

Universite De Technologie D 'haiti

UNITECH

Sciences Informatiques

Niveau III

CyberSecurite

Virtulisation sur Linux

Preparer par : Sebastien CELENT

Prof : Ismael SAINT AMOUR

Date : le 13 /02 /2024

Introduction

Dans le cadre de ce travail dirigé, j'ai réalisé une série d'opérations sur **Kali Linux** afin de mieux comprendre l'utilisation d'une machine virtuelle, la gestion des fichiers et dossiers, ainsi que l'analyse d'un réseau. Ce rapport présente les différentes étapes effectuées, les commandes utilisées et les résultats obtenus.

L'objectif principal est d'explorer les fonctionnalités essentielles de **Kali Linux**, notamment la virtualisation, la manipulation de fichiers, les scans réseau avec **nmap**, la gestion des permissions et l'utilisation de commandes avancées dans le terminal.

Ce document détaille ainsi :

- La mise en place et la gestion d'une structure de fichiers,
- L'analyse réseau et la gestion des processus,
- La manipulation des permissions et l'exploitation de certaines commandes essentielles.

Enfin, je conclus par une réflexion sur les compétences acquises et l'importance de ces manipulations dans un contexte de **cybersécurité**.

Creation du Depot Cybersec sur Github

Afin de conserver et partager mon travail, j'ai créé un dépôt GitHub où j'ai ajouté la structure de dossiers Cybersec. Cette approche permet de versionner les fichiers et d'assurer un accès facile depuis n'importe quel environnement.

```
(scelent@Kali)-[~]  
$ git clone https://github.com/Celent19/Cybersec.git  
Clonage dans 'Cybersec' ...  
remote: Enumerating objects: 3, done.  
remote: Counting objects: 100% (3/3), done.  
Réception d'objets: 100% (3/3), fait.  
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
```

Creation des sous dossier scan / logs / scripts

```
(sclent@Kali)-[~]  
$ mkdir -p Cybersec/scan Cybersec/logs Cybersec/scripts
```

Ajout du
fichier notes.txt dans le dossier scan et logs

```
(sclent@Kali)-[~]  
$ touch Cybersec/scan/notes.txt Cybersec/logs/notes.txt
```

Ajout du contenu dans les fichiers textes notes.txt

```
(sclent@Kali)-[~]  
$ echo "Ceci est mon fichier dans scan " > Cybersec/scan/notes.txt  
  
(sclent@Kali)-[~]  
$ echo "Ceci est mon fichier dans logs " > Cybersec/logs/notes.txt
```

Affichage des contenu des fichiers.

```
(sclent@Kali)-[~]  
$ cat Cybersec/scan/notes.txt  
Ceci est mon fichier dans scan  
  
(sclent@Kali)-[~]  
$ cat Cybersec/logs/notes.txt  
Ceci est mon fichier dans logs
```

Copie du fichier notes.txt dans le sous-dossier scripts .

```
(sclent@Kali)-[~]  
$ cp Cybersec/scan/notes.txt Cybersec/scripts
```

Vérification pour voir si le fichiers a été copié.

```
(scelent@Kali)-[~]  
$ ls Cybersec/scripts  
notes.txt
```

Déplacement du fichier notes.txt dans le sous-dossier scan .

```
(scelent@Kali)-[~]  
$ mv Cybersec/scripts/notes.txt Cybersec/scan
```

Supprimez le fichier (notes.txt) dans le sous-dossier scripts .

```
(scelent@Kali)-[~]  
$ rm Cybersec/scripts/notes.txt
```

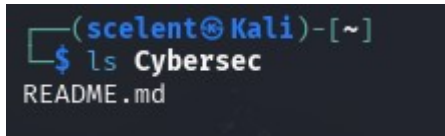
vérifier si le fichiers a été supprimé.

```
(scelent@Kali)-[~]  
$ ls Cybersec/scripts
```

Supprimez les sous-dossiers : scan , logs , scripts

```
(scelent@Kali)-[~]  
$ rm -r Cybersec/scan Cybersec/logs Cybersec/scripts
```

vérifier si les sous-dossiers ont été supprimés.



```
(sclent@Kali)-[~]  
$ ls Cybersec  
README.md
```

Le fichier README.md qui est dans le dossier Cybersec est écrit en Markdown (.md), un format permettant de structurer le texte avec des titres, des listes et des liens. Il est particulièrement utile sur GitHub, car il s'affiche automatiquement sur la page principale du dépôt.

Dans cette partie du travail, j'ai créé une structure de dossiers et manipulé plusieurs fichiers sous Kali Linux. Ces opérations m'ont permis de mieux comprendre la gestion des fichiers et des dossiers à l'aide de commandes Linux.

Tout d'abord, j'ai créé un dossier principal nommé **Cybersec**. À l'intérieur de ce dossier, j'ai ajouté trois sous-dossiers : **scan**, **logs** et **scripts**. Cette organisation permet une meilleure structuration des fichiers liés aux différentes activités de cybersécurité.

Ensuite, j'ai créé un fichier **notes.txt** dans les dossiers **scan** et **logs**. J'ai ajouté du contenu dans ces fichiers en utilisant la commande **echo**, puis j'ai vérifié que les modifications avaient bien été prises en compte en affichant leur contenu avec la commande **cat**.

Après cela, j'ai copié le fichier **notes.txt** du dossier **scan** vers le dossier **scripts**, puis j'ai vérifié qu'il était bien présent dans ce dernier. Par la suite, j'ai déplacé ce fichier du dossier **scripts** vers le dossier **scan**, avant de le supprimer complètement du dossier **scripts**. À chaque étape, j'ai utilisé les commandes appropriées et vérifié que les fichiers avaient bien été copiés, déplacés ou supprimés.

Enfin, après avoir terminé ces manipulations, j'ai supprimé les trois sous-dossiers **scan**, **logs** et **scripts**. Pour m'assurer de leur suppression, j'ai listé le contenu du dossier **Cybersec**, constatant que seul le fichier **README.md** restait présent.

Ces différentes opérations m'ont permis d'acquérir des compétences essentielles en gestion de fichiers sous **Linux**. J'ai appris à créer, modifier, copier, déplacer et supprimer des fichiers et des dossiers en ligne de commande, ce qui est une compétence clé en cybersécurité et en administration système.

Analyse et Scan du Réseau avec Nmap

Dans cette section, j'ai effectué une analyse du réseau en utilisant plusieurs commandes Linux, notamment **ifconfig** (ou **ip a**) pour identifier les informations réseau de ma machine, puis **nmap** pour scanner mon réseau local et détecter les appareils connectés.

La commande ip a

```
(scelent@Kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault 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: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DO  
WN group default qlen 1000  
    link/ether a0:1d:48:f6:0b:3a brd ff:ff:ff:ff:ff:ff  
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP g  
roup default qlen 1000  
    link/ether fc:f8:ae:fc:d1:3b brd ff:ff:ff:ff:ff:ff  
    inet 192.168.231.170/24 brd 192.168.231.255 scope global dynamic noprefix  
route wlan0  
        valid_lft 1810sec preferred_lft 1810sec  
    inet6 fe80::fef8:aefc:fefc:d13b/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Utilisez **nmap** pour scanner votre réseau local et identifier les appareils connectés.

```
(scelent@Kali)-[~]  
$ nmap -sn 192.168.231.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 22:57 EST  
Nmap scan report for 192.168.231.5  
Host is up (0.033s latency).  
MAC Address: DC:74:A8:13:F8:02 (Samsung Electronics)  
Nmap scan report for 192.168.231.208  
Host is up (0.089s latency).  
MAC Address: 8E:CC:B5:0E:AD:E8 (Unknown)  
Nmap scan report for 192.168.231.170  
Host is up.  
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.76 seconds
```

Manipuler les permissions :

Créez un fichier secret.txt

```
(scelent@Kali)-[~]  
$ touch secret.txt
```

changez ses permissions pour qu'il ne soit accessible qu'en lecture par le propriétaire.

```
(scelent@Kali)-[~]  
$ chmod 400 secret.txt
```

```
(scelent@Kali)-[~]  
$ ls -l secret.txt  
-r----- 1 scelent scelent 0 12 fév 23:00 secret.txt  
(scelent@Kali)-[~]
```

Utiliser grep :

Créez un fichier log.txt avec des lignes de texte, puis utilisez grep pour rechercher un mot spécifique.

```
(sclent@Kali)-[~]  
$ echo "Salut je suis Celent et je suis nouveuax sur linux " > Cybersec/log.txt  
  
(sclent@Kali)-[~]  
$ echo "Salut je suis Celent et je suis nouveuax sur linux " >> Cybersec/log.txt  
  
(sclent@Kali)-[~]  
$ echo " Je trouve que linux est tres securiser " >> Cybersec/log.txt  
  
(sclent@Kali)-[~]  
$ cat Cybersec/log.txt  
Salut je suis Celent et je suis nouveuax sur linux  
Salut je suis Celent et je suis nouveuax sur linux  
 Je trouve que linux est tres securiser  
  
(sclent@Kali)-[~]  
$ grep "linux" Cybersec/log.txt  
Salut je suis Celent et je suis nouveuax sur linux  
Salut je suis Celent et je suis nouveuax sur linux  
 Je trouve que linux est tres securiser
```

Exécuter ces commandes

df -h


```
(scelent@Kali)-[~]
$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                3,8G      0  3,8G   0% /dev
tmpfs                785M    1,5M  784M   1% /run
/dev/sda5            64G     17G   44G  28% /
tmpfs                3,9G    4,0K  3,9G   1% /dev/shm
tmpfs                1,0M      0  1,0M   0% /run/credentials/systemd-journald.service
tmpfs tmpfs suivante 5,0M      0  5,0M   0% /run/lock
tmpfs                3,9G   244K  3,9G   1% /tmp
tmpfs                1,0M      0  1,0M   0% /run/credentials/getty@tty1.service
tmpfs                785M   116K  785M   1% /run/user/1000
(scelent@Kali)-[~]
```

du -sh

```
(scelent@Kali)-[~]
$ du -sh
211M .
(scelent@Kali)-[~]
```

free -h

```
(scelent@Kali)-[~]
$ free -h
              total        used        libre    partagé  tamp/cache  disponible
Mem:          7,7Gi        3,0Gi        3,6Gi        728Mi        2,1Gi        4,7Gi
Échange:       3,5Gi           0B        3,5Gi
(scelent@Kali)-[~]
```

ps aux

```
(scelent@Kali)-[~]
$ ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.1 23092 14404 ?        Ss   20:41   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    20:41   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    20:41   0:00 [pool_workqueue_release]
root          4  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-netns]
root           9  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/0:0H-events_highpri]
root          12  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    20:41   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    20:41   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    20:41   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    20:41   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    20:41   0:02 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    20:41   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          19  0.0  0.0      0     0 ?        S    20:41   0:00 [rcu_exp_gp_kthread_worker]
root          20  0.0  0.0      0     0 ?        S    20:41   0:00 [migration/0]
root          21  0.0  0.0      0     0 ?        S    20:41   0:00 [idle_inject/0]
root          22  0.0  0.0      0     0 ?        S    20:41   0:00 [cpuhp/0]
root          23  0.0  0.0      0     0 ?        S    20:41   0:00 [cpuhp/2]
root          24  0.0  0.0      0     0 ?        S    20:41   0:00 [idle_inject/2]
root          25  0.0  0.0      0     0 ?        S    20:41   0:00 [migration/2]
root          26  0.0  0.0      0     0 ?        S    20:41   0:00 [ksoftirqd/2]
root          28  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/2:0H-events_highpri]
root          29  0.0  0.0      0     0 ?        S    20:41   0:00 [cpuhp/1]
root          30  0.0  0.0      0     0 ?        S    20:41   0:00 [idle_inject/1]
root          31  0.0  0.0      0     0 ?        S    20:41   0:00 [migration/1]
root          32  0.0  0.0      0     0 ?        S    20:41   0:00 [ksoftirqd/1]
root          34  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/1:0H-events_highpri]
root          35  0.0  0.0      0     0 ?        S    20:41   0:00 [cpuhp/3]
root          36  0.0  0.0      0     0 ?        S    20:41   0:00 [idle_inject/3]
root          37  0.0  0.0      0     0 ?        S    20:41   0:00 [migration/3]
root          38  0.0  0.0      0     0 ?        S    20:41   0:00 [ksoftirqd/3]
root          40  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/3:0H-events_highpri]
root          43  0.0  0.0      0     0 ?        I    20:41   0:02 [kworker/u16:2-events_unbound]
root          45  0.0  0.0      0     0 ?        S    20:41   0:00 [kdevtmpfs]
root          46  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-inet_frag_wq]
root          47  0.0  0.0      0     0 ?        S    20:41   0:00 [kauditd]
root          48  0.0  0.0      0     0 ?        S    20:41   0:00 [khungtaskd]
root          49  0.0  0.0      0     0 ?        S    20:41   0:00 [oom_reaper]
root          50  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-writeback]
root          51  0.0  0.0      0     0 ?        S    20:41   0:00 [kcompactd0]
root          52  0.0  0.0      0     0 ?        SN   20:41   0:00 [ksmd]
root          53  0.0  0.0      0     0 ?        SN   20:41   0:00 [khugepaged]
root          54  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-kintegrityd]
root          55  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-kblockd]
root          56  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-blkcg_punt_bio]
root          58  0.0  0.0      0     0 ?        S    20:41   0:00 [irq/9-acpi]
root          61  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-tpm_dev_wq]
root          62  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-edac-poller]
root          63  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-devfreq_wq]
root          64  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/1:1H-events_highpri]
root          65  0.0  0.0      0     0 ?        S    20:41   0:00 [kswapd0]
root          72  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-kthrotld]
root          76  0.0  0.0      0     0 ?        S    20:41   0:00 [irq/42-pciehp]
root          77  0.0  0.0      0     0 ?        I<   20:41   0:00 [kworker/R-acpi_thermal_pm]
```

lspci

```
(scelent@Kali)-[~]
$ lspci
00:00.0 Host bridge: Intel Corporation Haswell-ULT DRAM Controller (rev 0b)
00:02.0 VGA compatible controller: Intel Corporation Haswell-ULT Integrated Graphics Controller (rev 0b)
00:03.0 Audio device: Intel Corporation Haswell-ULT HD Audio Controller (rev 0b)
00:14.0 USB controller: Intel Corporation 8 Series USB xHCI HC (rev 04)
00:16.0 Communication controller: Intel Corporation 8 Series HECI #0 (rev 04)
00:16.3 Serial controller: Intel Corporation 8 Series HECI KT (rev 04)
00:19.0 Ethernet controller: Intel Corporation Ethernet Connection I218-LM (rev 04)
00:1b.0 Audio device: Intel Corporation 8 Series HD Audio Controller (rev 04)
00:1c.0 PCI bridge: Intel Corporation 8 Series PCI Express Root Port 1 (rev e4)
00:1c.3 PCI bridge: Intel Corporation 8 Series PCI Express Root Port 4 (rev e4)
00:1c.5 PCI bridge: Intel Corporation 8 Series PCI Express Root Port 6 (rev e4)
00:1d.0 USB controller: Intel Corporation 8 Series USB EHCI #1 (rev 04)
00:1f.0 ISA bridge: Intel Corporation 8 Series LPC Controller (rev 04)
00:1f.2 SATA controller: Intel Corporation 8 Series SATA Controller 1 [AHCI mode] (rev 04)
00:1f.3 SMBus: Intel Corporation 8 Series SMBus Controller (rev 04)
02:00.0 Network controller: Intel Corporation Wireless 7260 (rev 73)
03:00.0 Unassigned class [ff00]: Realtek Semiconductor Co., Ltd. RTS5227 PCI Express Card Reader (rev 01)
```

sudo apt install traceroute

```
(scelent@Kali)-[~]
$ sudo apt install traceroute
[sudo] Mot de passe de scelent :
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      libgl1-mesa-dev      libx10.9      libtag1v5-ct1 -b
  libbfio1               libgles-dev          libmagickcore-6.q16-7-extra libtag1v5-vanilla
  libc++1-19             libgles1             libmagickcore-6.q16-7t64  libtagc0
  libc++abi1-19          libglvnd-core-dev   libmagickwand-6.q16-7t64  libunwind-19
  libcapstone4           libglvnd-dev         libmbedcrypto7t64        libx265-209
  libdirectfb-1.7-7t64   libgtksourceview-3.0-1 libpaper1      python3-appdirs
  libegl-dev             libgtksourceview-3.0-common libqt5x11extras5
  libfmt9                libgtksourceviewmm-3.0-0v5 libsuperlu6
Veuillez utiliser « sudo apt autoremove » pour les supprimer.

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

traceroute google.com

```
(scelent@Kali)-[~]
$ traceroute google.com
traceroute to google.com (172.217.15.206), 30 hops max, 60 byte packets
 1  192.168.231.208 (192.168.231.208)  2.986 ms  3.053 ms  3.634 ms
 2  172.29.189.234 (172.29.189.234)  48.316 ms  *  *
 3  172.29.189.233 (172.29.189.233)  62.000 ms  172.29.189.229 (172.29.189.229)  71.781 ms  71.765 ms
 4  172.29.155.58 (172.29.155.58)  62.590 ms  172.29.149.94 (172.29.149.94)  61.934 ms  61.997 ms
 5  172.29.149.233 (172.29.149.233)  71.700 ms  172.29.155.57 (172.29.155.57)  71.684 ms  172.29.149.233
    (172.29.149.233)  71.668 ms
 6  172.29.149.94 (172.29.149.94)  62.043 ms  36.668 ms  55.017 ms
 7  172.20.179.13 (172.20.179.13)  84.457 ms  172.31.5.1 (172.31.5.1)  84.442 ms  172.29.149.233 (172.29
    .149.233)  58.504 ms
 8  172.31.13.43 (172.31.13.43)  84.410 ms  172.29.155.56 (172.29.155.56)  84.394 ms  123.004 ms
 9  66.54.126.96 (66.54.126.96)  122.988 ms  122.971 ms  122.955 ms
10  172.31.13.43 (172.31.13.43)  122.940 ms  72.14.217.114 (72.14.217.114)  132.779 ms  172.31.13.43 (17
    2.31.13.43)  122.909 ms
11  66.54.126.96 (66.54.126.96)  74.910 ms  142.250.225.79 (142.250.225.79)  124.861 ms  66.54.126.96 (6
    6.54.126.96)  75.061 ms
12  142.250.60.159 (142.250.60.159)  106.829 ms  72.14.217.114 (72.14.217.114)  98.805 ms  108.170.234.7
    5 (108.170.234.75)  106.416 ms
13  mia09s20-in-f14.1e100.net (172.217.15.206)  107.197 ms  107.179 ms  107.290 ms
```

netstat -tuln

```
(scelent@Kali)-[~]
$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
udp 0 0 0.0.0.0:50881 0.0.0.0:*
udp 0 0 0.0.0.0:44466 0.0.0.0:*
udp 0 0 192.168.231.170:3702 0.0.0.0:*
udp 0 0 239.255.255.250:3702 0.0.0.0:*
udp6 0 0 :::41383 :::*
udp6 0 0 fe80::fef8:aeff:fe:3702 :::*
udp6 0 0 ff02::c:3702 :::*
```

ss -tuln

```
(scelent@Kali)-[~]
$ ss -tuln
Netid  State  Recv-Q  Send-Q           Local Address:Port           Peer Address:Port
udp    UNCONN 0        0                0.0.0.0:50881                0.0.0.0:*
udp    UNCONN 0        0                0.0.0.0:44466                0.0.0.0:*
udp    UNCONN 0        0                192.168.231.170:3702         0.0.0.0:*
udp    UNCONN 0        0                239.255.255.250:3702         0.0.0.0:*
udp    UNCONN 0        0                *:41383                      *:
udp    UNCONN 0        0                [fe80::fef8:aeff:fefc:d13b]%wlan0:3702  [::]:*
udp    UNCONN 0        0                [ff02::c]%wlan0:3702         [::]:*
```


journalctl

```
(scelent@Kali)-[~]
$ journalctl
fév 01 06:34:24 Kali kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-10)) prebuilt on Debian GNU/Linux 12 (trixie)
fév 01 06:34:24 Kali kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=dccb1b6e-5500-4b00-b000-000000000000
fév 01 06:34:24 Kali kernel: BIOS-provided physical RAM map:
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009dbff] usable
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000009dc00-0x000000000009ffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x00000000000e0000-0x00000000000fffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x0000000001000000-0x000000000bab7efff] usable
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000bab7f000-0x000000000bbe7efff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000bbe7f000-0x000000000bbf7efff] ACPI NVS
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000bbf7f000-0x000000000bbffefff] ACPI data
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000bbfff000-0x000000000bbffffff] usable
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000bc000000-0x000000000bf1fffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000e0000000-0x000000000efffffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec0ffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000fed10000-0x000000000fed13fff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000fed18000-0x000000000fed19fff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000fed1c000-0x000000000fed1ffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee0ffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x000000000ff800000-0x000000000ffffffff] reserved
fév 01 06:34:24 Kali kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000023edfffff] usable
fév 01 06:34:24 Kali kernel: NX (Execute Disable) protection: active
fév 01 06:34:24 Kali kernel: APIC: Static calls initialized
fév 01 06:34:24 Kali kernel: SMBIOS 2.7 present.
fév 01 06:34:24 Kali kernel: DMI: Hewlett-Packard HP EliteBook 850 G1/198F, BIOS L71 Ver. 01.05 12/04
fév 01 06:34:24 Kali kernel: DMI: Memory slots populated: 2/2
fév 01 06:34:24 Kali kernel: tsc: Fast TSC calibration using PIT
fév 01 06:34:24 Kali kernel: tsc: Detected 2693.792 MHz processor
fév 01 06:34:24 Kali kernel: e820: update [mem 0x000000000-0x00000ffff] usable ==> reserved
fév 01 06:34:24 Kali kernel: e820: remove [mem 0x000a00000-0x000ffffff] usable
fév 01 06:34:24 Kali kernel: last_pfn = 0x23ee00 max_arch_pfn = 0x400000000
fév 01 06:34:24 Kali kernel: MTRR map: 8 entries (3 fixed + 5 variable; max 23), built from 10 variable entries
fév 01 06:34:24 Kali kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
fév 01 06:34:24 Kali kernel: last_pfn = 0xbc000 max_arch_pfn = 0x400000000
fév 01 06:34:24 Kali kernel: Using GB pages for direct mapping
fév 01 06:34:24 Kali kernel: RAMDISK: [mem 0x296590000-0x30b23ffff]
fév 01 06:34:24 Kali kernel: ACPI: Early table checksum verification disabled
fév 01 06:34:24 Kali kernel: ACPI: RSDP 0x00000000000F2FE0 000024 (v02 HPQOEM)
fév 01 06:34:24 Kali kernel: ACPI: XSDT 0x000000000BBFFE120 0000AC (v01 HPQOEM SLIC-MPC 00000001 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: FACP 0x000000000BBFFC000 00010C (v05 HPQOEM 198F 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: DSDT 0x000000000BBFD1000 0252A1 (v02 HPQOEM 198F 00000001 INTL >
fév 01 06:34:24 Kali kernel: ACPI: FACS 0x000000000BBDE4000 000040
fév 01 06:34:24 Kali kernel: ACPI: FACS 0x000000000BBDE4000 000040
fév 01 06:34:24 Kali kernel: ACPI: HPET 0x000000000BBFFB000 000038 (v01 HPQOEM 198F 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: APIC 0x000000000BBFFA000 0000BC (v01 HPQOEM 198F 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: MCFG 0x000000000BBFF9000 00003C (v01 HPQOEM 198F 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: TCPA 0x000000000BBFF7000 000032 (v02 HPQOEM 198F 00000000 HP >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFCE000 000313 (v01 HPQOEM SATAHci 00001000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFCD000 00048A (v01 HPQOEM PtidDevc 00001000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: SLIC 0x000000000BBFCC000 000176 (v01 HPQOEM SLIC-MPC 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: MSDM 0x000000000BBFCB000 000055 (v03 HPQOEM SLIC-MPC 00000000 HP >
fév 01 06:34:24 Kali kernel: ACPI: FPDT 0x000000000BBFCA000 000044 (v01 HPQOEM 198F 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: BGRT 0x000000000BBFC9000 000038 (v00 HPQOEM 198F 00000001 HP >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFC5000 000466 (v01 Isct IsctAsl 00003000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFC4000 000544 (v01 PmRef Cpu0Ist 00003000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFC3000 000AF3 (v01 PmRef CpuPm 00003000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFC2000 0001D5 (v01 PmRef LakeTiny 00003000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: SSDT 0x000000000BBFC1000 0006BD (v01 SaSsdT SaSsdT 00003000 INTL >
fév 01 06:34:24 Kali kernel: ACPI: ASF! 0x000000000BBFF8000 0000A5 (v32 HPQOEM 198F 00000001 HP >
```

journalctl -f

```
(scelent@Kali)-[~]
$ journalctl -f
fév 12 23:46:59 Kali systemd[996]: Starting xfconfd.service - Xfce configuration service...
fév 12 23:46:59 Kali systemd[996]: Started xfconfd.service - Xfce configuration service.
fév 12 23:47:03 Kali dbus-daemon[667]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.125' (uid=1000 pid=96241 comm="xfce4-screenshooter --region")
fév 12 23:47:03 Kali systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 12 23:47:03 Kali systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 12 23:47:03 Kali dbus-daemon[667]: [system] Successfully activated service 'org.freedesktop.hostname1'
fév 12 23:47:06 Kali dbus-daemon[1018]: [session uid=1000 pid=1018 pidfd=5] Activating via systemd: service name='org.freedesktop.thumbnails.Thumbnailer1' unit='tumblerd.service' requested by ':1.29' (uid=1000 pid=1190 comm="Thunar --sm-client-id 274a1b3de-a6a8-4c07-9636-7eb")
fév 12 23:47:06 Kali systemd[996]: Starting tumblerd.service - Thumbnailing service...
fév 12 23:47:06 Kali dbus-daemon[1018]: [session uid=1000 pid=1018 pidfd=5] Successfully activated service 'org.freedesktop.thumbnails.Thumbnailer1'
fév 12 23:47:06 Kali systemd[996]: Started tumblerd.service - Thumbnailing service.
fév 12 23:47:33 Kali systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

journalctl -b

```
(scelent@Kali)-[~]
$ journalctl -b
fév 12 20:41:26 Kali kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-10)) #1 SMP PREEMPT_DYNAMIC Mon Feb 12 20:41:26 UTC 2025
fév 12 20:41:26 Kali kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=dccb1b6e-5d00-4b00-b000-000000000000 ro
fév 12 20:41:26 Kali kernel: BIOS-provided physical RAM map:
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009dbff] usable
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x00000000000009dc00-0x00000000000009ffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x0000000000000e0000-0x0000000000000fffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000bab7efff] usable
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000bab7f000-0x000000000000bbe7efff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000bbe7f000-0x000000000000bbf7efff] ACPI NVS
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000bbf7f000-0x000000000000bbffe7ff] ACPI data
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000bbfff000-0x000000000000bbffffff] usable
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000bc000000-0x000000000000bf1fffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000e0000000-0x000000000000efffffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000fec00000-0x000000000000fec0ffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000fed10000-0x000000000000fed13fff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000fed18000-0x000000000000fed19fff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000fed1c000-0x000000000000fed1ffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000fee00000-0x000000000000fee0ffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x000000000000ff800000-0x000000000000ffffffff] reserved
fév 12 20:41:26 Kali kernel: BIOS-e820: [mem 0x00000000000100000000-0x0000000000023edfffff] usable
fév 12 20:41:26 Kali kernel: NX (Execute Disable) protection: active
fév 12 20:41:26 Kali kernel: APIC: Static calls initialized
fév 12 20:41:26 Kali kernel: SMBIOS 2.7 present.
fév 12 20:41:26 Kali kernel: DMI: Hewlett-Packard HP EliteBook 850 G1/198F, BIOS L71 Ver. 01.05 12/04/2024
fév 12 20:41:26 Kali kernel: DMI: Memory slots populated: 2/2
fév 12 20:41:26 Kali kernel: tsc: Fast TSC calibration using PIT
fév 12 20:41:26 Kali kernel: tsc: Detected 2693.977 MHz processor
fév 12 20:41:26 Kali kernel: e820: update [mem 0x000000000-0x00000ffff] usable ==> reserved
fév 12 20:41:26 Kali kernel: e820: remove [mem 0x000a00000-0x000fffff] usable
fév 12 20:41:26 Kali kernel: last_pfn = 0x23ee00 max_arch_pfn = 0x400000000
fév 12 20:41:26 Kali kernel: MTRR map: 8 entries (3 fixed + 5 variable; max 23), built from 10 variables
fév 12 20:41:26 Kali kernel: x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
fév 12 20:41:26 Kali kernel: last_pfn = 0xbc000 max_arch_pfn = 0x400000000
fév 12 20:41:26 Kali kernel: Using GB pages for direct mapping
fév 12 20:41:26 Kali kernel: RAMDISK: [mem 0x2967d000-0x30b35ffff]
fév 12 20:41:26 Kali kernel: ACPI: Early table checksum verification disabled
fév 12 20:41:26 Kali kernel: ACPI: RSDP 0x000000000000F2FE0 000024 (v01 HPQOEM)
fév 12 20:41:26 Kali kernel: ACPI: XSDT 0x0000000000BBFF120 0000AC (v01 HPQOEM SLIC-MPC 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: FACP 0x0000000000BBFFC00 00010C (v05 HPQOEM 198F 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: DSDT 0x0000000000BBFD100 0252A1 (v02 HPQOEM 198F 00000001 INTL >
fév 12 20:41:26 Kali kernel: ACPI: FACS 0x0000000000BBDE400 000040
fév 12 20:41:26 Kali kernel: ACPI: FACS 0x0000000000BBDE400 000040
fév 12 20:41:26 Kali kernel: ACPI: HPET 0x0000000000BBFFB00 000038 (v01 HPQOEM 198F 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: APIC 0x0000000000BBFFA00 0000BC (v01 HPQOEM 198F 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: MCFG 0x0000000000BBFF900 00003C (v01 HPQOEM 198F 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: TCPA 0x0000000000BBFF700 000032 (v02 HPQOEM 198F 00000000 HP >
fév 12 20:41:26 Kali kernel: ACPI: SSDT 0x0000000000BBFFC00 000313 (v01 HPQOEM SataAhci 00001000 INTL >
fév 12 20:41:26 Kali kernel: ACPI: SSDT 0x0000000000BBFFC00 00048A (v01 HPQOEM PtidDevc 00001000 INTL >
fév 12 20:41:26 Kali kernel: ACPI: SLIC 0x0000000000BBFFC00 000176 (v01 HPQOEM SLIC-MPC 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: MSDM 0x0000000000BBFFC00 000055 (v03 HPQOEM SLIC-MPC 00000000 HP >
fév 12 20:41:26 Kali kernel: ACPI: FPDT 0x0000000000BBFFA00 000044 (v01 HPQOEM 198F 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: BGRT 0x0000000000BBFF900 000038 (v00 HPQOEM 198F 00000001 HP >
fév 12 20:41:26 Kali kernel: ACPI: SSDT 0x0000000000BBFF500 000466 (v01 Isct IsctAsl 00003000 INTL >
fév 12 20:41:26 Kali kernel: ACPI: SSDT 0x0000000000BBFFC00 000544 (v01 PmRef Cpu0Ist 00003000 INTL >
fév 12 20:41:26 Kali kernel: ACPI: SSDT 0x0000000000BBFF300 000AF3 (v01 PmRef CpuPm 00003000 INTL >
```

journalctl -n 10

```
(sclent@Kali)-[~]
$ journalctl -n 10
fév 12 23:47:03 Kali dbus-daemon[667]: [system] Successfully activated service 'org.freedesktop.hostname1'
fév 12 23:47:06 Kali dbus-daemon[1018]: [session uid=1000 pid=1018 pidfd=5] Activating via systemd: service name='org.freedesktop.thumbnai' unit='tumblerd.service' requested by ':1.29' (uid=1000 pid=1190 comm="Thunar --s"
fév 12 23:47:06 Kali systemd[996]: Starting tumblerd.service - Thumbnailing service...
fév 12 23:47:06 Kali dbus-daemon[1018]: [session uid=1000 pid=1018 pidfd=5] Successfully activated service 'org.freedesktop.thumbnails.Thumbnailer1'
fév 12 23:47:06 Kali systemd[996]: Started tumblerd.service - Thumbnailing service.
fév 12 23:47:33 Kali systemd[1]: systemd-hostnamed.service: Deactivated successfully.
fév 12 23:48:58 Kali dbus-daemon[667]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.127' (uid=1000 pid=97287 comm="xfce4-screenshooter --region"
fév 12 23:48:58 Kali systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 12 23:48:58 Kali systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 12 23:48:58 Kali dbus-daemon[667]: [system] Successfully activated service 'org.freedesktop.hostname1'
lines 1-10/10 (END) ... skipping ...
fév 12 23:47:03 Kali dbus-daemon[667]: [system] Successfully activated service 'org.freedesktop.hostname1'
fév 12 23:47:06 Kali dbus-daemon[1018]: [session uid=1000 pid=1018 pidfd=5] Activating via systemd: service name='org.freedesktop.thumbnails.Thumbnailer1' unit='tumblerd.service' requested by ':1.29' (uid=1000 pid=1190 comm="Thunar --s"
fév 12 23:47:06 Kali systemd[996]: Starting tumblerd.service - Thumbnailing service...
fév 12 23:47:06 Kali dbus-daemon[1018]: [session uid=1000 pid=1018 pidfd=5] Successfully activated service 'org.freedesktop.thumbnails.Thumbnailer1'
fév 12 23:47:06 Kali systemd[996]: Started tumblerd.service - Thumbnailing service.
fév 12 23:47:33 Kali systemd[1]: systemd-hostnamed.service: Deactivated successfully.
fév 12 23:48:58 Kali dbus-daemon[667]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.127' (uid=1000 pid=97287 comm="xfce4-screenshooter --region"
fév 12 23:48:58 Kali systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
fév 12 23:48:58 Kali systemd[1]: Started systemd-hostnamed.service - Hostname Service.
fév 12 23:48:58 Kali dbus-daemon[667]: [system] Successfully activated service 'org.freedesktop.hostname1'
```

date

```
(sclent@Kali)-[~]
$ date
mer 12 fév 2025 23:50:20 EST
```

timedatectl

```
(sclent@Kali)-[~]
$ timedatectl
          Local time: mer 2025-02-12 23:50:40 EST
          Universal time: jeu 2025-02-13 04:50:40 UTC
                RTC time: jeu 2025-02-13 04:50:40
          Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

hostnamectl

```
(sclent@Kali)-[~]
$ hostnamectl
          Static hostname: Kali
                Icon name: computer-laptop
                Chassis: laptop
          Machine ID: 6796cd03e7bd4612a1a94c2a9b83088b
          Boot ID: 3ba2257aba3f49cda2c0202ea02cc83c
    Operating System: Kali GNU/Linux Rolling
           Kernel: Linux 6.11.2-amd64
        Architecture: x86-64
        Hardware Vendor: Hewlett-Packard
        Hardware Model: HP EliteBook 850 G1
    Firmware Version: L71 Ver. 01.05
        Firmware Date: Wed 2013-12-04
        Firmware Age: 11y 2month 1w 3d
```


Pour changer le nom d'hôte, vous pouvez utiliser la commande suivante

`sudo hostnamectl set-hostname MIDAS`

```
(scelent@Kali)-[~]  
$ sudo hostnamectl set-hostname MIDAS  
  
(scelent@Kali)-[~]  
$ hostnamectl  
Static hostname: MIDAS  
Icon name: computer-laptop  
Chassis: laptop   
Machine ID: 6796cd03e7bd4612a1a94c2a9b83088b  
Boot ID: 3ba2257aba3f49cda2c0202ea02cc83c  
Operating System: Kali GNU/Linux Rolling  
Kernel: Linux 6.11.2-amd64  
Architecture: x86-64  
Hardware Vendor: Hewlett-Packard  
Hardware Model: HP EliteBook 850 G1  
Firmware Version: L71 Ver. 01.05  
Firmware Date: Wed 2013-12-04  
Firmware Age: 11y 2month 1w 3d
```

Ceci a ete mon travail realiser sur linux avec les lignes de code et screenshots