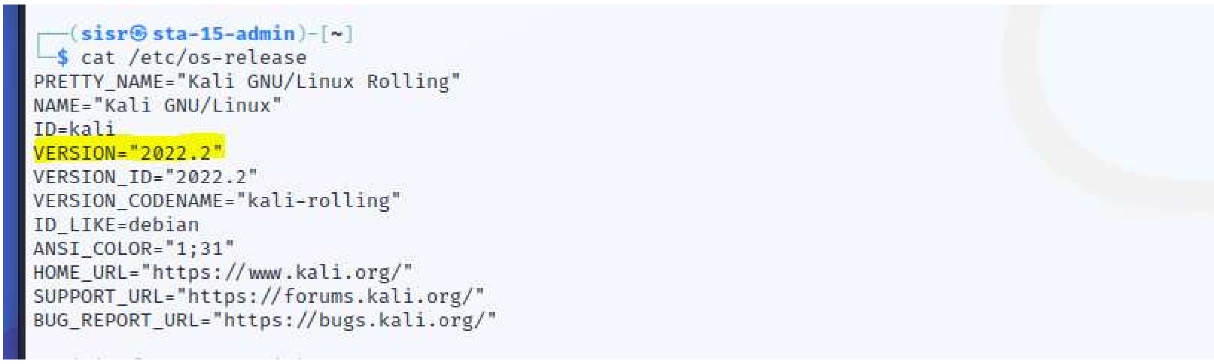
Journal De Bord

Tache n°1 importation des deux machines

Tache n°2 nom et adressage

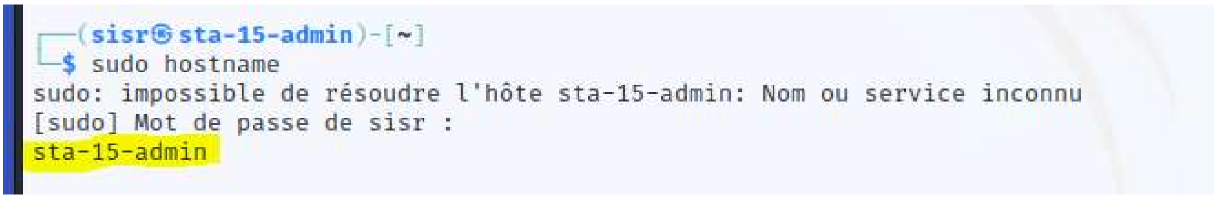
Tache n°3 répartitions du travail :

Version os :



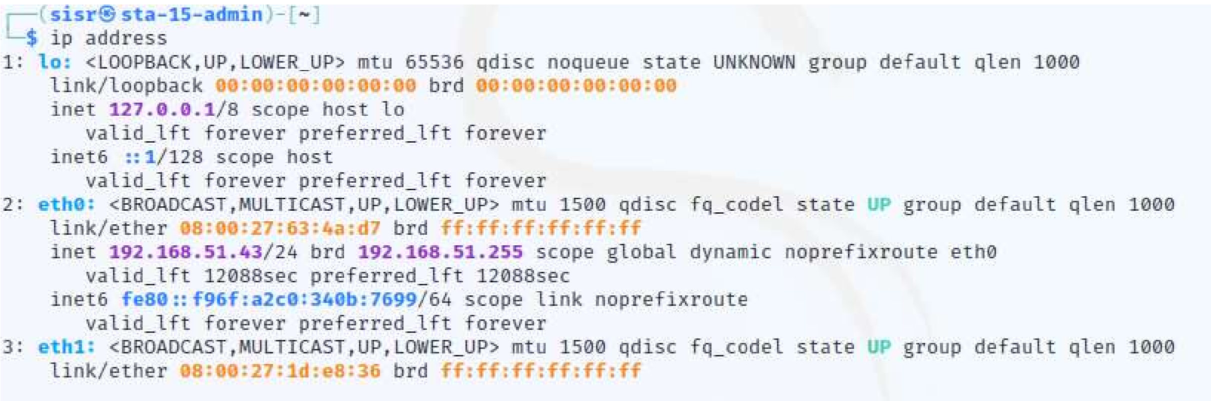
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2022.2"
VERSION_ID="2022.2"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
```

Nom d'hote :



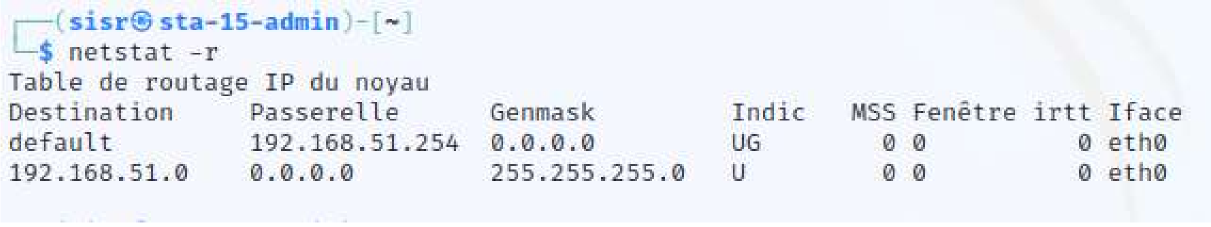
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ sudo hostname
sudo: impossible de résoudre l'hôte sta-15-admin: Nom ou service inconnu
[sudo] Mot de passe de sisr :
sta-15-admin
```

Configuration ip :



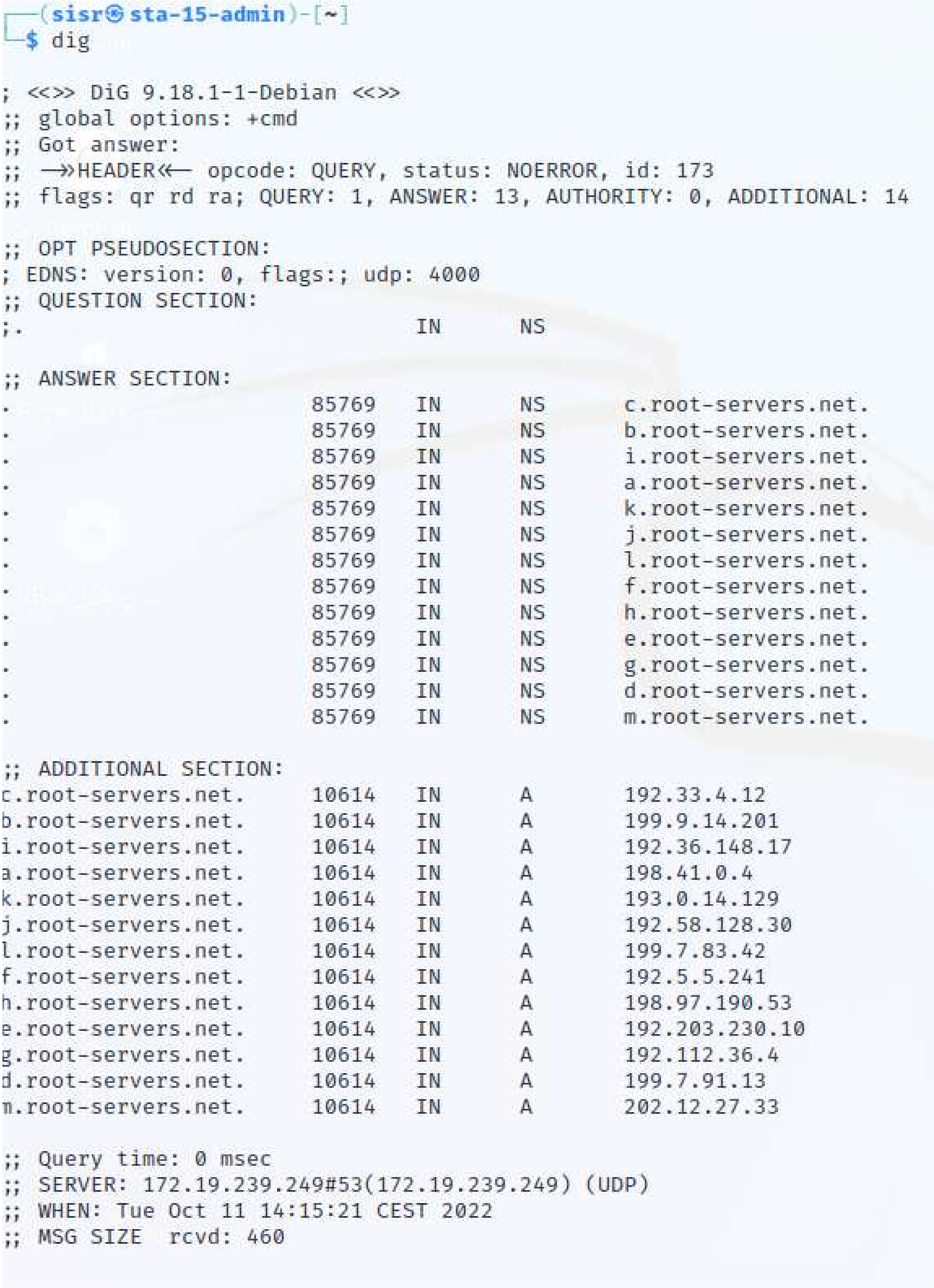
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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 08:00:27:63:4a:d7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.43/24 brd 192.168.51.255 scope global dynamic noprefixroute eth0
       valid_lft 12088sec preferred_lft 12088sec
    inet6 fe80::f96f:a2c0:340b:7699/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1d:e8:36 brd ff:ff:ff:ff:ff:ff
```

Table de routage et passerelle par défaut :



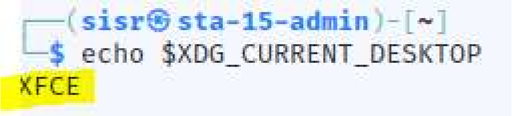
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ netstat -r
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
default         192.168.51.254  0.0.0.0         UG        0 0          0 eth0
192.168.51.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Serveur(s) de noms :



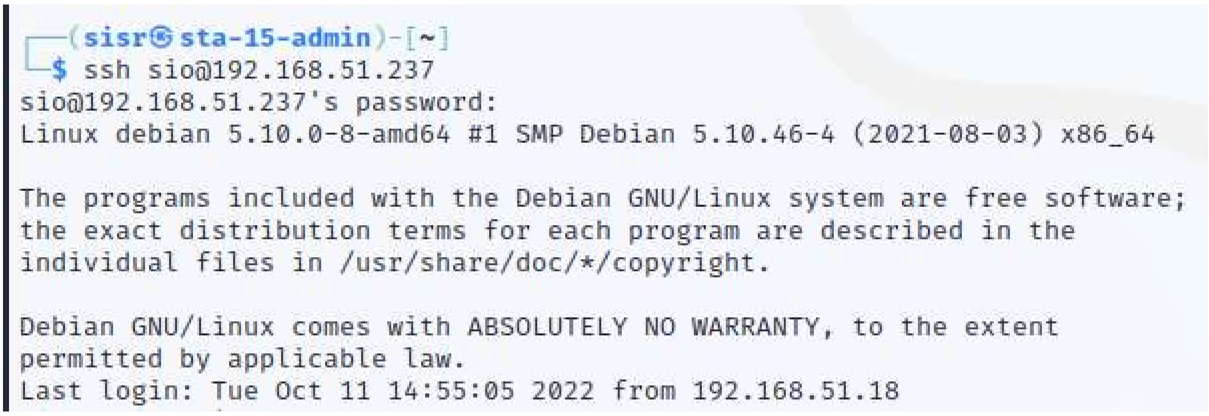
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ dig

; <<>> DiG 9.18.1-1-Debian <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 173
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       85769   IN      NS      c.root-servers.net.
.                       85769   IN      NS      b.root-servers.net.
.                       85769   IN      NS      i.root-servers.net.
.                       85769   IN      NS      a.root-servers.net.
.                       85769   IN      NS      k.root-servers.net.
.                       85769   IN      NS      j.root-servers.net.
.                       85769   IN      NS      l.root-servers.net.
.                       85769   IN      NS      f.root-servers.net.
.                       85769   IN      NS      h.root-servers.net.
.                       85769   IN      NS      e.root-servers.net.
.                       85769   IN      NS      g.root-servers.net.
.                       85769   IN      NS      d.root-servers.net.
.                       85769   IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
c.root-servers.net.     10614   IN      A       192.33.4.12
b.root-servers.net.     10614   IN      A       199.9.14.201
i.root-servers.net.     10614   IN      A       192.36.148.17
a.root-servers.net.     10614   IN      A       198.41.0.4
k.root-servers.net.     10614   IN      A       193.0.14.129
j.root-servers.net.     10614   IN      A       192.58.128.30
l.root-servers.net.     10614   IN      A       199.7.83.42
f.root-servers.net.     10614   IN      A       192.5.5.241
h.root-servers.net.     10614   IN      A       198.97.190.53
e.root-servers.net.     10614   IN      A       192.203.230.10
g.root-servers.net.     10614   IN      A       192.112.36.4
d.root-servers.net.     10614   IN      A       199.7.91.13
m.root-servers.net.     10614   IN      A       202.12.27.33

;; Query time: 0 msec
;; SERVER: 172.19.239.249#53(172.19.239.249) (UDP)
;; WHEN: Tue Oct 11 14:15:21 CEST 2022
;; MSG SIZE  rcvd: 460
```

Environnement graphique sur la STA(GUI/Desktop Environment) :



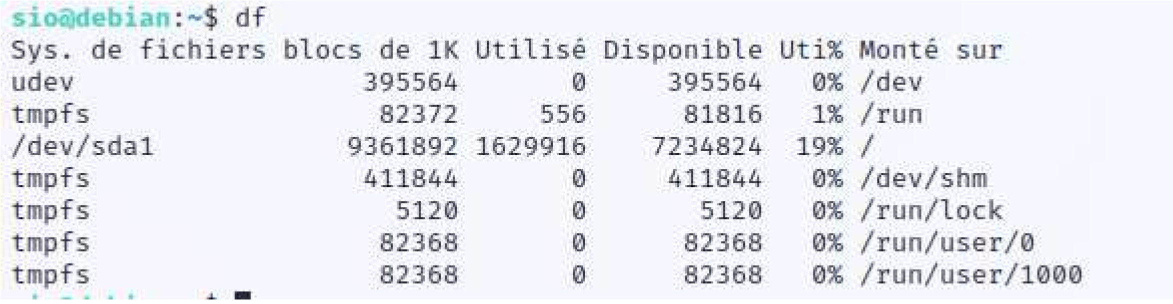
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ echo $XDG_CURRENT_DESKTOP
XFCE
```

Connection en ssh à INTRALAB :



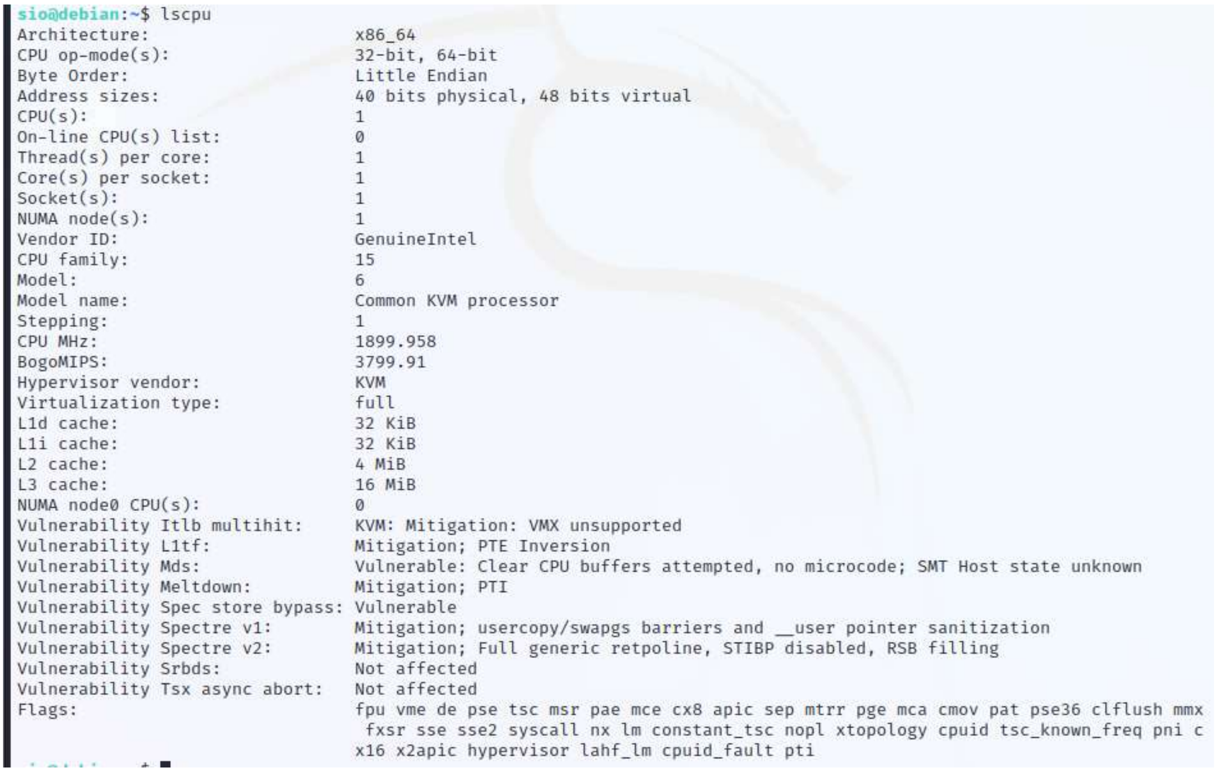
```
┌──(sisr㉿sta-15-admin)-[~]
└─$ ssh sio@192.168.51.237
sio@192.168.51.237's password:
Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 11 14:55:05 2022 from 192.168.51.18
```

Espace de stockage persistant (HDD) :



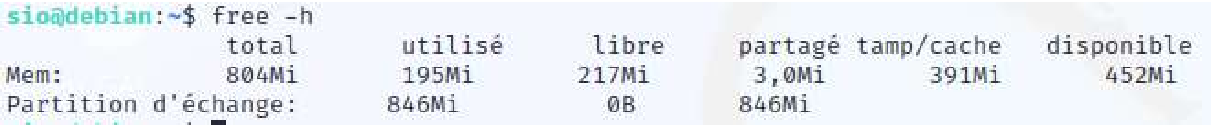
```
sio@debian:~$ df
Sys. de fichiers blocs de 1K Utilisé Disponible Uti% Monté sur
udev                  395564       0     395564   0% /dev
tmpfs                  82372     556      81816   1% /run
/dev/sda1            9361892 1629916    7234824  19% /
tmpfs                 411844       0     411844   0% /dev/shm
tmpfs                   5120       0       5120   0% /run/lock
tmpfs                  82368       0      82368   0% /run/user/0
tmpfs                  82368       0      82368   0% /run/user/1000
```

Processeur(s) (CPU) :



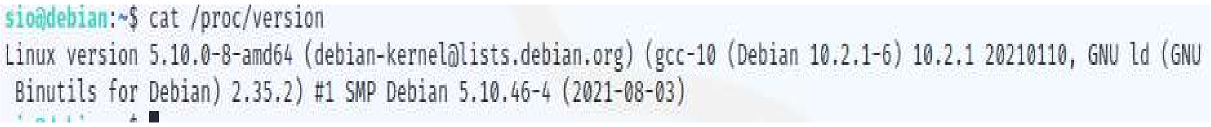
```
sio@debian:~$ lscpu
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   40 bits physical, 48 bits virtual
CPU(s):                          1
On-line CPU(s) list:             0
Thread(s) per core:              1
Core(s) per socket:              1
Socket(s):                       1
NUMA node(s):                    1
Vendor ID:                       GenuineIntel
CPU family:                      15
Model:                           6
Model name:                      Common KVM processor
Stepping:                        1
CPU MHz:                         1899.958
BogoMIPS:                        3799.91
Hypervisor vendor:               KVM
Virtualization type:             full
L1d cache:                       32 KiB
L1i cache:                       32 KiB
L2 cache:                        4 MiB
L3 cache:                        16 MiB
NUMA node0 CPU(s):               0
Vulnerability Itlb multihit:     KVM: Mitigation: VMX unsupported
Vulnerability L1tf:              Mitigation; PTE Inversion
Vulnerability Mds:               Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown
Vulnerability Meltdown:          Mitigation; PTI
Vulnerability Spec store bypass: Vulnerable
Vulnerability Spectre v1:        Mitigation; usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2:        Mitigation; Full generic retpoline, STIBP disabled, RSB filling
Vulnerability Srbds:             Not affected
Vulnerability Tsx async abort:   Not affected
Flags:                           fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx
                                  fxsr sse sse2 syscall nx lm constant_tsc nopl xtopology cpuid tsc_known_freq pni c
                                 x16 x2apic hypervisor lahf_lm cpuid_fault pti
```

Mémoire Vive (RAM) :



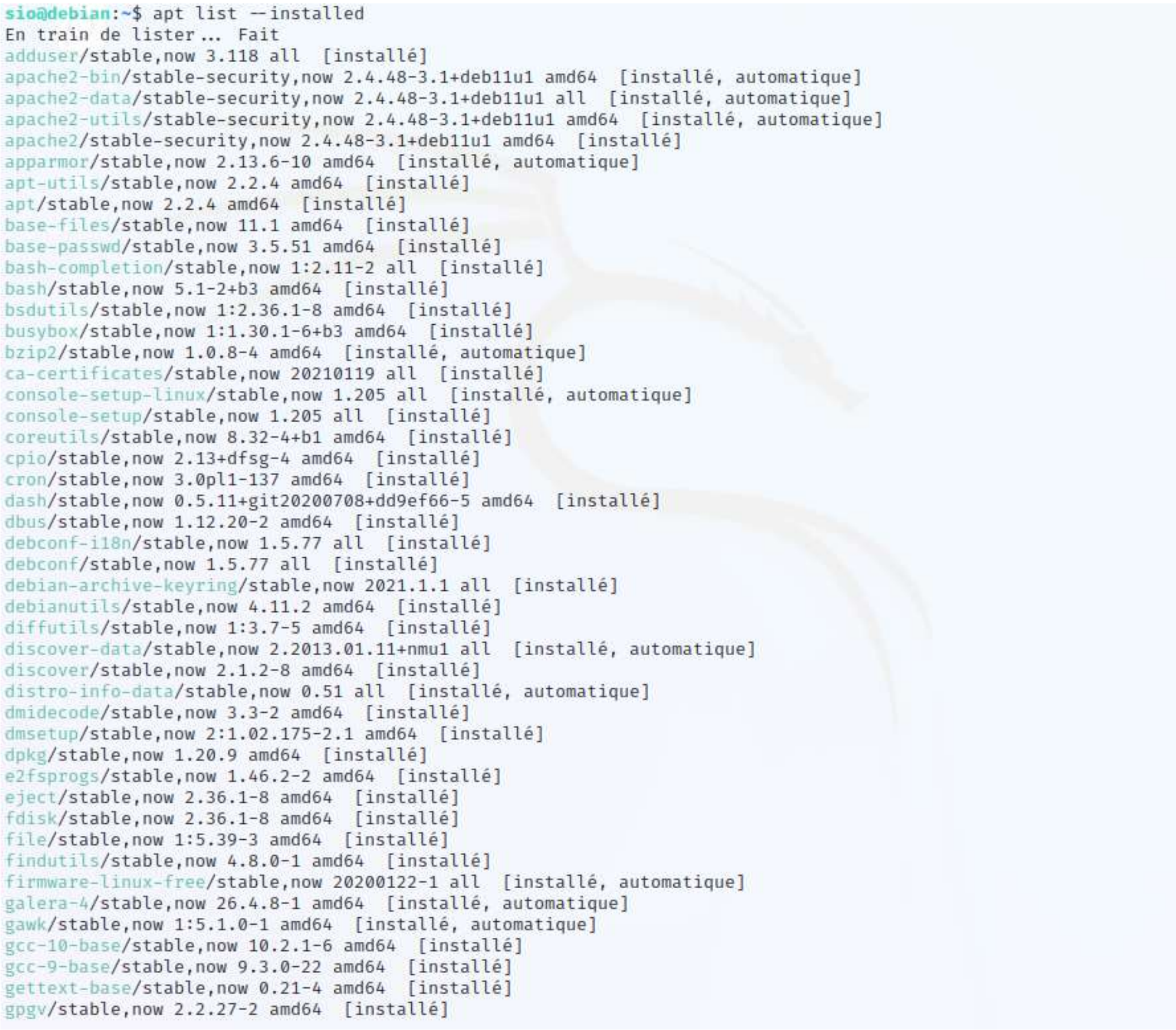
```
sio@debian:~$ free -h
               total       utilisé      libre     partagé tamp/cache   disponible
Mem:           804Mi        195Mi       217Mi       3,0Mi      391Mi        452Mi
Partition d'échange:      846Mi         0B        846Mi
```

Système d'exploitation (OS) :



```
sio@debian:~$ cat /proc/version
Linux version 5.10.0-8-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian 10.2.1-6) 10.2.1 20210110, GNU ld (GNU
 Binutils for Debian) 2.35.2) #1 SMP Debian 5.10.46-4 (2021-08-03)
```

Liste des services installés (avec leur numéro de version) :



```
sio@debian:~$ apt list --installed
En train de lister... Fait
adduser/stable,now 3.118 all  [installé]
apache2-bin/stable-security,now 2.4.48-3.1+deb11u1 amd64  [installé, automatique]
apache2-data/stable-security,now 2.4.48-3.1+deb11u1 all  [installé, automatique]
apache2-utils/stable-security,now 2.4.48-3.1+deb11u1 amd64  [installé, automatique]
apache2/stable-security,now 2.4.48-3.1+deb11u1 amd64  [installé]
apparmor/stable,now 2.13.6-10 amd64  [installé, automatique]
apt-utils/stable,now 2.2.4 amd64  [installé]
apt/stable,now 2.2.4 amd64  [installé]
base-files/stable,now 11.1 amd64  [installé]
base-passwd/stable,now 3.5.51 amd64  [installé]
bash-completion/stable,now 1:2.11-2 all  [installé]
bash/stable,now 5.1-2+b3 amd64  [installé]
bsdutils/stable,now 1:2.36.1-8 amd64  [installé]
busybox/stable,now 1:1.30.1-6+b3 amd64  [installé]
bzip2/stable,now 1.0.8-4 amd64  [installé, automatique]
ca-certificates/stable,now 20210119 all  [installé]
console-setup-linux/stable,now 1.205 all  [installé, automatique]
console-setup/stable,now 1.205 all  [installé]
coreutils/stable,now 8.32-4+b1 amd64  [installé]
cpio/stable,now 2.13+dfsg-4 amd64  [installé]
cron/stable,now 3.0pl1-137 amd64  [installé]
dash/stable,now 0.5.11+git20200708+dd9ef66-5 amd64  [installé]
dbus/stable,now 1.12.20-2 amd64  [installé]
debconf-i18n/stable,now 1.5.77 all  [installé]
debconf/stable,now 1.5.77 all  [installé]
debian-archive-keyring/stable,now 2021.1.1 all  [installé]
debianutils/stable,now 4.11.2 amd64  [installé]
diffutils/stable,now 1:3.7-5 amd64  [installé]
discover-data/stable,now 2.2013.01.11+nmu1 all  [installé, automatique]
discover/stable,now 2.1.2-8 amd64  [installé]
distro-info-data/stable,now 0.51 all  [installé, automatique]
dmidecode/stable,now 3.3-2 amd64  [installé]
dmsetup/stable,now 2:1.02.175-2.1 amd64  [installé]
dpkg/stable,now 1.20.9 amd64  [installé]
e2fsprogs/stable,now 1.46.2-2 amd64  [installé]
eject/stable,now 2.36.1-8 amd64  [installé]
fdisk/stable,now 2.36.1-8 amd64  [installé]
file/stable,now 1:5.39-3 amd64  [installé]
findutils/stable,now 4.8.0-1 amd64  [installé]
firmware-linux-free/stable,now 20200122-1 all  [installé, automatique]
galera-4/stable,now 26.4.8-1 amd64  [installé, automatique]
gawk/stable,now 1:5.1.0-1 amd64  [installé, automatique]
gcc-10-base/stable,now 10.2.1-6 amd64  [installé]
gcc-9-base/stable,now 9.3.0-22 amd64  [installé]
gettext-base/stable,now 0.21-4 amd64  [installé]
gpgv/stable,now 2.2.27-2 amd64  [installé]
```

Copie de la base de données :

Copie du fichier ou des fichiers de l'application web :