

# **Université de Technologie d'Haïti (UNITECH)**

**Sujet : Travaux dirigés Virtualisation de Kali Linux**

**Préparé Par :  
DIEUVEUILLE Ruth**

**Propose Par :  
SAINT AMOUR Ismaël**

**Le 16/02/24**

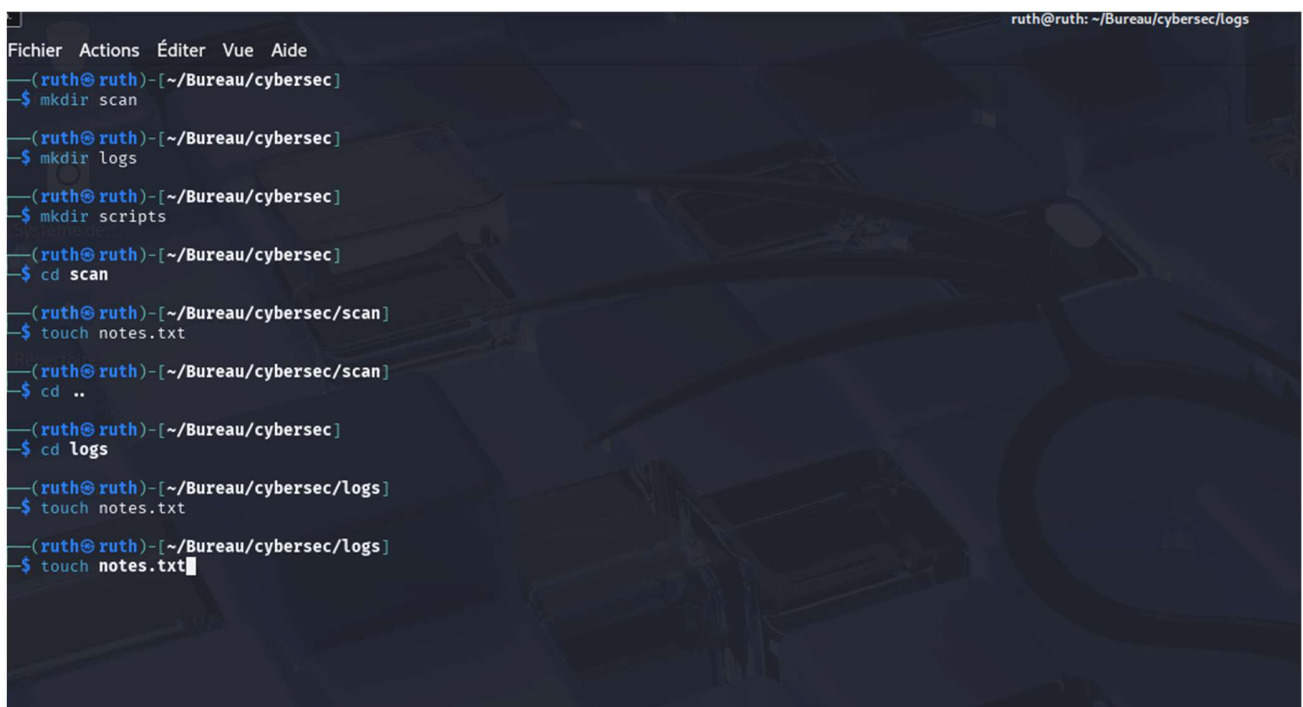
Ce devoir contient la virtualisation et l'installation d'un système d'exploitation kali Linux. On trouve premièrement la virtualisation avec Virtual Box et l'installation de kali dans une machine virtuelle, une mise à jour de kali et quelques commandes.

On aura quelques captures qui représenteront les différentes commandes.

1ere commande :

On crée un dossier cybersec

dans ce dossier on a créé 3 sous-dossiers:scan,logs et Scripts.



```
Fichier Actions Éditer Vue Aide
(ruth@ruth)-[~/Bureau/cybersec]
$ mkdir scan
(ruth@ruth)-[~/Bureau/cybersec]
$ mkdir logs
(ruth@ruth)-[~/Bureau/cybersec]
$ mkdir scripts
(ruth@ruth)-[~/Bureau/cybersec]
$ cd scan
(ruth@ruth)-[~/Bureau/cybersec/scan]
$ touch notes.txt
(ruth@ruth)-[~/Bureau/cybersec/scan]
$ cd ..
(ruth@ruth)-[~/Bureau/cybersec]
$ cd logs
(ruth@ruth)-[~/Bureau/cybersec/logs]
$ touch notes.txt
(ruth@ruth)-[~/Bureau/cybersec/logs]
$ touch notes.txt
```

Dans cette 2eme partie :

On trouve la création d'un fichier avec « touch » et ajout de texte grâce à la commande echo.

```

Fichier Actions Éditer Vue Aide
ruth@ruth: ~/Bureau/cybersec/scripts
$ cd ..
(ruth@ruth)~/Bureau/cybersec
$ cd logs
(ruth@ruth)~/Bureau/cybersec/logs
$ touch notes.txt
(ruth@ruth)~/Bureau/cybersec/logs
$ echo "La cybersecurite designe l'ensemble des technologies,pratiques et p
olitiques destinees a prevenir les cyberattaques."> notes.txt
echoLa cybersecurite designe l'ensemble des technologies,pratiques et politi
ques destinees a prevenir les cyberattaques. : commande introuvable
(ruth@ruth)~/Bureau/cybersec/logs
$ echo "La cybersecurite designe l'ensemble des technologies,pratiques et politiques destinees a prevenir les cyberattaques."> notes.txt
(ruth@ruth)~/Bureau/cybersec/logs
$ cat notes.txt
La cybersecurite designe l'ensemble des technologies,pratiques et politiques destinees a prevenir les cyberattaques.
(ruth@ruth)~/Bureau/cybersec/logs
$ cp notes.txt scripts
(ruth@ruth)~/Bureau/cybersec/logs
$ cd ..
(ruth@ruth)~/Bureau/cybersec
$ cd scan
(ruth@ruth)~/Bureau/cybersec/scan
$ echo "La cybersecurite designe l'ensemble des technologies,pratiques et politiques destinees a prevenir les cyberattaques."> notes.txt
(ruth@ruth)~/Bureau/cybersec/scan
$ cat notes.txt
La cybersecurite designe l'ensemble des technologies,pratiques et politiques destinees a prevenir les cyberattaques.
(ruth@ruth)~/Bureau/cybersec/scan
$ cd ..
(ruth@ruth)~/Bureau/cybersec
$ cd scripts
```

Dans cette 3eme partie :

On fait la copie avec la commande  
`cp chemin/nomfichier.ext versChemindusecondrepertoire.`

Il y a aussi suppression avec la commande  
`rm -r nomrep` afin de supprimer tout le contenu du répertoire.

```
(ruth@ruth)-[~/Bureau/cybersec/scan]
$ cd ..

(ruth@ruth)-[~/Bureau/cybersec]
$ cp ~/Bureau/cybersec/scan/notes.txt ~/Bureau/cybersec/scripts

(ruth@ruth)-[~/Bureau/cybersec]
$ ls -l
total 12
-rwxrwxr-x 2 ruth ruth 4096 14 fév 13:00 logs
-rwxrwxr-x 2 ruth ruth 4096 14 fév 13:00 scan
-rwxrwxr-x 2 ruth ruth 4096 14 fév 13:03 scripts

(ruth@ruth)-[~/Bureau/cybersec]
$ cd scripts

(ruth@ruth)-[~/Bureau/cybersec/scripts]
$ ls -l
total 4
-rw-rw-r-- 1 ruth ruth 39 14 fév 13:03 notes.txt

(ruth@ruth)-[~/Bureau/cybersec/scripts]
$ mv ~/Bureau/cybersec/scripts/notes.txt ~/Bureau/cybersec/scan

(ruth@ruth)-[~/Bureau/cybersec/scripts]
$ ls -l
total 0

(ruth@ruth)-[~/Bureau/cybersec/scripts]
$ rm scan
rm: impossible de supprimer 'scan': Aucun fichier ou dossier de ce nom

(ruth@ruth)-[~/Bureau/cybersec/scripts]
$ cd ..

(ruth@ruth)-[~/Bureau/cybersec]
$ rm scan
rm: impossible de supprimer 'scan': est un dossier

(ruth@ruth)-[~/Bureau/cybersec]
$ rm -r scan

(ruth@ruth)-[~/Bureau/cybersec]
$ rm -r scripts

(ruth@ruth)-[~/Bureau/cybersec]
$ rm -r logs

(ruth@ruth)-[~/Bureau/cybersec]
$
```

**Dans cette 4eme partie :**

**On trouve les informations de réseau grâce à la commande ifconfig.**

```
(ruth@ruth)-[~/Bureau/cybersec]
$ 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 fd00::ba81:73b8:eca6:6cf5 prefixlen 64 scopeid 0<global>
    inet6 fd00::a00:27ff:fe98:c7cf prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe98:c7cf prefixlen 64 scopeid 0<link>
    ether 08:00:27:98:c7:cf txqueuelen 1000 (Ethernet)
    RX packets 29 bytes 17323 (16.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 58 bytes 19905 (19.4 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<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

(ruth@ruth)-[~/Bureau/cybersec]
$
```

**Et aussi la scannerisation du réseau local grâce à nmap**

```

(ruth@ruthD)-[~/cybersec]
$ nmap 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 12:45 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(ruth@ruthD)-[~/cybersec]
$

```

Ici il y a :

**Création d'un fichier secret et modification d'accès lecture uniquement grâce a la commande chmod 3chiffres mis pour lecture ,écriture et exécution.**

**La commande df -h permet d'afficher l'espace disponible et utilise.**

```

(ruth@ruth)-[~/Bureau/cybersec]
$ touch secret.txt

(ruth@ruth)-[~/Bureau/cybersec]
$ chmod 722 secret.txt

(ruth@ruth)-[~/Bureau/cybersec]
$ touch log.txt

(ruth@ruth)-[~/Bureau/cybersec]
$ echo "La Journalisation du fichier" >log.txt

(ruth@ruth)-[~/Bureau/cybersec]
$ grep "la" log.txt

(ruth@ruth)-[~/Bureau/cybersec]
$ df -h

```

Sys. de fichiers	Taille	Utilisé	Dispo	Uti%	Monté sur
udev	925M	0	925M	0%	/dev
tmpfs	198M	992K	197M	1%	/run
/dev/sda1	19G	16G	2,2G	88%	/
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	988M	168K	988M	1%	/tmp
tmpfs	1,0M	0	1,0M	0%	/run/credentials/getty@tty1.servi
ce					



Il y a la commande ps aux qui permet d'obtenir des informations sur les processus en cours d'exécution.

```
(ruth@ruth) [~/Bureau/cybersec]
$ ps aux
SER PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root    1  0.1  0.7  23064 14192 ?        Ss   12:55   0:01 /sbin/init
root    2  0.0  0.0      0  0 ?        S    12:55   0:00 [kthreadd
root    3  0.0  0.0      0  0 ?        S    12:55   0:00 [pool_wor
root    4  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root    5  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root    6  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root    7  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   11  0.0  0.0      0  0 ?        I    12:55   0:00 [kworker/
root   12  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   13  0.0  0.0      0  0 ?        I    12:55   0:00 [rcu_task
root   14  0.0  0.0      0  0 ?        I    12:55   0:00 [rcu_task
root   15  0.0  0.0      0  0 ?        I    12:55   0:00 [rcu_task
root   16  0.0  0.0      0  0 ?        S    12:55   0:00 [ksoftirq
root   17  0.0  0.0      0  0 ?        I    12:55   0:00 [rcu_pree
root   18  0.0  0.0      0  0 ?        S    12:55   0:00 [rcu_exp_
root   19  0.0  0.0      0  0 ?        S    12:55   0:00 [rcu_exp_
root   20  0.0  0.0      0  0 ?        S    12:55   0:00 [migratio
root   21  0.0  0.0      0  0 ?        S    12:55   0:00 [idle_in]
root   22  0.0  0.0      0  0 ?        S    12:55   0:00 [cpuhp/0]
root   24  0.0  0.0      0  0 ?        S    12:55   0:00 [kdevtmpf
root   25  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   26  0.0  0.0      0  0 ?        I    12:55   0:01 [kworker/
root   27  0.0  0.0      0  0 ?        S    12:55   0:00 [kauditd]
root   28  0.0  0.0      0  0 ?        S    12:55   0:00 [khungtas
root   29  0.0  0.0      0  0 ?        S    12:55   0:00 [oom_reap
root   30  0.0  0.0      0  0 ?        I    12:55   0:00 [kworker/
root   31  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   32  0.0  0.0      0  0 ?        S    12:55   0:00 [kcompact
root   33  0.0  0.0      0  0 ?        SN   12:55   0:00 [ksmd]
root   34  0.0  0.0      0  0 ?        SN   12:55   0:00 [khugepag
root   35  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   36  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   37  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   38  0.0  0.0      0  0 ?        S    12:55   0:00 [irq/9-ac
root   39  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   40  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   41  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   42  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   43  0.0  0.0      0  0 ?        S    12:55   0:00 [kswapd0]
root   51  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   55  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   56  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   57  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   62  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   66  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   71  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  241  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  243  0.0  0.0      0  0 ?        S    12:55   0:00 [scsi_ah
root  244  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  245  0.0  0.0      0  0 ?        S    12:55   0:00 [scsi_ah
root   41  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   42  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   43  0.0  0.0      0  0 ?        S    12:55   0:00 [kswapd0]
root   51  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   55  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   56  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   57  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   62  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   66  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root   71  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  241  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  243  0.0  0.0      0  0 ?        S    12:55   0:00 [scsi_ah
root  244  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  245  0.0  0.0      0  0 ?        S    12:55   0:00 [scsi_ah
root  246  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  247  0.0  0.0      0  0 ?        S    12:55   0:00 [scsi_ah
root  248  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  251  0.0  0.0      0  0 ?        S    12:55   0:00 [irq/18-v
root  252  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  253  0.0  0.0      0  0 ?        I    12:55   0:00 [kworker/
root  254  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  297  0.0  0.0      0  0 ?        S    12:55   0:00 [jbd2/sda
root  298  0.0  0.0      0  0 ?        I<   12:55   0:00 [kworker/
root  359  0.0  0.8  50364 16604 ?        Ss   12:55   0:00 /usr/lib/
root  391  0.0  0.0      0  0 ?        R    12:55   0:00 [kworker/
root  410  0.0  0.5  35520 10468 ?        Ss   12:55   0:00 /usr/lib/
root  411  0.0  0.0      0  0 ?        S    12:55   0:00 [psimon]
root  532  0.0  0.3   8368 6484 ?        Ss   12:55   0:00 /usr/sbin
root  534  0.0  0.3 309152 7536 ?        Ssl  12:55   0:00 /usr/libe
message+ 535  0.0  0.3  10012 6448 ?        Ss   12:55   0:01 /usr/bin/
polkitd  537  0.0  0.4 382328 9972 ?        Ssl  12:56   0:00 /usr/lib/
root  539  0.0  0.4 18208 9012 ?        Ss   12:56   0:00 /usr/lib/
root  564  0.0  0.0      0  0 ?        I<   12:56   0:00 [kworker/
root  568  0.0  0.0      0  0 ?        I<   12:56   0:00 [kworker/
root  570  0.0  0.1   6784 2560 ?        Ss   12:56   0:00 /usr/sbin
root  617  0.0  0.9 335936 19552 ?        Ssl  12:56   0:00 /usr/sbin
root  620  0.0  0.1 291644 3316 ?        Sl   12:56   0:00 /usr/sbin
root  637  0.0  0.5 316448 12032 ?        Ssl  12:56   0:00 /usr/sbin
root  663  0.0  0.3 380792 7132 ?        Ssl  12:56   0:00 /usr/sbin
root  680  0.0  0.1   8096 2548 tty1  Ss+  12:56   0:00 /sbin/ag
root  681  1.9  6.1 468128 124996 tty7  Ssl+ 12:56   0:29 /usr/lib/
root  701  0.0  0.0      0  0 ?        S    12:56   0:00 [psimon]
rtkit   735  0.0  0.1 21428 3048 ?        Ssl  12:56   0:00 /usr/libe
root  802  0.0  0.4 236392 8840 ?        Sl   12:56   0:00 lightdm -
ruth    816  0.0  0.6 22300 12604 ?        Ss   12:56   0:00 /usr/lib/
ruth    818  0.0  0.1 22664 3620 ?        S    12:56   0:00 (sd-pam)
ruth    837  0.0  0.1   7092 3544 ?        Ss   12:56   0:00 /usr/bin/
ruth    838  0.0  0.5 100952 11928 ?        Ssl  12:56   0:00 /usr/bin/
ruth    839  0.0  0.2  84524 5168 ?        Ssl  12:56   0:00 /usr/bin/
ruth    841  0.0  0.9 480148 18824 ?        Ssl  12:56   0:00 /usr/bin/
ruth    843  0.0  0.4  98948 8956 ?        Ssl  12:56   0:00 /usr/bin/
ruth    844  0.0  0.5 314220 10156 ?        Ssl  12:56   0:00 /usr/bin/
ruth    845  0.0  0.2   9032 5736 ?        Ss   12:56   0:00 /usr/bin/
ruth    868  0.0  1.7 348708 36052 ?        Ssl  12:56   0:00 xfce4-ses
ruth    927  0.0  0.0  17116 1636 ?        S    12:56   0:00 /usr/bin/
ruth    934  0.0  0.2 215304 4192 ?        Sl   12:56   0:00 /usr/bin/
```

## Dans la partie ci-dessous :

Il y a les commandes :

Journalctl qui permet de limiter et de configurer l'espace de stockage que les fichiers journaux occupent sur le disque dur.

Journalctl -f qui permet d'afficher uniquement les entrées du journal les plus récentes et en continu imprimer les nouvelles entrées au fur et à mesure.

Journalctl -b qui permet d'afficher que les logs depuis le dernier démarrage du système.

Journalctl -n 10 qui permet d'afficher les 10 évènements les plus récents du journal.

```
(ruth@ruth) [~/Bureau/cybersec]
$ journalctl
fév 09 11:55:55 ruth systemd-xdg-autostart-generator[838]: Exec binary 'xca'
fév 09 11:55:55 ruth systemd-xdg-autostart-generator[838]: /etc/xdg/autosta
fév 09 11:55:55 ruth systemd[824]: Queued start job for default target defa
fév 09 11:55:55 ruth systemd[824]: Created slice app.slice - User Applicati
fév 09 11:55:55 ruth systemd[824]: Created slice session.slice - User Core >
fév 09 11:55:55 ruth systemd[824]: Reached target paths.target - Paths.
fév 09 11:55:55 ruth systemd[824]: Reached target timers.target - Timers.
fév 09 11:55:55 ruth systemd[824]: Starting dbus.socket - D-Bus User Messag
fév 09 11:55:55 ruth systemd[824]: Listening on dirmngr.socket - GnuPG netw
fév 09 11:55:55 ruth systemd[824]: Starting gcr-ssh-agent.socket - GCR ssh->
fév 09 11:55:55 ruth systemd[824]: Listening on gnome-keyring-daemon.socket
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent-browser.socket - >
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent-extra.socket - Gn
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent-ssh.socket - GnuP
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent.socket - GnuPG cr
fév 09 11:55:55 ruth systemd[824]: Listening on pipewire-pulse.socket - Pip
fév 09 11:55:55 ruth systemd[824]: Listening on pipewire.socket - PipeWire >
fév 09 11:55:55 ruth systemd[824]: Listening on gcr-ssh-agent.socket - GCR >
fév 09 11:55:55 ruth systemd[824]: Listening on dbus.socket - D-Bus User Me
fév 09 11:55:55 ruth systemd[824]: Reached target sockets.target - Sockets.
fév 09 11:55:55 ruth systemd[824]: Reached target basic.target - Basic Syst
fév 09 11:55:55 ruth systemd[824]: Started pipewire.service - PipeWire Mult
lines 1-22 ... skipping ...
fév 09 11:55:55 ruth systemd-xdg-autostart-generator[838]: Exec binary 'xcap' does not exist: No such file or directory
fév 09 11:55:55 ruth systemd-xdg-autostart-generator[838]: /etc/xdg/autostart/xcap-super-key-bind.desktop: not generating unit, executable specified in Exec= does not exist.
fév 09 11:55:55 ruth systemd[824]: Queued start job for default target default.target.
fév 09 11:55:55 ruth systemd[824]: Created slice app.slice - User Application Slice.
fév 09 11:55:55 ruth systemd[824]: Created slice session.slice - User Core Session Slice.
fév 09 11:55:55 ruth systemd[824]: Reached target paths.target - Paths.
fév 09 11:55:55 ruth systemd[824]: Reached target timers.target - Timers.
fév 09 11:55:55 ruth systemd[824]: Starting dbus.socket - D-Bus User Message Bus Socket ...
fév 09 11:55:55 ruth systemd[824]: Listening on dirmngr.socket - GnuPG network certificate management daemon.
fév 09 11:55:55 ruth systemd[824]: Starting gcr-ssh-agent.socket - GCR ssh-agent wrapper...
fév 09 11:55:55 ruth systemd[824]: Listening on gnome-keyring-daemon.socket - GNOME Keyring daemon.
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent-browser.socket - GnuPG cryptographic agent and passphrase cache (access for web browsers).
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent-extra.socket - GnuPG cryptographic agent and passphrase cache (restricted).
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
fév 09 11:55:55 ruth systemd[824]: Listening on gpg-agent.socket - GnuPG cryptographic agent and passphrase cache.
fév 09 11:55:55 ruth systemd[824]: Listening on pipewire-pulse.socket - PipeWire PulseAudio.
fév 09 11:55:55 ruth systemd[824]: Listening on pipewire.socket - PipeWire Multimedia System Sockets.
fév 09 11:55:55 ruth systemd[824]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
fév 09 11:55:55 ruth systemd[824]: Listening on dbus.socket - D-Bus User Message Bus Socket.
fév 09 11:55:55 ruth systemd[824]: Reached target sockets.target - Sockets.
fév 09 11:55:55 ruth systemd[824]: Reached target basic.target - Basic System.
fév 09 11:55:55 ruth systemd[824]: Started pipewire.service - PipeWire Multimedia Service.
fév 09 11:55:55 ruth systemd[824]: Started filter-chain.service - PipeWire filter chain daemon.
fév 09 11:55:55 ruth systemd[824]: Started wireplumber.service - Multimedia Service Session Manager.
fév 09 11:55:55 ruth systemd[824]: Started pipewire-pulse.service - PipeWire PulseAudio.
fév 09 11:55:55 ruth systemd[824]: Reached target default.target - Main User Target.
fév 09 11:55:55 ruth systemd[824]: Startup finished in 371ms.
fév 09 11:55:55 ruth systemd[824]: Started gnome-keyring-daemon.service - GNOME Keyring daemon.
```



```
-(ruth@ruth)-[~/Bureau/cybersec]
$ journalctl -f
v 14 13:30:46 ruth kernel: 18:30:46.973629 X11 events Sending monitor pos
ions (8 of them) to the host: VINF_SUCCESS
v 14 13:30:46 ruth kernel: 18:30:46.974577 X11 events received X11 event
9)
v 14 13:30:46 ruth kernel: 18:30:46.975134 X11 events RRScreenChangeNotif
event received
v 14 13:30:46 ruth kernel: 18:30:46.983865 X11 events Monitor 0 (w,h)=(64
480) (x,y)=(0,0)
v 14 13:30:46 ruth kernel: 18:30:46.984664 X11 events Sending monitor pos
ions (8 of them) to the host: VINF_SUCCESS
v 14 13:30:46 ruth kernel: 18:30:46.985659 X11 events received X11 event
9)
v 14 13:30:46 ruth kernel: 18:30:46.990731 X11 events RRScreenChangeNotif
event received
v 14 13:30:46 ruth kernel: 18:30:46.994530 X11 events Monitor 0 (w,h)=(64
480) (x,y)=(0,0)
v 14 13:30:47 ruth kernel: 18:30:47.001650 X11 events Sending monitor pos
ions (8 of them) to the host: VINF_SUCCESS
v 14 13:30:56 ruth systemd[1]: systemd-hostnamed.service: Deactivated succ
sfully.
```

```
-(ruth@ruth)-[~/Bureau/cybersec]
$ journalctl -b
v 14 12:55:54 ruth kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x>
v 14 12:55:54 ruth kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2->
v 14 12:55:54 ruth kernel: BIOS-provided physical RAM map:
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x0000000000009fc00-0x000000000>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x0000000007fff0000-0x000000000>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000f>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000f>
v 14 12:55:54 ruth kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000f>
v 14 12:55:54 ruth kernel: NX (Execute Disable) protection: active
v 14 12:55:54 ruth kernel: APIC: Static calls initialized
v 14 12:55:54 ruth kernel: SMBIOS 2.5 present.
v 14 12:55:54 ruth kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS >
v 14 12:55:54 ruth kernel: DMI: Memory slots populated: 0/0
v 14 12:55:54 ruth kernel: Hypervisor detected: KVM
v 14 12:55:54 ruth kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
v 14 12:55:54 ruth kernel: kvm-clock: using sched offset of 18197347230 c>
v 14 12:55:54 ruth kernel: clocksource: kvm-clock: mask: 0xffffffffffffff>
v 14 12:55:54 ruth kernel: tsc: Detected 2400.000 MHz processor
```

**La commande netstat -tuln permet d'afficher des informations relatives au réseau de votre système.**

```
(ruth@ruth)-[~/Bureau/cybersec]
$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
dp 0 0 0.0.0.0:39502 0.0.0.0:*
dp 0 0 10.0.2.15:3702 0.0.0.0:*
dp 0 0 239.255.255.250:3702 0.0.0.0:*
dp6 0 0 :::44588 :::*
dp6 0 0 fe80::a00:27ff:fe9:3702 :::*
dp6 0 0 ff02::c:3702 :::*

(ruth@ruth)-[~/Bureau/cybersec]
$ ss -tuln
Netid State Recv-Q Send-Q Peer Address:Port Local Address:Port
dp UNCONN 0 0 0.0.0.0:* 0.0.0.0:39502
dp UNCONN 0 0 0.0.0.0:* 10.0.2.15:3702
dp UNCONN 0 0 0.0.0.0:* 239.255.255.250:3702
dp UNCONN 0 0 *:44588
dp UNCONN 0 0 [fe80::a00:27ff:fe98:c7cf]:%eth0:3702
dp UNCONN 0 0 [::]:%eth0:3702
```

**La commande lspci**  
**qui répertorie tous les périphériques PCI d'un réseau.**

```
(ruth@ruth)-[~/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]
00:01.1 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/GBM/FR/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)
```

**L'installation de TraceRoute qui est un outil de diagnostic réseau utilise pour tracer le chemin emprunté par les paquets d'un ordinateur a une destination sur un réseau IP.**

```
(ruth@ruth)-[~/Bureau/cybersec]
$ sudo apt install traceroute
[sudo] Mot de passe de ruth :
traceroute est déjà la version la plus récente (1:2.1.6-1).
Les paquets suivants ont été installés automatiquement et ne sont plus néces
saires :
  imagemagick-6.q16      libhdf5-hl-100t64
  libbfiol               libjxl0.9
  libc++1-19             libmagickcore-6.q16-7-extra
  libc++abi1-19          libmagickcore-6.q16-7t64
  libcapstone4           libmagickwand-6.q16-7t64
  libconfig++9v5         libmbcrypto7t64
  libconfig9             libpaper1
  libdirectfb-1.7-7t64   libpoppler140
  libegl-dev            libqt5x11extras5
  libfmt9               libsuperlu6
  libgdal35             libtag1v5
  libgl1-mesa-dev       libtag1v5-vanilla
  libgles-dev           libtagc0
  libgles1              libunwind-19
  libglvnd-core-dev     libwebRTC-audio-processing1
  libglvnd-dev          libx265-209
  libgtksourceview-3.0-1 openjdk-23-jre
  libgtksourceview-3.0-common openjdk-23-jre-headless
  libgtksourceviewmm-3.0-0v5 python3-appdirs
  libhdf5-103-1t64
Veuillez utiliser « sudo apt autoremove » pour les supprimer.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(ruth@ruth)-[~/Bureau/cybersec]
$
```

**La commande date**  
**qui permet d'afficher la date et l'heure du système.**

```
Systeme de
(ruth@ruth)-[~/Bureau/cybersec]
$ date
ven 14 fév 2025 13:32:22 EST
```

### La commande timedatectl

qui permet d'afficher et de gérer les paramètres de date, d'heure et de fuseau horaire du système.

```
(ruth@ruth)-[~/Bureau/cybersec]
$ timedatectl
          Local time: ven 2025-02-14 13:32:38 EST
          Universal time: ven 2025-02-14 18:32:38 UTC
             RTC time: ven 2025-02-14 18:32:38
          Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

### La commande hostnamectl

qui permet de gérer le nom d'hôte du système et les paramètres associés.

### La commande sudo hostnamectl

qui permet de définir le nom d'hôte statique.

```
(ruth@ruth)-[~/Bureau/cybersec]
$ hostnamectl
Static hostname: ruth
          Icon name: computer-vm
          Chassis: vm 
          Machine ID: 834fa69da41442a5b4e3ab645b4a1cf9
          Boot ID: 3162463f60c641e89a431180b29ef0d2
  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 1d

(ruth@ruth)-[~/Bureau/cybersec]
$ sudo hostnamectl set-hostname ruthD

(ruth@ruth)-[~/Bureau/cybersec]
$
```

**Conclusion :**

**Ce devoir m'a permis d'apprendre à utiliser la virtualisation grâce au logiciel Virtual Box et apprendre à utiliser quelques courantes commandes via kali Linux en créant une machine virtuelle.**