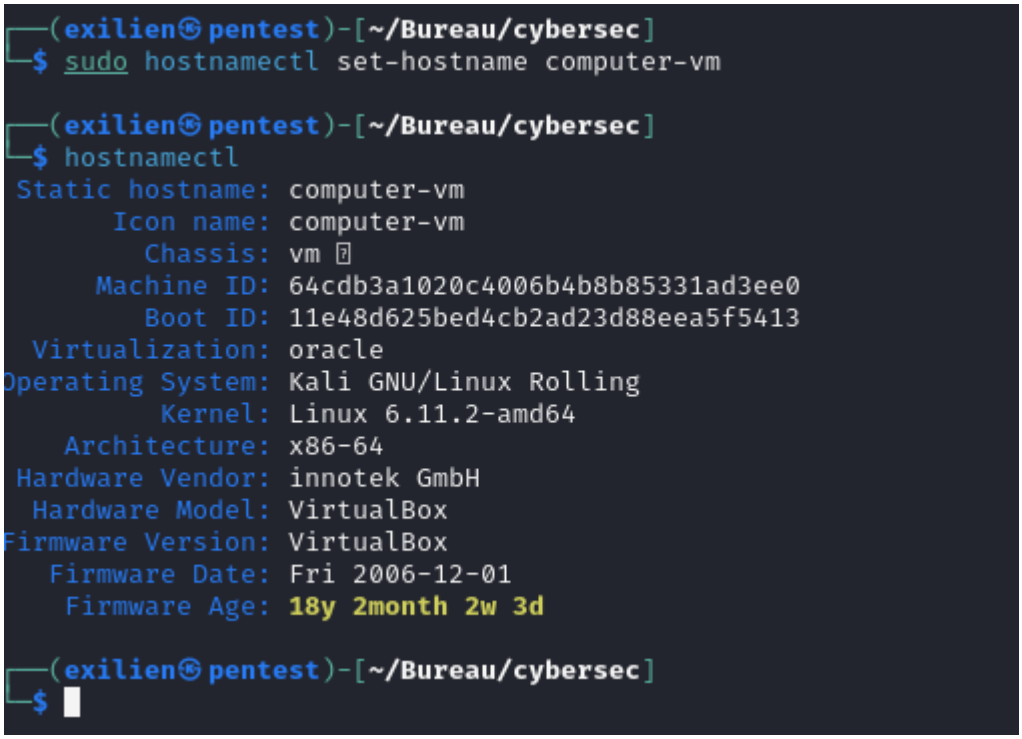
La commande **`timedatectl`** est utilisée pour **gérer et afficher** les **paramètres de date et d'heure** sur un système utilisant **systemd**.

La commande **`hostnamectl`** est utilisée pour **afficher ou configurer** le **nom d'hôte** de votre machine (le nom qui identifie l'ordinateur sur le réseau).

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ date
dim 16 fév 2025 15:01:00 EST

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ timedatectl
               Local time: dim 2025-02-16 15:01:31 EST
           Universal time: dim 2025-02-16 20:01:31 UTC
                 RTC time: dim 2025-02-16 15:01:30
                Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

```
┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$ hostnamectl
 Static hostname: pentest
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 64cdb3a1020c4006b4b8b85331ad3ee0
         Boot ID: 11e48d625bed4cb2ad23d88eea5f5413
  Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.11.2-amd64
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox
Firmware Version: VirtualBox
   Firmware Date: Fri 2006-12-01
    Firmware Age: 18y 2month 2w 3d

┌──(exilien㉿pentest)-[~/Bureau/cybersec]
└─$
```

La commande **`sudo hostnamectl set-hostname [nouveau_nom]`** est utilisée pour **changer le nom d'hôte** (hostname) de votre machine sous Linux.



En un mot ,la tâche consistait à explorer et expliquer plusieurs commandes Linux qui sont essentielles pour la gestion et la configuration des systèmes.