

Université de Technologie D'Haïti

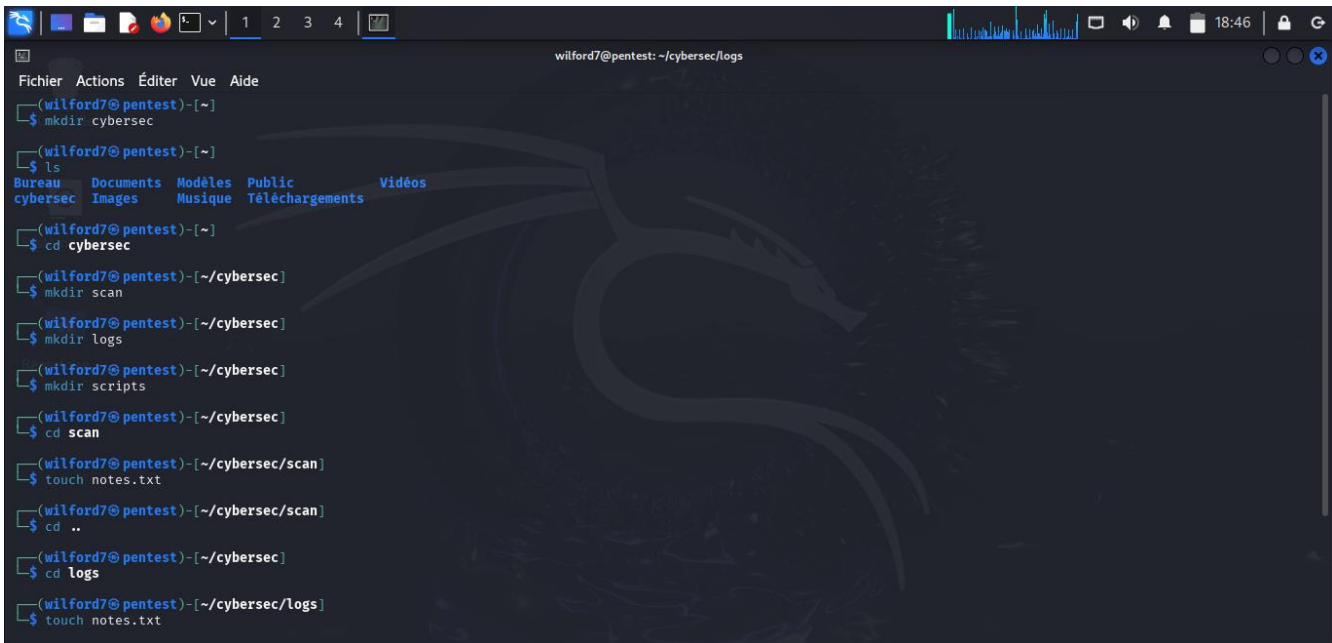
UNITECH

Titre : Virtualisation kali linux

Proposé par : Ismael SAINT AMOUR

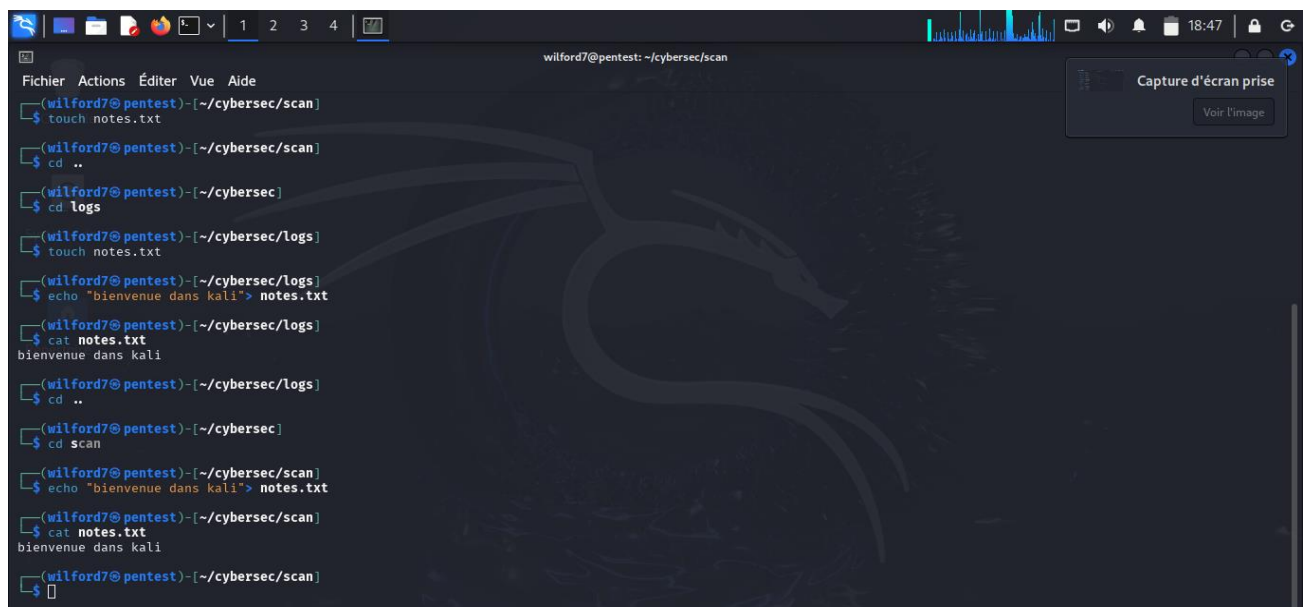
Préparé par : Wilford FONTIN

date: le 16/02/2025

A terminal window titled 'wilford7@pentest: ~/cybersec/logs' with a menu bar (Fichier, Actions, Éditer, Vue, Aide) and a Kali Linux dragon logo in the background. The terminal shows a sequence of commands: 'mkdir cybersec', 'ls', 'cd cybersec', 'mkdir scan', 'mkdir logs', 'mkdir scripts', 'cd scan', 'touch notes.txt', 'cd ..', 'cd logs', and 'touch notes.txt'.

```
wilford7@pentest: ~/cybersec/logs
Fichier Actions Éditer Vue Aide
(wilford7@pentest)-[~]
$ mkdir cybersec
(wilford7@pentest)-[~]
$ ls
Bureau Documents Modèles Public Vidéos
cybersec Images Musique Téléchargements
(wilford7@pentest)-[~]
$ cd cybersec
(wilford7@pentest)-[~/cybersec]
$ mkdir scan
(wilford7@pentest)-[~/cybersec]
$ mkdir logs
(wilford7@pentest)-[~/cybersec]
$ mkdir scripts
(wilford7@pentest)-[~/cybersec]
$ cd scan
(wilford7@pentest)-[~/cybersec/scan]
$ touch notes.txt
(wilford7@pentest)-[~/cybersec/scan]
$ cd ..
(wilford7@pentest)-[~/cybersec]
$ cd logs
(wilford7@pentest)-[~/cybersec/logs]
$ touch notes.txt
```

dans l'image ci-dessus vous pouvez voir des commandes comme:
mkdir : pour créer un dossier , ls: pour Lister les fichiers et dossiers dans le répertoire courant. , cd : Se déplacer vers un dossier spécifique , cd .. : pour remonter d'un niveau , touch : pour créer un fichier vide.

A terminal window titled 'wilford7@pentest: ~/cybersec/scan' with a menu bar and a Kali Linux dragon logo. It shows commands for creating 'notes.txt' in the 'scan' directory, moving to 'logs', creating 'notes.txt' there, and writing 'bienvenue dans kali' to it. The same sequence is repeated for the 'scan' directory. A 'Capture d'écran prise' (Screenshot taken) notification is visible in the top right corner.

```
wilford7@pentest: ~/cybersec/scan
Fichier Actions Éditer Vue Aide
(wilford7@pentest)-[~/cybersec/scan]
$ touch notes.txt
(wilford7@pentest)-[~/cybersec/scan]
$ cd ..
(wilford7@pentest)-[~/cybersec]
$ cd logs
(wilford7@pentest)-[~/cybersec/logs]
$ touch notes.txt
(wilford7@pentest)-[~/cybersec/logs]
$ echo "bienvenue dans kali"> notes.txt
(wilford7@pentest)-[~/cybersec/logs]
$ cat notes.txt
bienvenue dans kali
(wilford7@pentest)-[~/cybersec/logs]
$ cd ..
(wilford7@pentest)-[~/cybersec]
$ cd scan
(wilford7@pentest)-[~/cybersec/scan]
$ echo "bienvenue dans kali"> notes.txt
(wilford7@pentest)-[~/cybersec/scan]
$ cat notes.txt
bienvenue dans kali
(wilford7@pentest)-[~/cybersec/scan]
$
```

dans l' image 2, vous pouvez voir d'autres commandes comme :
echo,cat. Avec echo on peut ecrire dans un fichier vide et avec cat : on peut afficher le contenu d'un fichier.

```
wilford7@pentest: ~/cybersec/scripts
Fichier Actions Éditer Vue Aide
$ cat notes.txt
bienvenue dans kali

(wilford7@pentest)-[~/cybersec/logs]
$ cd ..

(wilford7@pentest)-[~/cybersec]
$ cd scan

(wilford7@pentest)-[~/cybersec/scan]
$ echo "bienvenue dans kali"> notes.txt

(wilford7@pentest)-[~/cybersec/scan]
$ cat notes.txt
bienvenue dans kali

(wilford7@pentest)-[~/cybersec/scan]
$ cp notes.txt ../scripts/

(wilford7@pentest)-[~/cybersec/scan]
$ cd ..

(wilford7@pentest)-[~/cybersec]
$ cd scripts

(wilford7@pentest)-[~/cybersec/scripts]
$ ls
notes.txt

(wilford7@pentest)-[~/cybersec/scripts]
$ mv notes.txt ../scan/

(wilford7@pentest)-[~/cybersec/scripts]
$
```

```
wilford7@pentest: ~/cybersec
Fichier Actions Éditer Vue Aide
(wilford7@pentest)-[~/cybersec]
$ cd scripts

(wilford7@pentest)-[~/cybersec/scripts]
$ ls
notes.txt

(wilford7@pentest)-[~/cybersec/scripts]
$ mv notes.txt ../scan/

(wilford7@pentest)-[~/cybersec/scripts]
$ rm notes.txt
rm: impossible de supprimer 'notes.txt': Aucun fichier ou dossier de ce nom

(wilford7@pentest)-[~/cybersec/scripts]
$ ls

(wilford7@pentest)-[~/cybersec/scripts]
$ cd ..

(wilford7@pentest)-[~/cybersec]
$ rm -r scan

(wilford7@pentest)-[~/cybersec]
$ rm -r logs

(wilford7@pentest)-[~/cybersec]
$ rm -r scripts

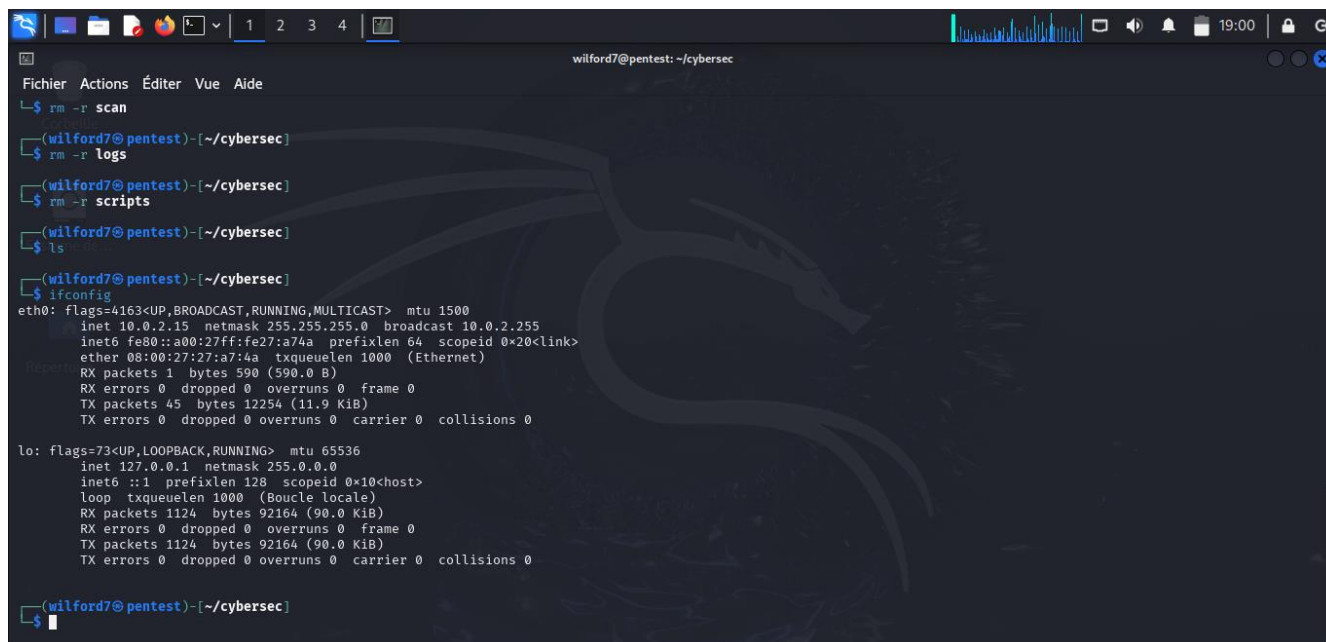
(wilford7@pentest)-[~/cybersec]
$ ls

(wilford7@pentest)-[~/cybersec]
$
```

Dans la 3eme image vous pouvez voir deux autres commandes , la commande cp et mv avec cp , vous pouvez copier un fichier et deplacer un dossier avec mv.

dans la 4eme image vous pouvez voir une autre commande , c'est la commande de suppression, rm pour supprimer un fichier , rm -r pour supprimer un dossier.

Avec ces commandes j'ai cree un dossier cybersec et trois sous dossier:scan,logs et scripts ,dans deux de ces sous dossier logs et scan, j'ai cree un fichier notes.txt puis je le copié dans le sous dossier scripts puis le deplacer dans scan . supprimer notes.txt dans scripts comme vous pouvez le constater il me donne une erreur impossible de supprimer le fichier, parce qu'il n'existe pas car il etait déjà déplacé pour finir avec la commande rm -r j'ai supprimé les sous dossiers.



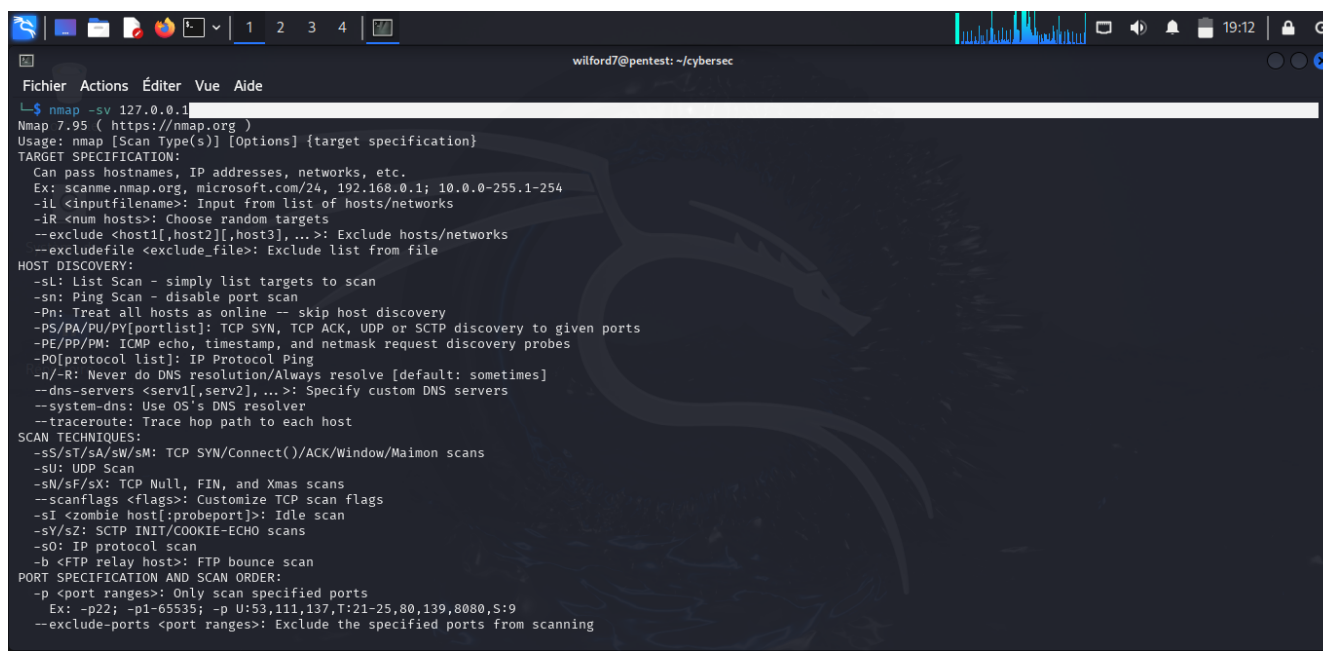
```
wilford7@pentest: ~/cybersec
$ rm -r scan
$ rm -r logs
$ rm -r scripts
$ ls
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe27:a74a  prefixlen 64  scopeid 0<20<link>
    ether 08:00:27:27:a7:4a  txqueuelen 1000  (Ethernet)
    RX packets 1  bytes 590 (590.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 45  bytes 12254 (11.9 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  (Boucle locale)
    RX packets 1124  bytes 92164 (90.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 1124  bytes 92164 (90.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

$
```

Dans l'image ci-dessus (image 5), la commande ifconfig permet d'Afficher les informations réseau.

la commande nmap dans l'image ci-dessous (image 6) permet de Scanner des ports et des services sur une machine.



```
wilford7@pentest: ~/cybersec
$ nmap -sv 127.0.0.1
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```

dans l'image ci-dessous j'ai cree un fichier secret.txt avec la commande touch puis avec la commande chmod 400 je donne la permission à l'utilisateur de lire le fichier puis j'utilise la commande grep pour rechercher (dans) dans le fichier log.txt.

```
wilford7@pentest: ~/cybersec
Fichier Actions Éditer Vue Aide

(wilford7@pentest)~/cybersec
$ touch secret.txt

(wilford7@pentest)~/cybersec
$ chmod 400 secret.txt

(wilford7@pentest)~/cybersec
$ ls -l secret.txt
-r----- 1 wilford7 wilford7 0 13 fév 19:25 secret.txt

(wilford7@pentest)~/cybersec
$ touch log.txt

(wilford7@pentest)~/cybersec
$ echo "bienvenue\n dans\n le monde\n kali"> log.txt

(wilford7@pentest)~/cybersec
$ grep "dans" log.txt
dans

(wilford7@pentest)~/cybersec
$ cat log.txt
bienvenue
dans
le monde
kali

(wilford7@pentest)~/cybersec
$

(wilford7@pentest)~/cybersec
$
```

```
wilford7@pentest: ~/cybersec
Fichier Actions Éditer Vue Aide

(wilford7@pentest)~/cybersec
$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                925M    0  925M   0% /dev
tmpfs               198M   980K  197M   1% /run
/dev/sda1           47G    19G   27G  42% /
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  520K  987M   1% /tmp
tmpfs               1,0M    0  1,0M   0% /run/credentials/getty@tty1.service
tmpfs               198M  116K  198M   1% /run/user/1000

(wilford7@pentest)~/cybersec
$ du -sh
8,0K .

(wilford7@pentest)~/cybersec
$ free -h
Mem:              total        utilisé       libre   partagé  tamp/cache  disponible
Échange:          2,0Gi         0B          2,0Gi         10Mi        991Mi         1,3Gi

(wilford7@pentest)~/cybersec
$

(wilford7@pentest)~/cybersec
$

(wilford7@pentest)~/cybersec
$
```


Dans l'image ci-dessous la commande ps aux permet d'afficher les processus en cours.

```
wilford7@pentest: ~/cybersec
Fichier Actions Éditer Vue Aide
(wilford7@pentest)-[~/cybersec]
$ ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root             1  0.1  0.6 22984 14056 ?        Ss   18:17   0:05 /sbin/init splash
root             2  0.0  0.0      0     0 ?        S    18:17   0:00 [kthreadd]
root             3  0.0  0.0      0     0 ?        S    18:17   0:00 [pool_workqueue_release]
root             4  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-rcu_gp]
root             5  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-sync_wq]
root             6  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-slub_flushwq]
root             7  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-netns]
root            12  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-mm_percpu_wq]
root            13  0.0  0.0      0     0 ?        I    18:17   0:00 [rcu_tasks_kthread]
root            14  0.0  0.0      0     0 ?        I    18:17   0:00 [rcu_tasks_rude_kthread]
root            15  0.0  0.0      0     0 ?        I    18:17   0:00 [rcu_tasks_trace_kthread]
root            16  0.1  0.0      0     0 ?        S    18:17   0:06 [ksoftirqd/0]
root            17  0.1  0.0      0     0 ?        I    18:17   0:08 [rcu_preempt]
root            18  0.0  0.0      0     0 ?        S    18:17   0:00 [rcu_exp_par_gp_kthread_worker/0]
root            19  0.0  0.0      0     0 ?        S    18:17   0:00 [rcu_exp_gp_kthread_worker]
root            20  0.0  0.0      0     0 ?        S    18:17   0:00 [migration/0]
root            21  0.0  0.0      0     0 ?        S    18:17   0:00 [idle_inject/0]
root            22  0.0  0.0      0     0 ?        S    18:17   0:00 [cpuhp/0]
root            24  0.0  0.0      0     0 ?        S    18:17   0:00 [kdevtmpfs]
root            25  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-inet_frag_wq]
root            27  0.0  0.0      0     0 ?        S    18:17   0:00 [kauditd]
root            28  0.0  0.0      0     0 ?        S    18:17   0:00 [khungtaskd]
root            29  0.0  0.0      0     0 ?        S    18:17   0:00 [oom_reaper]
root            31  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-writeback]
root            32  0.0  0.0      0     0 ?        S    18:17   0:01 [kcompactd0]
root            33  0.0  0.0      0     0 ?        SN   18:17   0:00 [ksmd]
root            34  0.0  0.0      0     0 ?        SN   18:17   0:00 [khugepaged]
root            35  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-kintegrityd]
root            36  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-blkcg]
root            37  0.0  0.0      0     0 ?        I<   18:17   0:00 [kworker/R-blkcg_punt_bio]
root            38  0.0  0.0      0     0 ?        S    18:17   0:00 [irq/9-acpi]
```

```
wilford7@pentest: ~/cybersec
Fichier Actions Éditer Vue Aide
wilford7 47163 175 0.2 9608 4320 pts/0 R+ 19:51 0:00 ps aux

(wilford7@pentest)-[~/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)

(wilford7@pentest)-[~/cybersec]
$ sudo apt install traceroute
[sudo] Mot de passe de wilford7 :
traceroute est déjà la version la plus récente (1:2.1.6-1).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  imagemagick-6.q16 libconfig9 libgles1 libhdf5-hl-100t64 libpaper1 libunwind-19
  libbfiol libdirectfb-1.7-t64 libglvnd-core-dev libjxl0.9 libqt5x11extras5 libwebRTC-audio-processing1
  libcapstone4 libgl-dev libglvnd-dev libmagickcore-6.q16-7-extra libsuperlu6 libx265-209
  libconfig+9v5 libgles-dev libgtksourceview-3.0-1 libmagickcore-6.q16-7t64 libtag1v5 python3-appdirs
  libcapstone4 libgl-mesa-dev libgtksourceview-3.0-common libmagickwand-6.q16-7t64 libtag1v5-vanilla
  libconfig+9v5 libgles-dev libgtksourceviewmm-3.0-0v5 libmbedcrypto7t64 libtagc0
Veuillez utiliser « sudo apt autoremove » pour les supprimer.

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

(wilford7@pentest)-[~/cybersec]
$
```

```
PS> wilford7@GFpenlove: /home/wilford7

Fichier Actions Éditer Vue Aide
└─ps> traceroute google.com
traceroute to google.com (142.250.64.174), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  9.305 ms  0.461 ms  0.420 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  * * *
```

```
wilford7@pentest: ~/cybersec

Fichier Actions Éditer Vue Aide

(wilford7@pentest)-[~/cybersec]
$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat

(wilford7@pentest)-[~/cybersec]
$ ss -tuln
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port

(wilford7@pentest)-[~/cybersec]
$ journalctl
fév 07 12:43:54 pentest kernel: Linux version 6.11.2-amd64 (dev@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-6) 14.2.0, GNU ld (GNU Binutils for Debian) 2.43.1)
fév 07 12:43:54 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=b2a560a6-7787-4b88-8285-c2a4d5174de4 ro quiet splash
fév 07 12:43:54 pentest kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
fév 07 12:43:54 pentest kernel: BIOS-provided physical RAM map:
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x0000000007fff0000-0x0000000007ffffff] ACPI data
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee0ffff] reserved
fév 07 12:43:54 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] reserved
fév 07 12:43:54 pentest kernel: NX (Execute Disable) protection: active
fév 07 12:43:54 pentest kernel: APIC: Static calls initialized
fév 07 12:43:54 pentest kernel: SMBIOS 2.5 present.
fév 07 12:43:54 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
fév 07 12:43:54 pentest kernel: DMI: Memory slots populated: 0/0
fév 07 12:43:54 pentest kernel: Hypervisor detected: KVM
fév 07 12:43:54 pentest kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
fév 07 12:43:54 pentest kernel: kvm-clock: using sched offset of 63535414143 cycles
fév 07 12:43:54 pentest kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
fév 07 12:43:54 pentest kernel: tsc: Detected 1347.472 MHz processor
fév 07 12:43:54 pentest kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```



```
wilford7@pentest: ~/cybersec

Fichier Actions Éditer Vue Aide

fév 07 12:44:47 pentest dbus-daemon[780]: [session uid=127 pid=780] Activating via systemd: service name='org.ally.Bus' unit='at-spi-dbus-bus.service' requested by '':>
fév 07 12:44:47 pentest systemd[755]: Starting at-spi-dbus-bus.service - Accessibility services bus ...
fév 07 12:44:47 pentest wireplumber[777]: default: Failed to get percentage from UPower: org.freedesktop.DBus.Error.NameHasNoOwner
fév 07 12:44:47 pentest wireplumber[777]: spa.bluez5: BlueZ system service is not available
fév 07 12:44:47 pentest dbus-daemon[780]: [session uid=127 pid=780] Successfully activated service 'org.ally.Bus'
fév 07 12:44:47 pentest systemd[755]: Started at-spi-dbus-bus.service - Accessibility services bus.
fév 07 12:44:47 pentest wireplumber[777]: wp-device: SPA handle 'api.libcamera.enum.manager' could not be loaded; is it installed?
fév 07 12:44:47 pentest wireplumber[777]: s-monitors-libcamera: PipeWire's libcamera SPA plugin is missing or broken. Some camera types may not be supported.
fév 07 12:44:48 pentest dbus-daemon[780]: [session uid=127 pid=780] Activating via systemd: service name='org.gtk.vfs.Daemon' unit='gvfs-daemon.service' requested by '>
fév 07 12:44:48 pentest systemd[755]: Starting gvfs-daemon.service - Virtual filesystem service ...
fév 07 12:44:48 pentest dbus-daemon[780]: [session uid=127 pid=780] Successfully activated service 'org.gtk.vfs.Daemon'
fév 07 12:44:48 pentest systemd[755]: Started gvfs-daemon.service - Virtual filesystem service.
fév 07 12:44:52 pentest systemd[1]: systemd-hostnamed.service: Deactivated successfully.
fév 07 12:44:56 pentest at-spi-bus-launcher[818]: dbus-daemon[818]: Activating service name='org.ally.atspi.Registry' requested by ':1.0' (uid=127 pid=779 comm="/usr/>
fév 07 12:44:56 pentest at-spi-bus-launcher[818]: dbus-daemon[818]: Successfully activated service 'org.ally.atspi.Registry'
fév 07 12:44:56 pentest at-spi-bus-launcher[853]: SpiRegistry daemon is running with well-known name - org.ally.atspi.Registry
fév 07 12:45:01 pentest CRON[857]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 07 12:45:01 pentest CRON[858]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 07 12:45:01 pentest CRON[857]: pam_unix(cron:session): session closed for user root
fév 07 12:45:36 pentest lightdm[861]: gkr-pam: unable to locate daemon control file

(wilford7@pentest)~(~/cybersec)
$ journalctl -f
fév 13 10:45:01 pentest CRON[43829]: pam_unix(cron:session): session closed for user root
fév 13 10:55:01 pentest CRON[48804]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 13 10:55:01 pentest CRON[48806]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 13 10:55:01 pentest CRON[48804]: pam_unix(cron:session): session closed for user root
fév 13 10:56:54 pentest sudo[49428]: wilford7 : TTY=pts/0 ; PWD=/home/wilford7/cybersec ; USER=root ; COMMAND=/usr/bin/apt install traceroute
fév 13 10:56:54 pentest sudo[49428]: pam_unix(sudo:session): session opened for user root(uid=0) by wilford7(uid=1000)
fév 13 10:57:22 pentest sudo[49428]: pam_unix(sudo:session): session closed for user root
fév 13 20:05:01 pentest CRON[53863]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 13 20:05:01 pentest CRON[53865]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 13 20:05:01 pentest CRON[53863]: pam_unix(cron:session): session closed for user root
```

```
PS> wilford7@pentest: /home/wilford7

Fichier Actions Éditer Vue Aide

Screenshot_2025-02-13_19_16_53.png Screenshot_2025-02-13_20_07_37.png

(wilford7@pentest)~(~/home/wilford7)
PS> traceroute google.com
google.com: Échec temporaire dans la résolution du nom
Cannot handle "host" cmdline arg 'google.com' on position 1 (argc 1)

(wilford7@pentest)~(~/home/wilford7)
PS> journalctl -b
fév 14 10:16:55 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org)>
fév 14 10:16:55 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11>
fév 14 10:16:55 pentest kernel: [Firmware Bug]: TSC doesn't count with P0 f>
fév 14 10:16:55 pentest kernel: BIOS-provided physical RAM map:
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x00000000000009fc00-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x000000000000f00000-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x0000000007fff0000-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x000000>
fév 14 10:16:55 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x000000>
fév 14 10:16:55 pentest kernel: NX (Execute Disable) protection: active
fév 14 10:16:55 pentest kernel: APIC: Static calls initialized
fév 14 10:16:55 pentest kernel: SMBIOS 2.5 present.
fév 14 10:16:55 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, Bi>
fév 14 10:16:55 pentest kernel: DMI: Memory slots populated: 0/0
fév 14 10:16:55 pentest kernel: Hypervisor detected: KVM
fév 14 10:16:55 pentest kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00>
fév 14 10:16:55 pentest kernel: kvm-clock: using sched offset of 2505624006>
fév 14 10:16:55 pentest kernel: clocksource: kvm-clock: mask: 0xfffffffffff>
fév 14 10:16:55 pentest kernel: tsc: Detected 1347.470 MHz processor
lines 1-22... skipping...
fév 14 10:16:55 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org)>
fév 14 10:16:55 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=b2a560a6-7787-4b88-8285-c2a4d5174de4 ro quiet splash
```

```
PS> journalctl -n 10
fév 14 10:35:58 pentest kernel: 15:35:58.732619 X11 events Monitor 0 (w,h)=(1366,657) (x,y)=(0,0)
fév 14 10:35:58 pentest kernel: 15:35:58.754682 X11 events Sending monitor positions (8 of them) to the host: VINF_SUCCESS
fév 14 10:35:58 pentest kernel: 15:35:58.808117 X11 events received X11 event (89)
fév 14 10:35:58 pentest kernel: 15:35:58.817037 X11 events RRSscreenChangeNotify event received
fév 14 10:35:59 pentest kernel: 15:35:59.537934 X11 events Monitor 0 (w,h)=(1366,657) (x,y)=(0,0)
fév 14 10:35:59 pentest kernel: 15:35:59.562204 X11 events Sending monitor positions (8 of them) to the host: VINF_SUCCESS
fév 14 10:36:04 pentest dbus-daemon[887]: [session uid=1000 pid=887 pidfd=5] Activating via systemd: service name='org.xfce.Xfconf' unit='xfconfd.service' requested b
fév 14 10:36:04 pentest systemd[858]: Starting xfconfd.service - Xfce configuration service...
fév 14 10:36:04 pentest dbus-daemon[887]: [session uid=1000 pid=887 pidfd=5] Successfully activated service 'org.xfce.Xfconf'
fév 14 10:36:04 pentest systemd[858]: Started xfconfd.service - Xfce configuration service.

(wilford7@pentest)-[/home/wilford7]
PS> date
ven 14 fév 2025 10:40:05 EST

(wilford7@pentest)-[/home/wilford7]
PS> timedatectl
    Local time: ven 2025-02-14 10:41:00 EST
    Universal time: ven 2025-02-14 15:41:00 UTC
    RTC time: ven 2025-02-14 15:40:59
    Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
    NTP service: inactive
    RTC in local TZ: no

(wilford7@pentest)-[/home/wilford7]
PS>

(wilford7@pentest)-[/home/wilford7]
PS>

(wilford7@pentest)-[/home/wilford7]
PS>
```

```
PS> date
ven 14 fév 2025 10:40:05 EST

(wilford7@pentest)-[/home/wilford7]
PS> timedatectl
    Local time: ven 2025-02-14 10:41:00 EST
    Universal time: ven 2025-02-14 15:41:00 UTC
    RTC time: ven 2025-02-14 15:40:59
    Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
        NTP service: inactive
    RTC in local TZ: no

(wilford7@pentest)-[/home/wilford7]
PS>

(wilford7@pentest)-[/home/wilford7]
PS>

(wilford7@pentest)-[/home/wilford7]
PS> hostnamectl
Static hostname: pentest
    Icon name: computer-vm
    Chassis: vm
    Machine ID: 212cb9c679c241afa809bc7737df26af
    Boot ID: c48b263a2e034ac5b078ac9db29f9efb
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
```

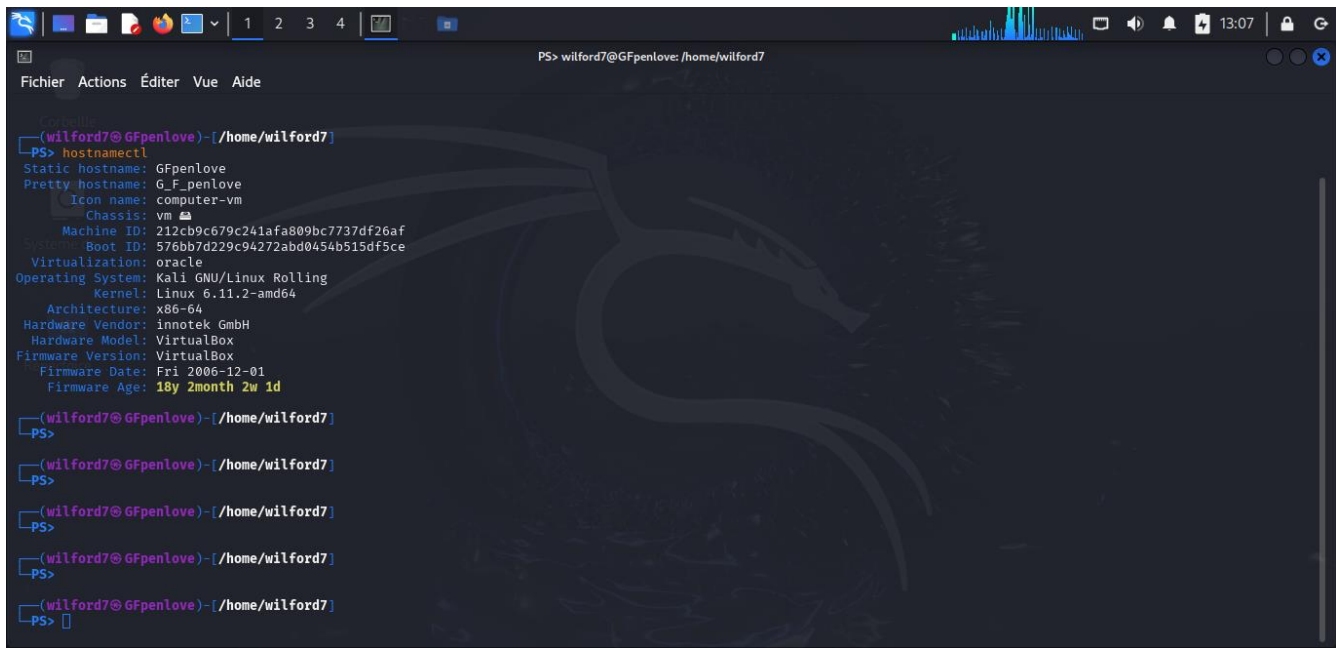
```
Fichier Actions Éditer Vue Aide
Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
NTP service: inactive
RTC in local TZ: no

(wilford7@pentest)-[/home/wilford7]
PS> hostnamectl
Static hostname: pentest
Icon name: computer-vm
Chassis: vm
Machine ID: 212cb9c679c241afa809bc7737df26af
Boot ID: c48b263a2e034ac5b078ac9db29f9efb
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.11.2-amd64
Architecture: x86_64
Hardware Vendor: Innatek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
Firmware Date: Fri 2006-12-01
Firmware Age: 18y 2month 2w 1d

(wilford7@pentest)-[/home/wilford7]
PS> sudo hostnamectl set-hostname G_F_penlove
[sudo] Mot de passe de wilford7 :

(wilford7@G_F_penlove)-[/home/wilford7]
PS>
```

Hostnamectl pour afficher l'information et `sudo hostnamectl set-hostname [nouveau_nom]` pour changer le nom.



The image shows a terminal window from a Kali Linux virtual machine. The window title is "PS> wilford7@GFpenlove: /home/wilford7". The menu bar includes "Fichier", "Actions", "Éditer", "Vue", and "Aide". The terminal output shows the command `hostnamectl` being executed, which displays system information: Static hostname: GFpenlove, Pretty hostname: G_F_penlove, Icon name: computer-vm, Chassis: vm, Machine ID: 212cb9c679c241afa809bc7737df26af, Systemd Boot ID: 576bb7d229c94272abd0454b515df5ce, 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, and Firmware Age: 18y 2month 2w 1d. Following this, there are five repeated prompts `(wilford7@GFpenlove)-[/home/wilford7]` and `PS>` without any further input or output.

```
(wilford7@GFpenlove)-[/home/wilford7]
PS> hostnamectl
Static hostname: GFpenlove
Pretty hostname: G_F_penlove
Icon name: computer-vm
Chassis: vm
Machine ID: 212cb9c679c241afa809bc7737df26af
Systemd Boot ID: 576bb7d229c94272abd0454b515df5ce
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

(wilford7@GFpenlove)-[/home/wilford7]
PS>

(wilford7@GFpenlove)-[/home/wilford7]
PS>

(wilford7@GFpenlove)-[/home/wilford7]
PS>

(wilford7@GFpenlove)-[/home/wilford7]
PS>

(wilford7@GFpenlove)-[/home/wilford7]
PS>
```

En conclusion ce td nous permet d'interagir avec kali et d'apprendre les commandes.