

UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI

UNITECH

Sécurité Informatique

Travaux Dirigés: Virtualisation de Kali Linux et Commandes

Professeur : Mr Ismael Saint Amour

Préparé par : Kendy Morandi COMPERE

Nom utilisateur : kali

Date: Le 16-02-2025

Description des résultats de la tâche

Kali Linux est un système d'exploitation spécialisé dans la Cyber Sécurité et l'analyse de réseaux, offrant une large gamme d'outils pour les tests d'intrusion et l'administration système. La création et la gestion de dossiers sont des compétences essentielles pour organiser et manipuler des fichiers efficacement.

Dans cet exercice, la structure de dossiers est créée avec un dossier principal "cybersec" contenant trois sous-dossiers : "scan", "logs" et "scripts". L'ajout des fichiers "notes.txt" et leur modification permettent de comprendre la manipulation des fichiers en ligne de commande. La copie, le déplacement et la suppression de fichiers assurent une maîtrise des commandes fondamentales comme ``cp``, ``mv``, et ``rm``.

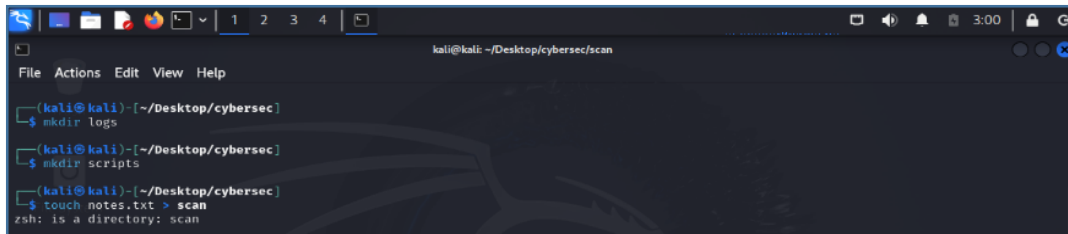
Ensuite, l'utilisation d'outils réseau comme ``ifconfig`` ou ``ip`` permet de récupérer des informations réseau essentielles, et ``nmap`` offre une méthode puissante pour analyser un réseau local et identifier les appareils connectés. L'utilisation de ``grep`` améliore la recherche d'informations spécifiques dans un fichier.

L'exécution des commandes système comme ``df -h``, ``du -sh``, et ``free -h`` donne un aperçu de l'utilisation des ressources du système. De même, ``ps aux``, ``lspci`` et ``netstat -tuln`` permettent d'obtenir des informations sur les processus actifs, les périphériques PCI, et les connexions réseau. La commande ``traceroute`` est utilisée pour tracer le chemin des paquets vers un serveur distant, illustrant ainsi les itinéraires empruntés sur Internet.

Enfin, ``journalctl`` et ses diverses options permettent d'afficher et de gérer les logs du système, tandis que ``date``, ``timedatectl`` et ``hostnamectl`` offrent un aperçu de la configuration du temps et du nom d'hôte du système.

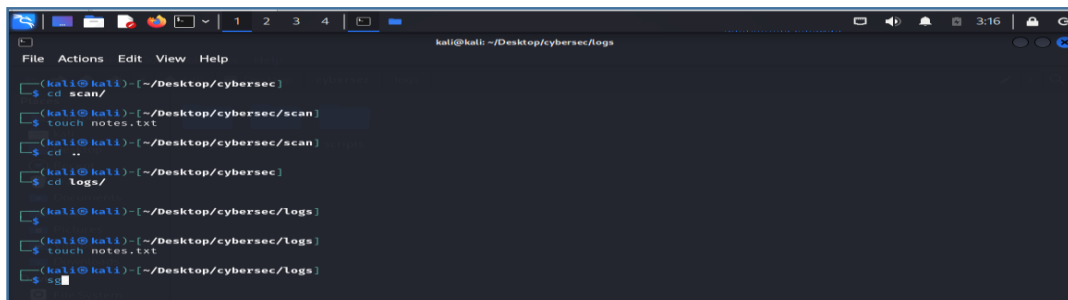
1. Creation d'une structure de dossiers

Creation dossier cybersec et les sous dossiers (logs, scripts, scan)



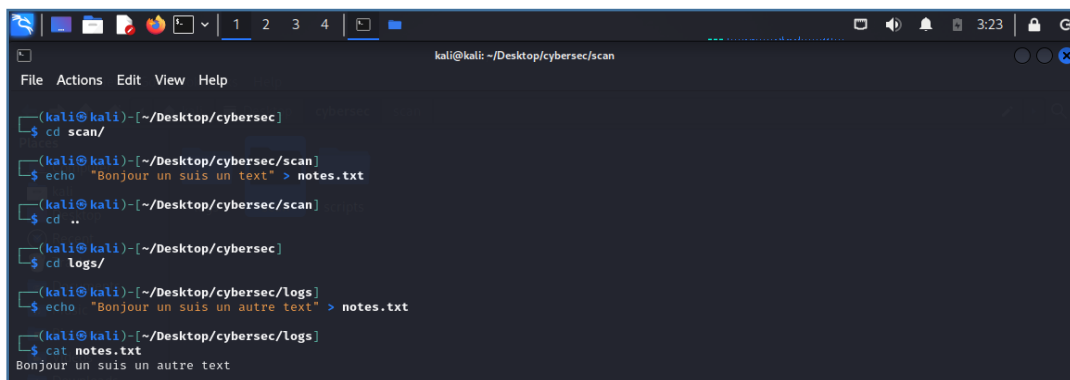
```
kali@kali: ~/Desktop/cybersec
$ mkdir logs
$ mkdir scripts
$ touch notes.txt
$ cd scan
zsh: is a directory: scan
```

Ajout d'un fichier (notes.txt) dans scan et logs



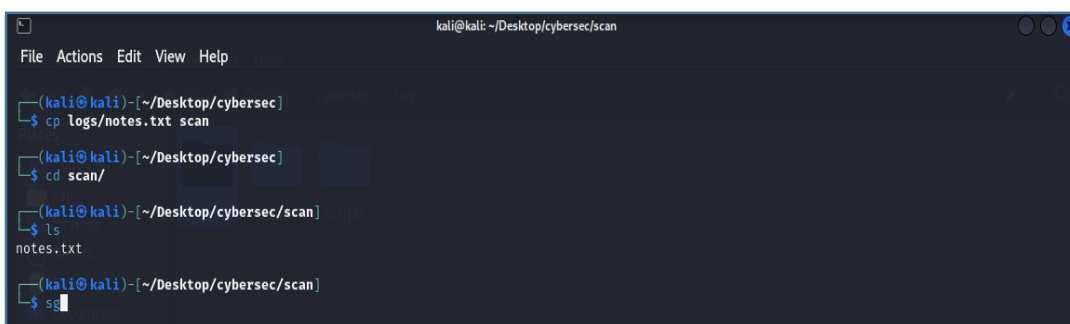
```
kali@kali: ~/Desktop/cybersec/logs
$ cd scan/
$ touch notes.txt
$ cd ..
$ cd logs/
$ touch notes.txt
$
```

Insertion contenu dans les fichiers textes (notes.txt) et Affichage



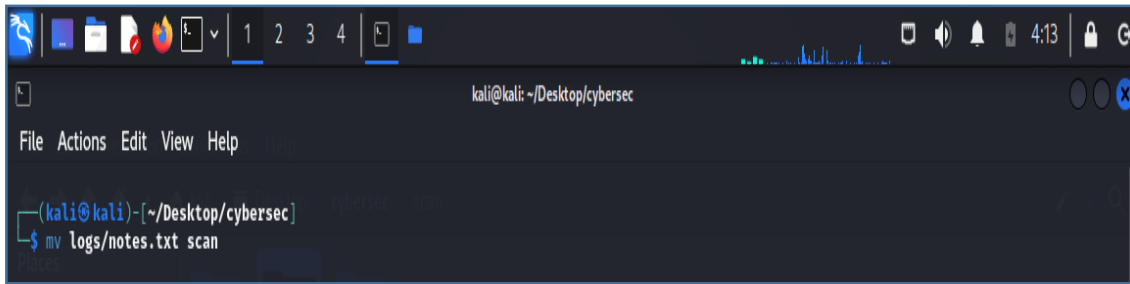
```
kali@kali: ~/Desktop/cybersec/scan
$ cd scan/
$ echo "Bonjour un suis un text" > notes.txt
$ cd ..
$ cd logs/
$ echo "Bonjour un suis un autre text" > notes.txt
$ cat notes.txt
Bonjour un suis un autre text
```

Copie des fichiers (notes.txt) dans scripts et Vérification du fichier



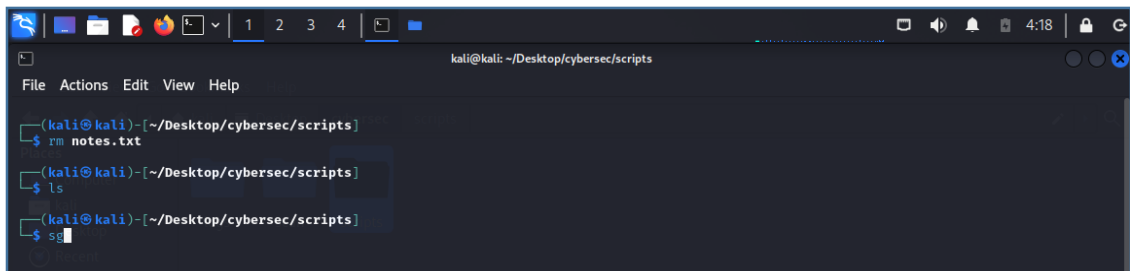
```
kali@kali: ~/Desktop/cybersec/scan
$ cp logs/notes.txt scan
$ cd scan/
$ ls
notes.txt
$
```

Déplacement du fichier (notes.txt) dans le sous dossier scan



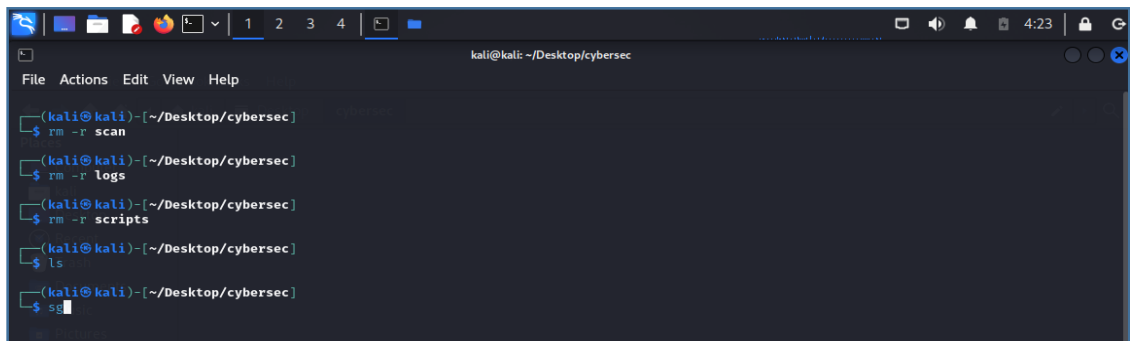
```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
(kali@kali)~/Desktop/cybersec
$ mv logs/notes.txt scan
```

Suppression du fichier (notes.txt) dans le sous dossier scripts et vérification



```
kali@kali: ~/Desktop/cybersec/scripts
File Actions Edit View Help
(kali@kali)~/Desktop/cybersec/scripts
$ rm notes.txt
(kali@kali)~/Desktop/cybersec/scripts
$ ls
(kali@kali)~/Desktop/cybersec/scripts
$ sg
```

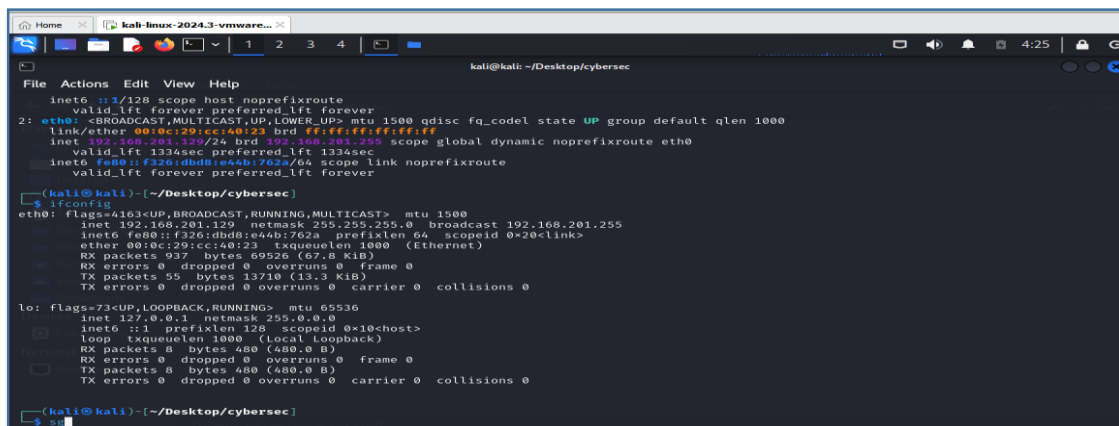
Suppression des sous-dossiers et vérification



```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
(kali@kali)~/Desktop/cybersec
$ rm -r scan
(kali@kali)~/Desktop/cybersec
$ rm -r logs
(kali@kali)~/Desktop/cybersec
$ rm -r scripts
(kali@kali)~/Desktop/cybersec
$ ls
(kali@kali)~/Desktop/cybersec
$ sg
```

2. Scannerisation d'un réseau

Utilisation Commande Ifconfig ou ip a



```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
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:cc:40:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.201.129/24 brd 192.168.201.255 scope global dynamic noprefixroute eth0
        valid_lft 1334sec preferred_lft 1334sec
    inet6 fe80::f26:dbd8:e44b:762a/64 scope link noprefixroute
        Valid_lft forever preferred_lft forever
(kali@kali)~/Desktop/cybersec
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.201.129 netmask 255.255.255.0 broadcast 192.168.201.255
    inet6 fe80::f26:dbd8:e44b:762a prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:cc:40:23 txqueuelen 1000 (Ethernet)
    RX packets 937 bytes 69826 (67.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 55 bytes 13710 (13.3 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali@kali)~/Desktop/cybersec
$ sg
```

Utilisation nmap

```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
-oN /ox/-os/-od <filename>: Output scan in normal, XML, sIcKtP kIddi3,
and Grapable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
-reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-G: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 -p 80
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

(kali@kali)~[~/Desktop/cybersec]
$
```

Création du fichier (secret.text)

```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
(kali@kali)~[~/Desktop/cybersec]
$ touch secret.txt
(kali@kali)~[~/Desktop/cybersec]
$ chmod 400
chmod: missing operand after '400'
Try 'chmod --help' for more information.
(kali@kali)~[~/Desktop/cybersec]
$ chmod 400 secret.txt
(kali@kali)~[~/Desktop/cybersec]
$ ls -l
total 0
-r-- 1 kali kali 0 Jan 23 04:34 secret.txt
```

Utilisation de la commande grep

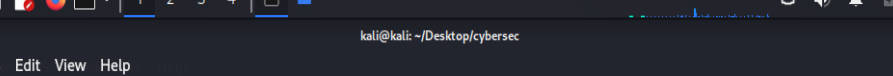
```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
(kali@kali)~[~/Desktop/cybersec]
$ touch log.txt
(kali@kali)~[~/Desktop/cybersec]
$ echo "Bonjour un suis le MOT a recherche" > log.txt
(kali@kali)~[~/Desktop/cybersec]
$ grep "MOT" log.txt
Bonjour un suis le MOT a recherche
(kali@kali)~[~/Desktop/cybersec]
$
```

4. Exécution des Commandes

df -h

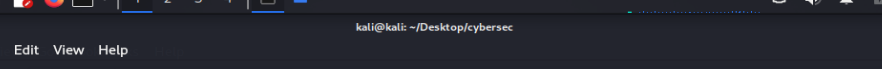
```
kali@kali: ~/Desktop/cybersec
File Actions Edit View Help
(kali@kali)~[~/Desktop/cybersec]
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            92.2M   0  92.2M   0% /dev
tmpfs           197M   1.3M  196M   1% /run
/dev/sda1       70G   15G   55G   21% /
tmpfs           98.3M   0   98.3M   0% /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           98.3M  8.0K   98.3M   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           197M  1.28K  197M   1% /run/user/1000
```

du -sh



The screenshot shows a Kali Linux terminal window. The title bar at the top includes standard Linux window controls and system status icons (network, volume, notifications, time 4:55). The terminal's title bar displays the user and path: 'kali@kali: ~/Desktop/cybersec'. The menu bar contains 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal content shows the user at the prompt '(kali@kali)-[~/Desktop/cybersec]' typing the command 'du -sh', which returns '8.0K'. On the next line, the user types 'sg' and the prompt changes to '#', indicating a successful privilege escalation. A file manager sidebar is visible on the left, showing 'Desktop' and 'Recent' sections.

free -h



The screenshot shows a Kali Linux terminal window with the title bar "kali@kali: ~/Desktop/cybersec". The terminal displays the command `free -h` and its output, which shows system memory usage in human-readable format. The output is as follows:

	total	used	free	shared	buff/cache	available
Mem:	1.9Gi	722Mi	939Mi	15Mi	461Mi	1.2Gi
Swap:	1.0Gi	0B	1.0Gi			

Below the memory output, the terminal shows the command `sg` being entered, followed by a cursor. The terminal window also shows standard menu options (File, Actions, Edit, View, Help) and window controls.

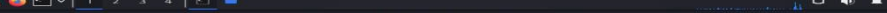
px aux

[illegible]

```

File Actions Edit View Help
root 4.5 0.0 0.0 0 0 7 1 I< 02:46 0.000 [kworker/R-int_]
root 4.6 0.0 0.0 0 0 7 1 I< 02:46 0.003 [kworker/R-us11-events_unbound]
root 4.7 0.0 0.0 0 0 7 5 S 02:46 0.000 [kauditd]
root 4.8 0.0 0.0 0 0 7 5 S 02:46 0.000 [khuatibsd]
root 5.0 0.0 0.0 0 0 7 5 S 02:46 0.000 [oom_reaper]
root 5.2 0.0 0.0 0 0 7 5 I< 02:46 0.000 [kworker/R-write]
root 5.3 0.0 0.0 0 0 7 5 S 02:46 0.000 [kcompasid]
root 5.4 0.0 0.0 0 0 7 5 SH 02:46 0.000 [kcmd]
root 5.6 0.0 0.0 0 0 7 5 I< 02:46 0.000 [kworker/R-kint]
root 5.7 0.0 0.0 0 0 7 5 I< 02:46 0.000 [kworker/R-kblk]
root 5.8 0.0 0.0 0 0 7 5 I< 02:46 0.000 [kworker/R-bkcg]
root 5.9 0.0 0.0 0 0 7 5 S 02:46 0.000 [irq/8-cpi]
root 6.1 0.0 0.0 0 0 7 5 I< 02:46 0.000 [kworker/R-tpm_d]
root 6.2 0.0 0.0 0 0 7 5 S 02:46 0.000 [kworker/R-svc-1]
root 6.3 0.0 0.0 0 0 7 5 I< 02:46 0.000 [kworker/R-dcwr]
root 6.5 0.0 0.0 0 0 7 5 S 02:46 0.000 [kworker/0-34-block]
root 6.6 0.0 0.0 0 0 7 5 S 02:46 0.000 [kswapd0]
root 6.7 0.0 0.0 0 0 7 5 I< 02:47 0.000 [kworker/R-us13-events_unbound]
root 7.6 0.0 0.0 0 0 7 5 S 02:47 0.000 [kworker/R-kthrw]
root 7.7 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/6-pcihp]
root 7.8 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/26-pcihp]
root 7.9 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/27-pcihp]
root 8.0 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/28-pcihp]
root 8.1 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/29-pcihp]
root 8.2 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/30-pcihp]
root 8.3 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/31-pcihp]
root 8.4 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/32-pcihp]
root 8.5 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/33-pcihp]
root 8.6 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/34-pcihp]
root 8.7 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/35-pcihp]
root 8.8 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/36-pcihp]
root 8.9 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/37-pcihp]
root 9.0 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/38-pcihp]
root 9.1 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/39-pcihp]
root 9.2 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/40-pcihp]
root 9.3 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/41-pcihp]
root 9.4 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/42-pcihp]
root 9.5 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/43-pcihp]
root 9.6 0.0 0.0 0 0 7 5 S 02:47 0.000 [irq/44-pcihp]

```


[illegible]

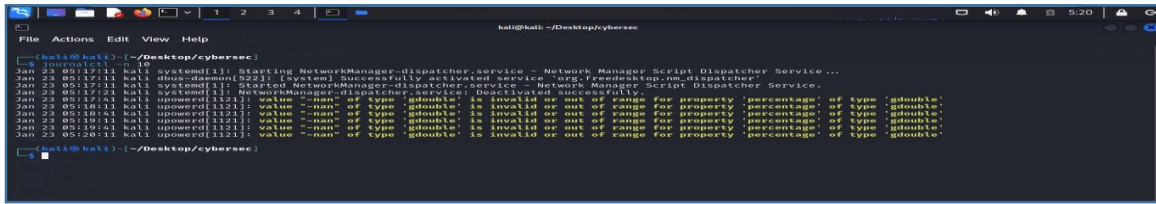
```
kal@kali: ~/Desktop/cybersec
File Actions Edit View Help
(kali@kali)~$ apt-get install tracertool
error: Unable to locate package tracertool
(kali@kali)~$
```

```
kali@kali - /Desktop/cybersec
File Actions Edit View Help

kali@kali:~/Desktop/cybersec$
kali@kali:~/Desktop/cybersec$ traceroute google.com
traceroute to google.com (192.178.201.2), 30 hops max, 60 byte packets
 0  *
 1  *
 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  *
```

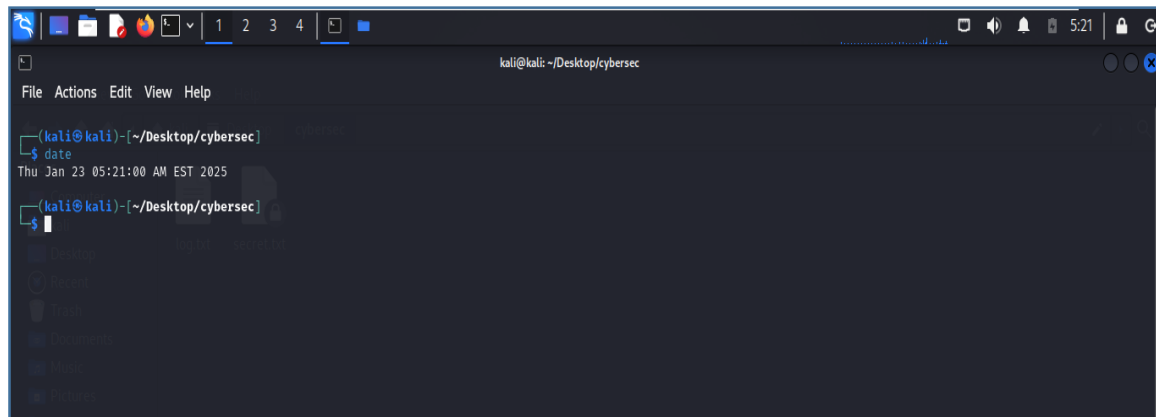
[illegible]

journalctl -n 10



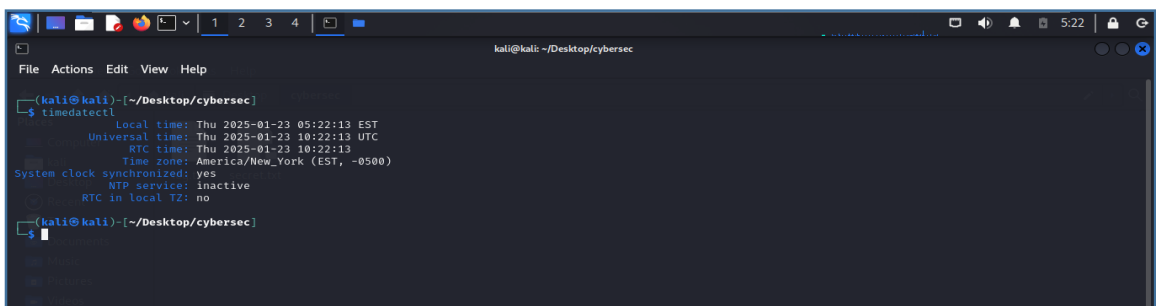
```
kali@kali: ~/Desktop/cybersec
journalctl -n 10
Jan 23 05:17:11 kali systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
Jan 23 05:17:13 kali dbus-daemon[522]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'.
Jan 23 05:17:13 kali Systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Jan 23 05:17:23 kali Systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Jan 23 05:18:11 kali nmmonitor[1221]: value "-nan" of type "double" is invalid or out of range for property 'percentage' of type 'double'.
Jan 23 05:18:13 kali nmmonitor[1221]: value "-nan" of type "double" is invalid or out of range for property 'percentage' of type 'double'.
Jan 23 05:19:11 kali nmmonitor[1221]: value "-nan" of type "double" is invalid or out of range for property 'percentage' of type 'double'.
Jan 23 05:19:13 kali nmmonitor[1221]: value "-nan" of type "double" is invalid or out of range for property 'percentage' of type 'double'.
Jan 23 05:20:11 kali nmmonitor[1221]: value "-nan" of type "double" is invalid or out of range for property 'percentage' of type 'double'.
Jan 23 05:20:13 kali nmmonitor[1221]: value "-nan" of type "double" is invalid or out of range for property 'percentage' of type 'double'.
```

date



```
kali@kali: ~/Desktop/cybersec
date
Thu Jan 23 05:21:00 AM EST 2025
```

timedatectl



```
kali@kali: ~/Desktop/cybersec
timedatectl
Local time: Thu 2025-01-23 05:22:13 EST
Universal time: Thu 2025-01-23 10:22:13 UTC
RTC time: Thu 2025-01-23 10:22:13
Time zone: America/New_York (EST, -0500)
System clock synchronized: yes
NTP service: inactive
RTC in local TZ: no
```

hostnamectl



```
kali@kali: ~/Desktop/cybersec
hostnamectl
Hostname: kali
Icon: computer-vm
FQDN: kali
Static IP: 10.0.2.15
MAC: 08:00:27:1c:3d:9f
UUID: a95b2acc-139a-4d50-9a4f-a899450b0afe
AP-Vendor: 25502650
Virtualization: vmware
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.8.11-amd64
Architecture: x86_64
Hardware Vendor: VMware, Inc.
Hardware Model: VMware Virtual Platform
Firmware Version: 6.00
Firmware Date: Thu 2020-11-12
Firmware Age: 4y 2month 1w 4d
```

Conclusion

Cet exercice met en avant les compétences essentielles pour la gestion des fichiers, l'analyse réseau et l'administration système sous Kali Linux. La maîtrise de ces commandes est cruciale pour tout professionnel de la CyberSécurité, car elle permet d'automatiser des tâches, d'analyser les performances du système et de sécuriser un réseau efficacement. Kali Linux demeure un outil puissant pour les experts en sécurité informatique, et ces exercices pratiques renforcent la compréhension et l'application des fonctionnalités fondamentales de cet environnement.