Nom : Dupoux

Prénom : Andy Jefferson

Option : Sciences informatiques

Cours : Cyber-Sécurité

Date : 16/02/2025

File   Machine   View   Input   Devices   Help

1   2   3   4

canopus@Canopus: ~

File   Actions   Edit   View   Help

```
┌──(canopus㊉Canopus)-[~]
└─$ sudo apt upgrade
[sudo] password for canopus:
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(canopus㊉Canopus)-[~]
└─$ sudo apt upgrade -y
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(canopus㊉Canopus)-[~]
└─$ sudo apt dist-upgrade -y
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(canopus㊉Canopus)-[~]
└─$ pwd
/home/canopus

┌──(canopus㊉Canopus)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(canopus㊉Canopus)-[~]
└─$ ▮
```

Right Ctrl

canopus@Canopus: ~/Desktop/cybersec

File   Actions   Edit   View   Help

```
┌──(canopus㊉Canopus)-[~]
└─$ cd Desktop

┌──(canopus㊉Canopus)-[~/Desktop]
└─$ mkdir c

┌──(canopus㊉Canopus)-[~/Desktop]
└─$ rm -r c

┌──(canopus㊉Canopus)-[~/Desktop]
└─$ mkdir cybersec

┌──(canopus㊉Canopus)-[~/Desktop]
└─$ cd cybersec

┌──(canopus㊉Canopus)-[~/Desktop/cybersec]
└─$ mkdir scan

┌──(canopus㊉Canopus)-[~/Desktop/cybersec]
└─$ mkdir logs

┌──(canopus㊉Canopus)-[~/Desktop/cybersec]
└─$ mkdir scripts

┌──(canopus㊉Canopus)-[~/Desktop/cybersec]
└─$ cd scan

┌──(canopus㊉Canopus)-[~/Desktop/cybersec/scan]
└─$ touch notes.txt

┌──(canopus㊉Canopus)-[~/Desktop/cybersec/scan]
└─$ cd logs
cd: no such file or directory: logs
```

```
┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ touch notes.txt

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ cd logs
cd: no such file or directory: logs

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ cd ..
Could not find command-not-found database. Run 'sudo apt update' to populate it.
cd..: command not found

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ cd~
Could not find command-not-found database. Run 'sudo apt update' to populate it.
cd~: command not found

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ cd ~

┌──(canopus㊀Canopus)-[~]
└─$ cd Desktop

┌──(canopus㊀Canopus)-[~/Desktop]
└─$ cd cybersec

┌──(canopus㊀Canopus)-[~/Desktop/cybersec]
└─$ cd logs

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/logs]
└─$ touch notes.txt

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/logs]
└─$
```

```
┌──(canopus㊀Canopus)-[~/Desktop/cybersec/logs]
└─$ echo"bonjour, je m'appelle Dupoux andy jefferson" notes.txt
Could not find command-not-found database. Run 'sudo apt update' to populate it.
echobonjour, je m'appelle Dupoux andy jefferson: command not found

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/logs]
└─$ echo "bonjour, je m'appelle Dupoux andy jefferson" > notes.txt

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/logs]
└─$ cat notes.txt
bonjour, je m'appelle Dupoux andy jefferson

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/logs]
└─$ cd ..

┌──(canopus㊀Canopus)-[~/Desktop/cybersec]
└─$ cd scan

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ echo "bonjour, comment allez-vous" > notes.txt

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$ cat notes.txt
bonjour, comment allez-vous

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$

┌──(canopus㊀Canopus)-[~/Desktop/cybersec/scan]
└─$
```

```
canopus@Canopus: ~/Desktop/cybersec

File  Actions  Edit  View  Help

┌──(canopus㉿Canopus)-[~]
└─$ cd Desktop

┌──(canopus㉿Canopus)-[~/Desktop]
└─$ cd cybersec

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ cp ~/Desktop/cybersec/scan/notes.txt ~/Desktop/cybersec/scripts

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ █
```
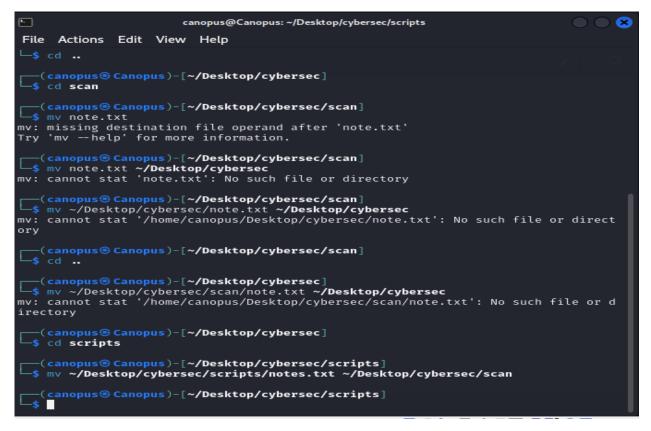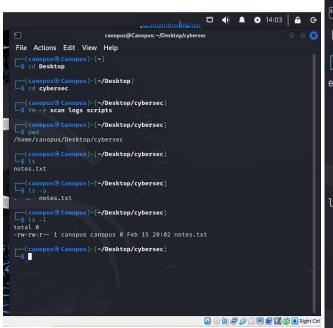
```
canopus@Canopus: ~/Desktop/cybersec/scripts

File  Actions  Edit  View  Help

┌──(canopus㉿Canopus)-[~]
└─$ cd Desktop

┌──(canopus㉿Canopus)-[~/Desktop]
└─$ cd cybersec

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ cp ~/Desktop/cybersec/scan/notes.txt ~/Desktop/cybersec/scripts

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ cd scripts

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ ls
notes.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ ls -l
total 4
-rw-rw-r-- 1 canopus canopus 28 Feb 15 19:18 notes.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ █
```

```
canopus@Canopus: ~/Desktop/cybersec/scripts

File  Actions  Edit  View  Help
└─$ cd ..

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ cd scan

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ mv note.txt
mv: missing destination file operand after 'note.txt'
Try 'mv --help' for more information.

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ mv note.txt ~/Desktop/cybersec
mv: cannot stat 'note.txt': No such file or directory

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ mv ~/Desktop/cybersec/note.txt ~/Desktop/cybersec
mv: cannot stat '/home/canopus/Desktop/cybersec/note.txt': No such file or direct
ory

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ cd ..

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ mv ~/Desktop/cybersec/scan/note.txt ~/Desktop/cybersec
mv: cannot stat '/home/canopus/Desktop/cybersec/scan/note.txt': No such file or d
irectory

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ cd scripts

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ mv ~/Desktop/cybersec/scripts/notes.txt ~/Desktop/cybersec/scan

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ █
```

```
┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ mv ~/Desktop/cybersec/scan/notes.txt ~/Desktop/cybersec

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ cd..

^[[A^[[A^[[A^[[B^[[B^[[BCould not find command-not-found database. Run 'sudo apt
update' to populate it.
cd..: command not found
^[[B^[[B

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scan]
└─$ cd ..

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ rm ~/Desktop/cybersec/scripts/notes.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ cd scripts

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ ls -l
total 0

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ ls

┌──(canopus㉿Canopus)-[~/Desktop/cybersec/scripts]
└─$ ls a
ls: cannot access 'a': No such file or directory
```

```
─ ☐ ✕
☐ ◀ 🔔 ⏻ 14:03 🔒 ⟳

                    canopus@Canopus: ~/Desktop/cybersec

File  Actions  Edit  View  Help
┌──(canopus㉿Canopus)-[~]
└─$ cd Desktop
┌──(canopus㉿Canopus)-[~/Desktop]
└─$ cd cybersec
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ rm -r scan logs scripts
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ pwd
/home/canopus/Desktop/cybersec
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ ls
notes.txt
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ ls -a
.    ..    notes.txt
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ ls -l
total 0
-rw-rw-r-- 1 canopus canopus 0 Feb 15 20:02 notes.txt
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$
```

```
                    canopus@Canopus: ~/Desktop/cybersec

File  Actions  Edit  View  Help
┌──(canopus㉿Canopus)-[~/Desktop/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:fece:3b59  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ce:3b:59  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 6251 (6.1 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        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

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ 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:ce:3b:59 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 84527sec preferred_lft 84527sec
```

```
canopus@Canopus: ~/Desktop/cybersec

File  Actions  Edit  View  Help

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ nmap
Nmap 7.94SVN ( 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 <host1[,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/PU/PY[portlist]: TCP SYN/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
  -sY/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
```

```
canopus@Canopus: ~/Desktop/cybersec

File  Actions  Edit  View  Help

  -6: 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 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ touch secret.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ chmod 755 secret.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ chmod 755 secret.txt lecture
chmod: cannot access 'lecture': No such file or directory

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ chmod 755 secret.txt read
chmod: cannot access 'read': No such file or directory

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ chmod 755 secret.txt #lecture

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$
```

```
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ touch logs.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ echo "je suis Canopus est black hat ravi de faire votre connaissance" >logs.txt

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ grep "black hat" logs.txt
je suis Canopus est black hat ravi de faire votre connaissance

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$
```

```
canopus@Canopus: ~/Desktop/cybersec

File  Actions  Edit  View  Help

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            948M     0  948M   0% /dev
tmpfs           198M  980K  197M   1% /run
/dev/sda1        39G   14G   24G  37% /
tmpfs           989M     0  989M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           198M  120K  198M   1% /run/user/1000

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ du -sh
8.0K    .

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       690Mi       986Mi       3.8Mi       443Mi       1.3Gi
Swap:          974Mi          0B       974Mi
```

File Actions Edit View Help

```
┌──(canopus⊛Canopus)-[~/Desktop/cybersec]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.6  22540 13144 ?        Ss   13:39   0:03 /sbin/init spl
root           2  0.0  0.0      0     0 ?        S    13:39   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    13:39   0:00 [pool_workqueu
root           4  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-rcu
root           5  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-rcu
root           6  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-slu
root           7  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-net
root           8  0.0  0.0      0     0 ?        I    13:39   0:01 [kworker/0:0-a
root          11  0.0  0.0      0     0 ?        I    13:39   0:02 [kworker/u2:0-
root          12  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-mm_
root          13  0.0  0.0      0     0 ?        I    13:39   0:00 [rcu_tasks_kth
root          14  0.0  0.0      0     0 ?        I    13:39   0:00 [rcu_tasks_rud
root          15  0.0  0.0      0     0 ?        I    13:39   0:00 [rcu_tasks_tra
root          16  0.0  0.0      0     0 ?        S    13:39   0:01 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    13:39   0:02 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    13:39   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    13:39   0:00 [idle_inject/0
root          20  0.0  0.0      0     0 ?        S    13:39   0:00 [cpuhp/0]
root          22  0.0  0.0      0     0 ?        S    13:39   0:00 [kdevtmpfs]
root          23  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-ine
root          24  0.0  0.0      0     0 ?        I    13:39   0:00 [kworker/u2:1-
root          25  0.0  0.0      0     0 ?        S    13:39   0:00 [kauditd]
root          26  0.0  0.0      0     0 ?        S    13:39   0:00 [khungtaskd]
root          27  0.0  0.0      0     0 ?        S    13:39   0:00 [oom_reaper]
root          29  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-wri
root          30  0.0  0.0      0     0 ?        S    13:39   0:00 [kcompactd0]
root          31  0.0  0.0      0     0 ?        SN   13:39   0:00 [ksmd]
root          32  0.0  0.0      0     0 ?        SN   13:39   0:00 [khugepaged]
root          33  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-kin
root          34  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-kbl
root          35  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-blk
```

File Actions Edit View Help

```
root          36  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-tpm
root          37  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-eda
root          38  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-dev
root          39  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/0:1H-
root          40  0.0  0.0      0     0 ?        S    13:39   0:00 [kswapd0]
root          48  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-kth
root          50  0.0  0.6      0     0 ?        I<   13:39   0:03 [kworker/R-acp
root          51  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-mld
root          52  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-ipv
root          57  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-kst
root          59  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/u3:0]
root         157  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-cry
root         162  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-ata
root         169  0.0  0.0      0     0 ?        S    13:39   0:00 [scsi_eh_0]
root         172  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-scs
root         174  0.0  0.0      0     0 ?        S    13:39   0:00 [scsi_eh_1]
root         175  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-scs
root         182  0.0  0.0      0     0 ?        S    13:39   0:00 [scsi_eh_2]
root         183  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-scs
root         224  0.0  0.0      0     0 ?        S    13:39   0:00 [irq/18-vmwgfx
root         226  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-ttm
root         239  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/0:2H-
root         285  0.0  0.0      0     0 ?        S    13:39   0:00 [jbd2/sda1-8]
root         286  0.0  0.0      0     0 ?        I<   13:39   0:00 [kworker/R-ext
root         343  0.0  0.9  67804 19644 ?        Ss   13:40   0:00 /usr/lib/syste
root         391  0.0  0.4  29576  8272 ?        Ss   13:40   0:01 /usr/lib/syste
root         463  0.0  0.3   8276  7636 ?        Ss   13:40   0:01 /usr/sbin/have
root         466  0.0  0.0      0     0 ?        I<   13:40   0:00 [kworker/R-rpc
root         467  0.0  0.0      0     0 ?        I<   13:40   0:00 [kworker/R-xpr
root         469  0.0  0.0      0     0 ?        S    13:40   0:00 [psimon]
root         574  0.0  0.3 311420  7520 ?        Ssl  13:40   0:00 /usr/libexec/a
root         575  0.0  0.1   7048  2432 ?        Ss   13:40   0:00 /usr/sbin/cron
message+     576  0.0  0.2  10696  5888 ?        Ss   13:40   0:02 /usr/bin/dbus-
polkitd      578  0.0  0.5 310620 10344 ?        Ssl  13:40   0:00 /usr/lib/polki
root         579  0.0  0.4  19056  8960 ?        Ss   13:40   0:00 /usr/lib/syste
```

```
root         636  0.0  0.1 293380   3456 ?         Sl    13:40   0:00 /usr/sbin/VBox
root         648  0.0  1.0 336028  21200 ?         Ssl   13:40   0:00 /usr/sbin/Netw
root         657  0.0  0.7 318504  14480 ?         Ssl   13:40   0:00 /usr/sbin/Mode
root         711  0.0  0.4 380256   9220 ?         SLsl  13:40   0:00 /usr/sbin/ligh
root         727  0.0  0.1   9480   2816 tty1      Ss+   13:40   0:00 /sbin/agetty -
root         729  2.9  4.7 369416  95592 tty7      Ssl+  13:40   1:26 /usr/lib/xorg/
root         754  0.0  0.0      0      0 ?         S     13:41   0:00 [psimon]
rtkit        783  0.0  0.1  22824   3200 ?         SNsl  13:41   0:00 /usr/libexec/r
root         854  0.0  0.4 234380   8244 ?         Sl    13:42   0:00 lightdm --sess
canopus      861  0.0  0.5  21276  11648 ?         Ss    13:43   0:00 /usr/lib/syste
canopus      862  0.0  0.1  21904   3356 ?         S     13:43   0:00 (sd-pam)
canopus      877  0.0  0.7 117856  14760 ?         S<sl  13:43   0:00 /usr/bin/pipew
canopus      878  0.0  0.2  95652   6016 ?         Ssl   13:43   0:00 /usr/bin/pipew
canopus      880  0.0  1.7 643036  35748 ?         S<sl  13:43   0:00 /usr/bin/wirep
canopus      881  0.0  0.4 101756   9344 ?         S<sl  13:43   0:00 /usr/bin/pipew
canopus      882  0.0  0.5 314760  12120 ?         SLsl  13:43   0:00 /usr/bin/gnome
canopus      889  0.0  0.2   9900   5488 ?         Ss    13:43   0:00 /usr/bin/dbus-
canopus      909  0.0  1.3 340024  27428 ?         Ssl   13:43   0:01 xfce4-session
canopus      962  0.0  0.0  17500   1664 ?         S     13:43   0:00 /usr/bin/VBoxC
canopus      966  0.0  0.1 215688   3968 ?         Sl    13:43   0:00 /usr/bin/VBoxC
canopus      977  0.0  0.0  17500   1536 ?         S     13:43   0:00 /usr/bin/VBoxC
canopus      979  0.1  0.1 215800   3328 ?         Sl    13:43   0:03 /usr/bin/VBoxC
canopus      982  0.0  0.0  17500   1664 ?         S     13:43   0:00 /usr/bin/VBoxC
canopus      988  0.3  0.1 216316   3200 ?         Sl    13:43   0:10 /usr/bin/VBoxC
canopus      998  0.0  0.0   9736   1540 ?         Ss    13:43   0:00 /usr/bin/ssh-a
canopus     1012  0.0  0.0  17500   1664 ?         S     13:43   0:00 /usr/bin/VBoxC
canopus     1013  0.0  0.1 215892   3584 ?         Sl    13:43   0:01 /usr/bin/VBoxC
canopus     1018  0.0  0.4 383184   8192 ?         Ssl   13:43   0:00 /usr/libexec/a
canopus     1025  0.0  0.2   9444   4992 ?         S     13:43   0:00 /usr/bin/dbus-
canopus     1036  0.0  0.4 236564   8320 ?         Sl    13:43   0:00 /usr/libexec/a
canopus     1049  0.0  0.2  81676   5308 ?         SLs   13:43   0:00 /usr/bin/gpg-a
canopus     1051  0.5  5.7 674720 115876 ?         Sl    13:43   0:14 xfwm4 --displa
canopus     1055  0.0  0.5 312336  12024 ?         Ssl   13:43   0:00 /usr/libexec/g
canopus     1061  0.0  0.5 457796  10832 ?         Sl    13:43   0:00 /usr/libexec/g
canopus     1084  0.0  1.4 304184  29656 ?         Sl    13:43   0:01 xfsettingsd --
```

```
┌──(canopus㉿Canopus)-[~/Desktop/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 Controlle
r (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 Contro
ller (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) USB
2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Contr
oller [AHCI mode] (rev 02)
```

```
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ sudo apt install traceroute
[sudo] password for canopus:
traceroute is already the newest version (1:2.1.5-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```

```
┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ traceroute www.google.com
www.google.com: Temporary failure in name resolution
Cannot handle "host" cmdline arg `www.google.com' on position 1 (argc 1)

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ traceroute google.com
google.com: Temporary failure in name resolution
Cannot handle "host" cmdline arg `google.com' on position 1 (argc 1)

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ █
```

```
                          canopus@Canopus: ~/Desktop/cybersec

File   Actions   Edit   View   Help

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ ss -tuln
Netid   State   Recv-Q   Send-Q      Local Address:Port      Peer Address:Port
```

```
                          canopus@Canopus: ~/Desktop/cybersec

File   Actions   Edit   View   Help

┌──(canopus㉿Canopus)-[~/Desktop/cybersec]
└─$ journalctl
Feb 01 16:12:04 Canopus kernel: Linux version 6.6.15-amd64 (devel@kali.org) (gcc>
Feb 01 16:12:04 Canopus kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-am>
Feb 01 16:12:04 Canopus kernel: BIOS-provided physical RAM map:
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×0000000000000000-0×00000000000>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×000000000009fc00-0×00000000000>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000000f0000-0×00000000000>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×0000000000100000-0×000000007ff>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×000000007fff0000-0×000000007ff>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000fec00000-0×00000000fec>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000fee00000-0×00000000fee>
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000fffc0000-0×00000000fff>
Feb 01 16:12:04 Canopus kernel: NX (Execute Disable) protection: active
Feb 01 16:12:04 Canopus kernel: APIC: Static calls initialized
Feb 01 16:12:04 Canopus kernel: SMBIOS 2.5 present.
Feb 01 16:12:04 Canopus kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vi>
Feb 01 16:12:04 Canopus kernel: Hypervisor detected: KVM
Feb 01 16:12:04 Canopus kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 01 16:12:04 Canopus kernel: kvm-clock: using sched offset of 217624556454 cy>
Feb 01 16:12:04 Canopus kernel: clocksource: kvm-clock: mask: 0×ffffffffffffffff>
Feb 01 16:12:04 Canopus kernel: tsc: Detected 1895.613 MHz processor
Feb 01 16:12:04 Canopus kernel: e820: update [mem 0×00000000-0×00000fff] usable >
-- Boot a2149ae304cc4c55ae2c73e70fa2e697 --
Feb 01 19:52:12 Canopus kernel: Linux version 6.6.15-amd64 (devel@kali.org) (gcc>
Feb 01 19:52:12 Canopus kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-am>
Feb 01 19:52:12 Canopus kernel: BIOS-provided physical RAM map:
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×0000000000000000-0×00000000000>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×000000000009fc00-0×00000000000>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000000f0000-0×00000000000>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×0000000000100000-0×000000007ff>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×000000007fff0000-0×000000007ff>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000fec00000-0×00000000fec>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000fee00000-0×00000000fee>
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000fffc0000-0×00000000fff>
```

File   Actions   Edit   View   Help

```
Feb 01 16:12:04 Canopus kernel: Linux version 6.6.15-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-24) 13.2.0, GNU ld (GNU Binutils for Debian) 2.42) #1 SMP PREEMPT_D>
Feb 01 16:12:04 Canopus kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-amd64 root=UUID=df4825ba-d936-4af8-bc03-5f38d7f0178c ro quiet splash
Feb 01 16:12:04 Canopus kernel: BIOS-provided physical RAM map:
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×0000000000000000-0×000000000009fbff] usable
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×000000000009fc00-0×000000000009ffff] reserved
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000000f0000-0×00000000000fffff] reserved
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×0000000000100000-0×000000007ffeffff] usable
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×000000007fff0000-0×000000007fffffff] ACPI data
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000fec00000-0×00000000fec00fff] reserved
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000fee00000-0×00000000fee00fff] reserved
Feb 01 16:12:04 Canopus kernel: BIOS-e820: [mem 0×00000000fffc0000-0×00000000ffffffff] reserved
Feb 01 16:12:04 Canopus kernel: NX (Execute Disable) protection: active
Feb 01 16:12:04 Canopus kernel: APIC: Static calls initialized
Feb 01 16:12:04 Canopus kernel: SMBIOS 2.5 present.
Feb 01 16:12:04 Canopus kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Feb 01 16:12:04 Canopus kernel: Hypervisor detected: KVM
Feb 01 16:12:04 Canopus kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 01 16:12:04 Canopus kernel: kvm-clock: using sched offset of 217624556454 cycles
Feb 01 16:12:04 Canopus kernel: clocksource: kvm-clock: mask: 0×ffffffffffffffff max_cycles: 0×1cd42e4dffb, max_idle_ns: 881590591483 ns
Feb 01 16:12:04 Canopus kernel: tsc: Detected 1895.613 MHz processor
Feb 01 16:12:04 Canopus kernel: e820: update [mem 0×00000000-0×00000fff] usable ⟹ reserved
-- Boot a2149ae304cc4c55ae2c73e70fa2e697 --
Feb 01 19:52:12 Canopus kernel: Linux version 6.6.15-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-24) 13.2.0, GNU ld (GNU Binutils for Debian) 2.42) #1 SMP PREEMPT_D>
Feb 01 19:52:12 Canopus kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-amd64 root=UUID=df4825ba-d936-4af8-bc03-5f38d7f0178c ro quiet splash
Feb 01 19:52:12 Canopus kernel: BIOS-provided physical RAM map:
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×0000000000000000-0×000000000009fbff] usable
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×000000000009fc00-0×000000000009ffff] reserved
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000000f0000-0×00000000000fffff] reserved
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×0000000000100000-0×000000007ffeffff] usable
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×000000007fff0000-0×000000007fffffff] ACPI data
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000fec00000-0×00000000fec00fff] reserved
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000fee00000-0×00000000fee00fff] reserved
Feb 01 19:52:12 Canopus kernel: BIOS-e820: [mem 0×00000000fffc0000-0×00000000ffffffff] reserved
Feb 01 19:52:12 Canopus kernel: NX (Execute Disable) protection: active
lines 1-34
```

File   Actions   Edit   View   Help

```
┌──(canopus㉿Canopus)-[~]
└─$ journalctl -f
Feb 16 14:39:01 Canopus CRON[28477]: (root) CMD (   [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
Feb 16 14:39:01 Canopus systemd[1]: Starting phpsessionclean.service - Clean php session files ...
Feb 16 14:39:01 Canopus CRON[28476]: pam_unix(cron:session): session closed for user root
Feb 16 14:39:02 Canopus systemd[1]: phpsessionclean.service: Deactivated successfully.
Feb 16 14:39:02 Canopus systemd[1]: Finished phpsessionclean.service - Clean php session files.
Feb 16 14:43:36 Canopus dbus-daemon[889]: [session uid=1000 pid=889] Activating service name='org.xfce.Xfconf' requested by ':1.24' (uid=1000 pid=1094 comm="xfce4-pan
el --display :0.0 --sm-client-id 29515aeb")
Feb 16 14:43:36 Canopus dbus-daemon[889]: [session uid=1000 pid=889] Successfully activated service 'org.xfce.Xfconf'
Feb 16 14:45:01 Canopus CRON[31451]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Feb 16 14:45:01 Canopus CRON[31452]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 16 14:45:01 Canopus CRON[31451]: pam_unix(cron:session): session closed for user root
```

```
┌──(canopus㉿Canopus)-[~]
└─$ journalctl -b
Feb 16 13:40:17 Canopus kernel: Linux version 6.6.15-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-24) 13.2.0, GNU ld (GNU Binutils for Debian) 2.42) #1 SMP PREEMPT_>
Feb 16 13:40:17 Canopus kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-amd64 root=UUID=df4825ba-d936-4af8-bc03-5f38d7f0178c ro quiet splash
Feb 16 13:40:17 Canopus kernel: BIOS-provided physical RAM map:
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×0000000000000000-0×000000000009fbff] usable
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×000000000009fc00-0×000000000009ffff] reserved
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×00000000000f0000-0×00000000000fffff] reserved
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×0000000000100000-0×000000007ffeffff] usable
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×000000007fff0000-0×000000007fffffff] ACPI data
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×00000000fec00000-0×00000000fec00fff] reserved
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×00000000fee00000-0×00000000fee00fff] reserved
Feb 16 13:40:17 Canopus kernel: BIOS-e820: [mem 0×00000000fffc0000-0×00000000ffffffff] reserved
Feb 16 13:40:17 Canopus kernel: NX (Execute Disable) protection: active
Feb 16 13:40:17 Canopus kernel: APIC: Static calls initialized
Feb 16 13:40:17 Canopus kernel: SMBIOS 2.5 present.
Feb 16 13:40:17 Canopus kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Feb 16 13:40:17 Canopus kernel: Hypervisor detected: KVM
Feb 16 13:40:17 Canopus kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 16 13:40:17 Canopus kernel: kvm-clock: using sched offset of 309081565893 cycles
Feb 16 13:40:17 Canopus kernel: clocksource: kvm-clock: mask: 0×ffffffffffffffff max_cycles: 0×1cd42e4dffb, max_idle_ns: 881590591483 ns
Feb 16 13:40:17 Canopus kernel: tsc: Detected 1895.615 MHz processor
Feb 16 13:40:17 Canopus kernel: e820: update [mem 0×00000000-0×00000fff] usable ⟹ reserved
Feb 16 13:40:17 Canopus kernel: e820: remove [mem 0×000a0000-0×000fffff] usable
Feb 16 13:40:17 Canopus kernel: last_pfn = 0×7fff0 max_arch_pfn = 0×400000000
Feb 16 13:40:17 Canopus kernel: MTRRs disabled by BIOS
Feb 16 13:40:17 Canopus kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
Feb 16 13:40:17 Canopus kernel: found SMP MP-table at [mem 0×0009fff0-0×0009ffff]
Feb 16 13:40:17 Canopus kernel: RAMDISK: [mem 0×2e9f1000-0×334effff]
Feb 16 13:40:17 Canopus kernel: ACPI: Early table checksum verification disabled
Feb 16 13:40:17 Canopus kernel: ACPI: RSDP 0×00000000000E0000 000024 (v02 VBOX )
Feb 16 13:40:17 Canopus kernel: ACPI: XSDT 0×000000007FFF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
Feb 16 13:40:17 Canopus kernel: ACPI: FACP 0×000000007FFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001 ASL  00000061)
Feb 16 13:40:17 Canopus kernel: ACPI: DSDT 0×000000007FFF0610 002353 (v02 VBOX   VBOXBIOS 00000002 INTL 20100528)
Feb 16 13:40:17 Canopus kernel: ACPI: FACS 0×000000007FFF0200 000040
```

File   Actions   Edit   View   Help

```
┌──(canopus㉿Canopus)-[~]
└─$ journalctl -n 10
Feb 16 14:39:01 Canopus CRON[28477]: (root) CMD (   [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
Feb 16 14:39:01 Canopus systemd[1]: Starting phpsessionclean.service - Clean php session files ...
Feb 16 14:39:01 Canopus CRON[28476]: pam_unix(cron:session): session closed for user root
Feb 16 14:39:02 Canopus systemd[1]: phpsessionclean.service: Deactivated successfully.
Feb 16 14:39:02 Canopus systemd[1]: Finished phpsessionclean.service - Clean php session files.
Feb 16 14:43:36 Canopus dbus-daemon[889]: [session uid=1000 pid=889] Activating service name='org.xfce.Xfconf' requested by ':1.24' (uid=1000 pid=1094 comm="xfce4-pa>
Feb 16 14:43:36 Canopus dbus-daemon[889]: [session uid=1000 pid=889] Successfully activated service 'org.xfce.Xfconf'
Feb 16 14:45:01 Canopus CRON[31451]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Feb 16 14:45:01 Canopus CRON[31452]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 16 14:45:01 Canopus CRON[31451]: pam_unix(cron:session): session closed for user root
lines 1-10/10 (END)
```

Dans cette TD j'ai appris beaucoup de commande sur comment faire des dossiers, créer des fichiers, copié ou déplacé des fichiers, d'écrire dans un fichier texte que j'avais créé et de comment créer ma machine virtuelle et de faire toute sorte de manipulation.