

Universite de Technologie d'Haiti
Devoire de cyber de securite

Nom Dorceus

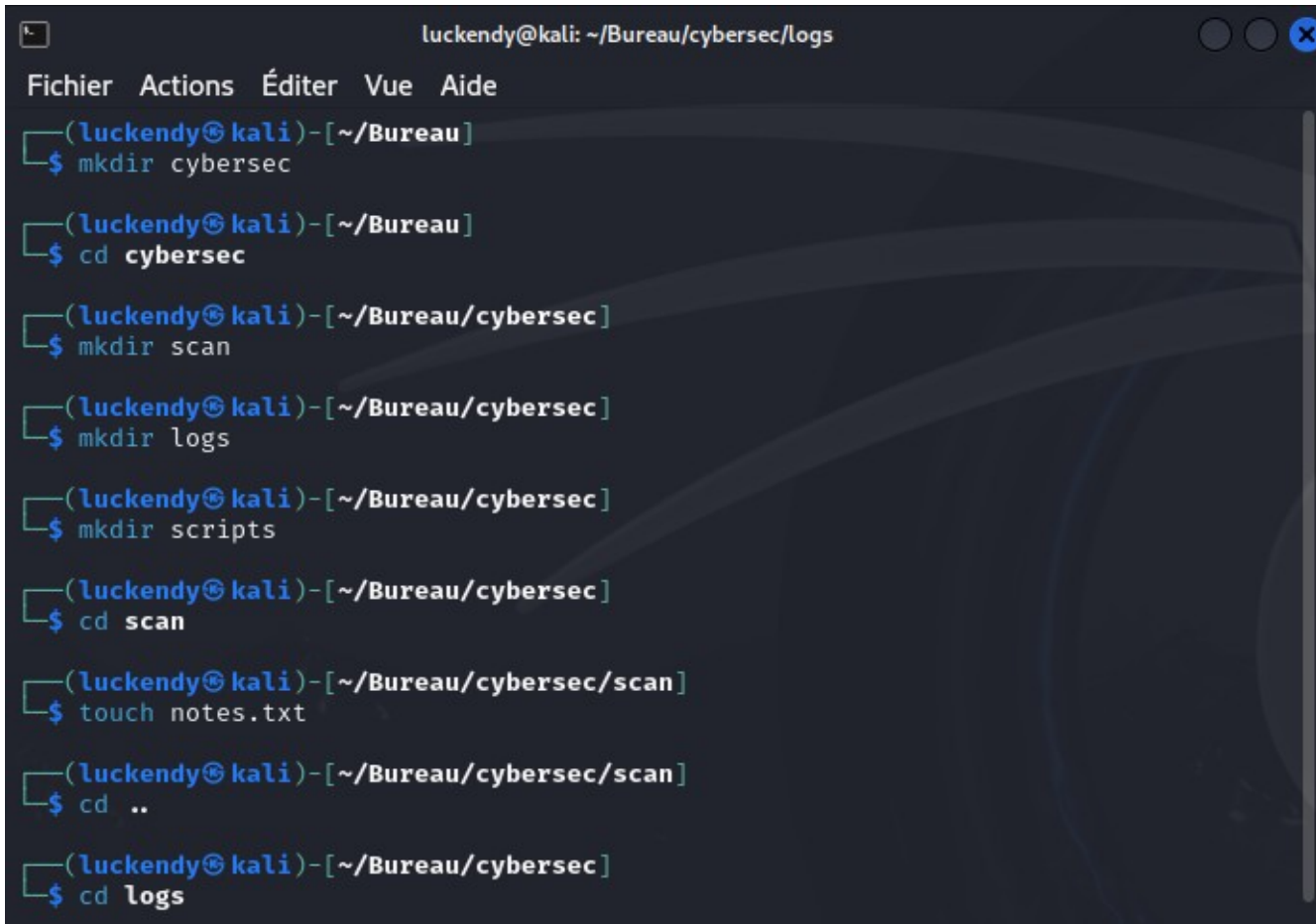
Prenom Luckendy

Option SC Informatique

Niveau 4em annee

Prof

Ce commande mkdir cybersec permet de cree un dossier cybersec

A terminal window with a dark background and light blue text. The title bar at the top reads 'luckendy@kali: ~/Bureau/cybersec/logs'. Below the title bar is a menu bar with the items 'Fichier', 'Actions', 'Éditer', 'Vue', and 'Aide'. The terminal shows a series of commands and their outputs, with the current directory path shown in brackets after the prompt. The commands are: 'mkdir cybersec' (moving from ~/Bureau to ~/Bureau/cybersec), 'cd cybersec', 'mkdir scan' (moving from ~/Bureau/cybersec to ~/Bureau/cybersec/scan), 'mkdir logs', 'mkdir scripts', 'cd scan', 'touch notes.txt', 'cd ..' (moving from ~/Bureau/cybersec/scan to ~/Bureau/cybersec), and 'cd logs' (moving from ~/Bureau/cybersec to ~/Bureau/cybersec/logs).

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

La commande cd ~ permet de retourner
cat permet d'afficher une contenu dans un fichier

```
(luckendy@kali)-[~/Bureau/cybersec]
$ cd scan

(luckendy@kali)-[~/Bureau/cybersec/scan]
$ cat notes.txt
Bonjour

(luckendy@kali)-[~/Bureau/cybersec/scan]
$ cd ..

(luckendy@kali)-[~/Bureau/cybersec]
$ cd logs

(luckendy@kali)-[~/Bureau/cybersec/logs]
$ cat notes.txt
Bonjour

(luckendy@kali)-[~/Bureau/cybersec/logs]
$
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ cd ~

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

(luckendy@kali)-[~]
$
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ ls -l ~/Bureau/cybersec/scripts/
total 4
-rw-rw-r-- 1 luckendy luckendy 8 15 fév 12:14 notes.txt
```

```
(luckendy@kali)~$ mv ~/Bureau/cybersec/scripts/notes.txt ~/Bureau/cybersec/notes.txt
(luckendy@kali)~$ ls -l ~
total 0
(luckendy@kali)~$ ls -l ~/Bureau/cybersec/scripts/
total 0
(luckendy@kali)~$ ls -l ~
total 4
-rw-rw-r-- 1 luckendy luckendy 8 15 fév 11:44 notes.txt
(luckendy@kali)~$
```

(luckendy@kali)-[~/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 fe80::a00:27ff:feca:7ba9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ca:7b:a9 txqueuelen 1000 (Ethernet)
    RX packets 5117 bytes 4944803 (4.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2764 bytes 456077 (445.3 KiB)
    TX errors 0 dropped 11 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 22 bytes 1856 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 1856 (1.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(luckendy@kali)-[~/Bureau/cybersec]

\$

(luckendy@kali)-[~/Bureau/cybersec]

\$ df -h

Sys. de fichiers	Taille	Utilisé	Dispo	Uti%	Monté sur
udev	926M	0	926M	0%	/dev
tmpfs	198M	996K	197M	1%	/run
/dev/sda1	38G	17G	20G	46%	/
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-udev-load-crede
ntials.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	36K	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	112K	198M	1%	/run/user/1000
tmpfs	1,0M	0	1,0M	0%	/run/credentials/systemd-journald.servic
e					

(luckendy@kali)-[~/Bureau/cybersec]

\$ nmap -sn 10.0.2.15

Starting Nmap 7.94SVN (<https://nmap.org>) at 2025-02-15 13:45 EST

Nmap scan report for 10.0.2.15

Host is up.

Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds

(luckendy@kali)-[~/Bureau/cybersec]

\$ █


```
(luckendy@kali)-[~/Bureau/cybersec]
$ echo "ce fichier est secret" > secret.txt

(luckendy@kali)-[~/Bureau/cybersec]
$ chmod 400 secret.txt

(luckendy@kali)-[~/Bureau/cybersec]
$ ls -l secret.txt
-r----- 1 luckendy luckendy 22 15 fév 13:55 secret.txt

(luckendy@kali)-[~/Bureau/cybersec]
$ echo -e "voici une ligne.\nCeci est un test.\nGrep est un outil puissant.\nIl est facile a utiliser." > 10g.txt

(luckendy@kali)-[~/Bureau/cybersec]
$ grep "test" 10g.txt
Ceci est un test.

(luckendy@kali)-[~/Bureau/cybersec]
$ grep -i "test" 10g.txt
Ceci est un test.

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

```
(luckendy@kali)-[~/Bureau/cybersec]
$ top -sh

Usage:
top [options]

Options:
-b, --batch-mode           run in non-interactive batch mode
-c, --cmdline-toggle       reverse last remembered 'c' state
-d, --delay =SECS [.TENTHS] iterative delay as SECS [.TENTHS]
-E, --scale-summary-mem =SCALE set mem as: k,m,g,t,p,e for SCALE
-e, --scale-task-mem =SCALE  set mem with: k,m,g,t,p for SCALE
-H, --threads-show        show tasks plus all their threads
-i, --idle-toggle         reverse last remembered 'i' state
-n, --iterations =NUMBER  exit on maximum iterations NUMBER
-O, --list-fields          output all field names, then exit
-o, --sort-override =FIELD force sorting on this named FIELD
-p, --pid =PIDLIST        monitor only the tasks in PIDLIST
-S, --accum-time-toggle   reverse last remembered 'S' state
-s, --secure-mode         run with secure mode restrictions
-U, --filter-any-user =USER show only processes owned by USER
-u, --filter-only-euser =USER show only processes owned by USER
-w, --width [=COLUMNS]   change print width [,use COLUMNS]
```

```
(luckendy@kali)-[~/Bureau/cybersec]  
$ free -h
```

	total	utilisé	libre	partagé	tamp/cache	disponible
Mem:	1,9Gi	1,0Gi	201Mi	22Mi	877Mi	915Mi
Échange:	2,0Gi	60Mi	1,9Gi			

```
(luckendy@kali)-[~/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/FBM/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)
```



```
(luckendy@kali)-[~/Bureau/cybersec]
$ sudo apt install traceroute
[sudo] Mot de passe de luckendy :
traceroute est déjà la version la plus récente (1:2.1.6-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1220
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ traceroute google.com
ngoogle.com: Échec temporaire dans la résolution du nom
Cannot handle "host" cmdline arg `google.com' on position 1 (argc 1)
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ netstar -tuln
La commande « netstar » n'a pas été trouvée, voulez-vous dire :
  commande « netstat » du deb net-tools
Essayez : sudo apt install <nom du deb>
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ ss -tuln
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
-------	-------	--------	--------	--------------------	-------------------

```
(luckendy@kali)-[~/Bureau/cybersec]
```

```
$ journalctl -f
```

```
fév 15 14:17:01 kali CRON[88333]: pam_unix(cron:session): session closed for user root
fév 15 14:21:04 kali sudo[90164]: luckendy : TTY=pts/0 ; PWD=/home/luckendy/Bureau/cybersec ; USER=root ; COMMAND=/usr/bin/apt install traceroute
fév 15 14:21:04 kali sudo[90164]: pam_unix(sudo:session): session opened for user root(uid=0) by luckendy(uid=1000)
fév 15 14:21:04 kali sudo[90164]: pam_unix(sudo:session): session closed for user root
fév 15 14:22:04 kali kernel: e1000: eth0 NIC Link is Down
fév 15 14:22:08 kali kernel: e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
fév 15 14:22:08 kali NetworkManager[589]: <info> [1739647328.2293] device (eth0): carrier: link connected
fév 15 14:25:01 kali CRON[92372]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 15 14:25:01 kali CRON[92373]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 15 14:25:01 kali CRON[92372]: pam_unix(cron:session): session closed for user root
```

```
(luckendy@kali)-[~/Bureau/cybersec]
```

```
$ journalctl -n 10
```

```
La commande « journalctl » n'a pas été trouvée, voulez-vous dire :
  commande « journalctl » du deb systemd
Essayez : sudo apt install <nom du deb>
```

```
(luckendy@kali)-[~/Bureau/cybersec]
```

```
$ date
```

```
sam 15 fév 2025 14:38:43 EST
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ timedatectl
    Local time: sam 2025-02-15 14:39:43 EST
    Universal time: sam 2025-02-15 19:39:43 UTC
        RTC time: sam 2025-02-15 19:27:13
        Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
        NTP service: inactive
    RTC in local TZ: no
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ hostnamectl
Static hostname: kali
    Icon name: computer-vm
    Chassis: vm 🖥️
    Machine ID: dd4b2a54598b49d8adb03b0e78b92e27
    Boot ID: 3bc60613b0b14211bcd714a53e1ac81
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 2d
```

```
(luckendy@kali)-[~/Bureau/cybersec]
$ sudo hostnamectl set-hostname [securite]
[sudo] Mot de passe de luckendy :
```

conclusion

En conclusion, les etapes que nous avons suivies nous aident a apprendre a gerer des fichiers, a analyser des reseaux, et a manipulerles permission et l'etat du systeme sur linux

