UNIVERSITE DE TECHNOLOGIE D'HAÏTI ET DU SCIENCE INFORMATIQUE

(UNITECH)

Nom: SAINT JEAN

Prenom: Wills Edhersen

Cour : Cybersecurity

Devoir: TD2

Date: Le 14/02/2025

1- **Créez** un dossier cybersec avec trois sous-dossiers : scan , logs , scripts .

Cd Bureau
Mkdir cybersec
Cd cybersec
Mkdir scan
Mkdir logs
Mkdir
scripts

```
wills1@pentest: ~/Bureau/cybersec/logs
Fichier  Actions  Éditer  Vue  Aide
┌──(wills1㉿pentest)-[~]
└─$ cd Bureau

┌──(wills1㉿pentest)-[~/Bureau]
└─$ mkdir cybersec

┌──(wills1㉿pentest)-[~/Bureau]
└─$ cd cybersec
```

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ mkdir scan

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ mkdir logs

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ mkdir scripts
```

2-Ajoutez un fichier notes.txt dans scan et logs.

Cd scan

Touch Notes.txt

Cd ..

Cd logs

Touch Notes.txt

```
wills1@pentest: ~/Bureau/cybersec/logs
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd scan

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ touch Notes.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cd ..

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd logs

┌──(wills1㉿pentest)-[~/Bureau/cybersec/logs]
└─$ touch Notes.txt
```

3-Ajoutez du contenu dans les fichiers textes (notes.txt), puis affichez le contenu des fichiers.

Cd scan

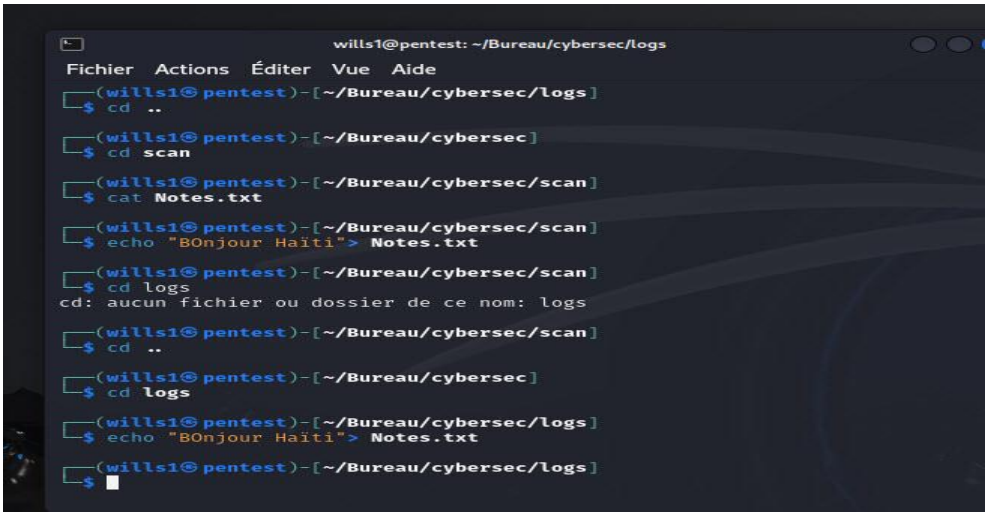
Cat Notes.txt

Echo ‘’Bonjour Haiti’’> Notes.txt

Cd logs

Cat Notes.txt

Echo ‘’Bonjour Haiti’’> Notes.txt



```
wills1@pentest: ~/Bureau/cybersec/logs
Fichier  Actions  Éditer  Vue  Aide

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cd ..

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd logs

┌──(wills1㉿pentest)-[~/Bureau/cybersec/logs]
└─$ touch Notes.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec/logs]
└─$ cat Notes.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec/logs]
└─$ cd..
cd.. : commande introuvable

┌──(wills1㉿pentest)-[~/Bureau/cybersec/logs]
└─$ cd ..

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd scan

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cat Notes.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
```

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

Cd scan

Cp Note.txt ~Bureau/cybersec/scan

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec/logs]
└─$ cd ..

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd scan

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cp Notes.txt ~/Bureau/cybersec/scripts/

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$
```

5-vérifier si le fichiers a été copié.

Cd scripts

Cat Notes.txt

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cd ..

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd scripts

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scripts]
└─$ cat Notes.txt
Bonjour Haïti

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scripts]
└─$
```

6- Déplacez le fichier (notes.txt) dans le sous-dossier scan .

Mv ~/Bureau/cybersec/scan/Notes.txt ~/Bureau/cybersec/scripts

Ls -l

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ mv ~/Bureau/cybersec/scan/Notes.txt ~/Bureau/cybersec/scripts

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ ls -l
total 0

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$
```

7-Supprimez le fichier (notes.txt)dans le sous-dossier scripts . Vérifier si le fichiers a été supprimé.

Cd scripts

Rm Notes.txt

Ls -l

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cd ..

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ cd scripts

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scripts]
└─$ rm Notes.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scripts]
└─$ ls -l
total 0

┌──(wills1㉿pentest)-[~/Bureau/cybersec/scripts]
└─$
```

8-Supprimez les sous-dossiers : scan , logs , scripts .

rm –r scan

rm –r logs

rm –r scripts

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r scan

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r logs

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r scripts
```

9-vérifier si les sous-dossiers ont été supprimés.

ls -l

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r scan

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r logs

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r scripts
```

11- ifconfig ou ip a : Affiche les informations réseau

Ip a

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ 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: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:64:e1:e5 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 83466sec preferred_lft 83466sec
    inet6 fe80::a00:27ff:fe64:e1e5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

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

nmap

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-12 14:23 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

13-Créez un fichier secret.txt et changez ses permissions pour qu'il ne soit accessible qu'en lecture par le propriétaire

```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ touch secret.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ chmod 400 secret.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

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

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ touch logs.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ echo "je suis Wills Edhersen SAINT JEAN"> logs.txt

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ grep "Wills" logs.txt
je suis Wills Edhersen SAINT JEAN

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

Exécution des commandes

df -h

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev               423M       0  423M   0% /dev
tmpfs               97M    960K   96M   1% /run
/dev/sda1           26G     16G  9,0G  63% /
tmpfs              484M    4,0K  484M   1% /dev/shm
tmpfs              5,0M       0  5,0M   0% /run/lock
tmpfs              1,0M       0  1,0M   0% /run/credentials/systemd-journald.
service
tmpfs              1,0M       0  1,0M   0% /run/credentials/systemd-udev-load
-credentials.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.se
rvice
tmpfs              1,0M       0  1,0M   0% /run/credentials/systemd-tmpfiles-
setup-dev.service
tmpfs              484M    160K  484M   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.servic
e
tmpfs               97M    116K   97M   1% /run/user/1000

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

du -sh

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ du -sh
8,0K    .

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

free -h

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ free -h
              total        utilisé      libre     partagé tamp/cache   disponible
Mem:          967Mi        472Mi       169Mi        14Mi       479Mi        495Mi
Échange:      1,0Gi        205Mi       816Mi

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

ps aux

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  1.4  22572 13952 ?        Ss   13:33   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    13:33   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    13:33   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-netns]
root           8  0.1  0.0      0     0 ?        I    13:33   0:04 [kworker/0:0-ata_sff]
root           9  0.1  0.0      0     0 ?        I    13:33   0:05 [kworker/0:1-events]
root          12  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    13:33   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    13:33   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    13:33   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    13:33   0:01 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    13:33   0:01 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    13:33   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          19  0.0  0.0      0     0 ?        S    13:33   0:00 [rcu_exp_gp_kthread_worker]
root          20  0.0  0.0      0     0 ?        S    13:33   0:00 [migration/0]
root          21  0.0  0.0      0     0 ?        S    13:33   0:00 [idle_inject/0]
root          22  0.0  0.0      0     0 ?        S    13:33   0:00 [cpuhp/0]
root          24  0.0  0.0      0     0 ?        S    13:33   0:00 [kdevtmpfs]
root          25  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-inet_frag_wq]
root          26  0.1  0.0      0     0 ?        I    13:33   0:05 [kworker/u4:1-flush-8:0]
root          27  0.0  0.0      0     0 ?        S    13:33   0:00 [kauditd]
root          28  0.0  0.0      0     0 ?        S    13:33   0:00 [khungtaskd]
root          29  0.0  0.0      0     0 ?        S    13:33   0:00 [oom_reaper]
root          30  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-writeback]
root          32  0.0  0.0      0     0 ?        S    13:33   0:00 [kcompactd0]
root          33  0.0  0.0      0     0 ?        SN   13:33   0:00 [ksmd]
root          34  0.0  0.0      0     0 ?        SN   13:33   0:00 [khugepaged]
root          35  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-kintegrityd]
root          36  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-kblockd]
root          37  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-blkcg_punt_bio]
root          38  0.0  0.0      0     0 ?        S    13:33   0:00 [irq/9-acpi]
root          39  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-tpm_dev_wq]
root          40  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-edac-poller]
root          41  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-devfreq_wq]
root          42  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/0:1H-kblockd]
root          43  0.0  0.0      0     0 ?        S    13:33   0:01 [kswapd0]
root          51  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-kthrotld]
root          55  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-acpi_thermal_pm]
root          56  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-mld]
root          57  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-ipv6_addrconf]
root          62  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-kstrp]
root          66  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/u5:0-ttm]
root          71  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-cryptd]
root         167  0.0  0.0      0     0 ?        I<   13:33   0:00 [kworker/R-ata_sff]
root         169  0.0  0.0      0     0 ?        S    13:33   0:00 [scsi_eh_0]
```

Lspci

```
┌──(wills1㉿pentest)-[~/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)
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

sudo apt install traceroute

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ sudo apt install traceroute
[sudo] Mot de passe de wills1 :
traceroute est déjà la version la plus récente (1:2.1.6-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1167

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

traceroute google.com

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ traceroute google.com
traceroute to google.com (172.217.15.206), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  8.303 ms  7.766 ms  7.247 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

netstat –tuln

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

ss –tuln

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ ss -tuln
Netid                State                Recv-Q               Send-Q                              Local Address:Port                                  Peer Address:Port

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

journalctl

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl
fév 08 12:06:08 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-6) 14.2.0, GNU ld (GNU Binutils for Debian) 2.43.1) #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15)
fév 08 12:06:08 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=81479cf5-86c4-4039-b996-e2b3ca26376c ro quiet splash
fév 08 12:06:08 pentest kernel: BIOS-provided physical RAM map:
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffefffff] usable
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x00000000bfff0000-0x00000000bffffffff] ACPI data
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
fév 08 12:06:08 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
fév 08 12:06:08 pentest kernel: NX (Execute Disable) protection: active
fév 08 12:06:08 pentest kernel: APIC: Static calls initialized
fév 08 12:06:08 pentest kernel: SMBIOS 2.5 present.
fév 08 12:06:08 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
fév 08 12:06:08 pentest kernel: DMI: Memory slots populated: 0/0
fév 08 12:06:08 pentest kernel: Hypervisor detected: KVM
fév 08 12:06:08 pentest kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
fév 08 12:06:08 pentest kernel: kvm-clock: using sched offset of 7097515370620 cycles
fév 08 12:06:08 pentest kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
fév 08 12:06:08 pentest kernel: tsc: Detected 2399.998 MHz processor
fév 08 12:06:08 pentest kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
fév 08 12:06:08 pentest kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
fév 08 12:06:08 pentest kernel: last_pfn = 0x40000 max_arch_pfn = 0x400000000
fév 08 12:06:08 pentest kernel: MTRRs disabled by BIOS
fév 08 12:06:08 pentest kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
fév 08 12:06:08 pentest kernel: found SMP MP-table at [mem 0x0009ff00-0x0009ffff]
fév 08 12:06:08 pentest kernel: RAMDISK: [mem 0x29653000-0x30b20fff]
fév 08 12:06:08 pentest kernel: ACPI: Early table checksum verification disabled
fév 08 12:06:08 pentest kernel: ACPI: RSDP 0x000000000000E0000 000024 (v02 VBOX  )
fév 08 12:06:08 pentest kernel: ACPI: XSDT 0x00000000BFFF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
fév 08 12:06:08 pentest kernel: ACPI: FACP 0x00000000BFFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001 ASL  00000061)
fév 08 12:06:08 pentest kernel: ACPI: DSDT 0x00000000BFFF0470 002325 (v02 VBOX   VBOXBIOS 00000002 INTL 20100528)
fév 08 12:06:08 pentest kernel: ACPI: FACS 0x00000000BFFF0200 000040
fév 08 12:06:08 pentest kernel: ACPI: FACS 0x00000000BFFF0200 000040
fév 08 12:06:08 pentest kernel: ACPI: APIC 0x00000000BFFF0240 000054 (v02 VBOX   VBOXAPIC 00000001 ASL  00000061)
fév 08 12:06:08 pentest kernel: ACPI: SSDT 0x00000000BFFF02A0 0001CC (v01 VBOX   VBOXCPUT 00000002 INTL 20100528)
fév 08 12:06:08 pentest kernel: ACPI: Reserving FACP table memory at [mem 0x3fff00f0-0x3fff01e3]
fév 08 12:06:08 pentest kernel: ACPI: Reserving DSDT table memory at [mem 0x3fff0470-0x3fff2794]
fév 08 12:06:08 pentest kernel: ACPI: Reserving FACS table memory at [mem 0x3fff0200-0x3fff023f]
fév 08 12:06:08 pentest kernel: ACPI: Reserving FACS table memory at [mem 0x3fff0200-0x3fff023f]
fév 08 12:06:08 pentest kernel: ACPI: Reserving APIC table memory at [mem 0x3fff0240-0x3fff0293]
fév 08 12:06:08 pentest kernel: ACPI: Reserving SSDT table memory at [mem 0x3fff02a0-0x3fff046b]
fév 08 12:06:08 pentest kernel: No NUMA configuration found
fév 08 12:06:08 pentest kernel: Faking a node at [mem 0x0000000000000000-0x00000000bffffffff]
fév 08 12:06:08 pentest kernel: NODE_DATA(0) allocated [mem 0x3ffc5000-0x3ffeffff]
fév 08 12:06:08 pentest kernel: Zone ranges:
fév 08 12:06:08 pentest kernel:   DMA      [mem 0x0000000000001000-0x0000000000ffffff]
```

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -b
fév 12 13:33:44 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) >
fév 12 13:33:44 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.>
fév 12 13:33:44 pentest kernel: BIOS-provided physical RAM map:
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x000000003fff0000-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x0000000>
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x0000000>
fév 12 13:33:44 pentest kernel: NX (Execute Disable) protection: active
fév 12 13:33:44 pentest kernel: APIC: Static calls initialized
fév 12 13:33:44 pentest kernel: SMBIOS 2.5 present.
fév 12 13:33:44 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIO>
fév 12 13:33:44 pentest kernel: DMI: Memory slots populated: 0/0
fév 12 13:33:44 pentest kernel: Hypervisor detected: KVM
fév 12 13:33:44 pentest kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
fév 12 13:33:44 pentest kernel: kvm-clock: using sched offset of 27783628542>
fév 12 13:33:44 pentest kernel: clocksource: kvm-clock: mask: 0xffffffffffff>
fév 12 13:33:44 pentest kernel: tsc: Detected 2399.998 MHz processor
fév 12 13:33:44 pentest kernel: e820: update [mem 0x00000000-0x00000fff] usa>
fév 12 13:33:44 pentest kernel: e820: remove [mem 0x000a0000-0x000fffff] usa>
fév 12 13:33:44 pentest kernel: last_pfn = 0x40000 max_arch_pfn = 0x400000000
lines 1-24 ... skipping ...
fév 12 13:33:44 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-6) 14.2.0, GNU ld (GNU Binut
fév 12 13:33:44 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=81479cf5-86c4-4039-b996-e2b3ca26376c ro quiet spla
fév 12 13:33:44 pentest kernel: BIOS-provided physical RAM map:
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
fév 12 13:33:44 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
```

journalctl –f

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -f
fév 12 14:39:42 pentest systemd[1]: Finished phpsessionclean.service - Clean
php session files.
fév 12 14:42:44 pentest sudo[34474]:   wills1 : TTY=pts/0 ; PWD=/home/wills1/
Bureau/cybersec ; USER=root ; COMMAND=/usr/bin/apt install traceroute
fév 12 14:42:44 pentest sudo[34474]: pam_unix(sudo:session): session opened f
or user root(uid=0) by wills1(uid=1000)
fév 12 14:42:46 pentest sudo[34474]: pam_unix(sudo:session): session closed f
or user root
fév 12 14:45:01 pentest CRON[35713]: pam_unix(cron:session): session opened f
or user root(uid=0) by root(uid=0)
fév 12 14:45:01 pentest CRON[35714]: (root) CMD (command -v debian-sa1 > /dev
/null && debian-sa1 1 1)
fév 12 14:45:01 pentest CRON[35713]: pam_unix(cron:session): session closed f
or user root
fév 12 14:55:01 pentest CRON[40568]: pam_unix(cron:session): session opened f
or user root(uid=0) by root(uid=0)
fév 12 14:55:01 pentest CRON[40569]: (root) CMD (command -v debian-sa1 > /dev
/null && debian-sa1 1 1)
fév 12 14:55:01 pentest CRON[40568]: pam_unix(cron:session): session closed f
or user root
```

journalctl -b

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -n 10
fév 12 14:39:42 pentest systemd[1]: Finished phpsessionclean.service - Clean php session files.
fév 12 14:42:44 pentest sudo[34474]:   wills1 : TTY=pts/0 ; PWD=/home/wills1/Bureau/cybersec ; USER=root ; COMMAND=/usr/bin/apt install traceroute
fév 12 14:42:44 pentest sudo[34474]: pam_unix(sudo:session): session opened for user root(uid=0) by wills1(uid=1000)
fév 12 14:42:46 pentest sudo[34474]: pam_unix(sudo:session): session closed for user root
fév 12 14:45:01 pentest CRON[35713]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 12 14:45:01 pentest CRON[35714]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 12 14:45:01 pentest CRON[35713]: pam_unix(cron:session): session closed for user root
fév 12 14:55:01 pentest CRON[40568]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 12 14:55:01 pentest CRON[40569]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 12 14:55:01 pentest CRON[40568]: pam_unix(cron:session): session closed for user root

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$

wills1     962  0.0  0.7 380912  7084 ?        Ssl  13:35   0:00 /usr/libexec/at-spi-bus-launcher
wills1     969  0.0  0.4   7352  4608 ?        S    13:35   0:00 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 11 --address=unix:path=/run/user/1000/at-spi/bus_0
wills1     980  0.0  0.7 234048  7496 ?        Sl   13:35   0:00 /usr/libexec/at-spi2-registryd --use-gnome-session
wills1     988  0.0  0.0   9916   520 ?        Ss   13:35   0:00 /usr/bin/ssh-agent -s
wills1     995  0.0  0.3  81672  3060 ?        SLs  13:35   0:00 /usr/bin/gpg-agent --supervised
wills1     998  0.5  5.6 689080 56376 ?        Sl   13:35   0:19 xfwm4 --display :0.0 --sm-client-id 270023b2b-e10d-429b-9b77-d79bba322019
wills1    1003  0.0  0.1  17256  1424 ?        S    13:35   0:00 /usr/bin/VBoxClient --vmsvga
wills1    1004  0.0  0.3 215648  3508 ?        Sl   13:35   0:01 /usr/bin/VBoxClient --vmsvga
root      1008  0.0  0.0      0     0 ?        I<   13:35   0:00 [kworker/u5:1-ttm]
wills1    1013  0.0  0.7 312864  7180 ?        Ssl  13:35   0:00 /usr/libexec/gvfsd
wills1    1019  0.0  0.7 532636  7476 ?        Sl   13:35   0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f
wills1    1030  0.0  1.9 302588 19696 ?        Sl   13:36   0:00 xfsettingsd --display :0.0 --sm-client-id 22e1ecdbc-08a2-4707-b84a-42c7fe973a7a
wills1    1034  0.0  2.6 536392 26124 ?        Sl   13:36   0:01 xfce4-panel --display :0.0 --sm-client-id 26d7a8acb-a526-42c1-a3c8-e62f3ffb0ca7
wills1    1039  0.2  4.0 544072 40096 ?        Sl   13:36   0:08 Thunar --sm-client-id 2d811089c-0ff3-4090-8586-ed8c32bfadf6 --daemon
wills1    1045  0.1  4.1 565704 41228 ?        Sl   13:36   0:04 xfdesktop --display :0.0 --sm-client-id 2ea583794-2034-49ce-a097-19c7664b413e
wills1    1046  0.0  2.3 534896 23284 ?        Sl   13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1 27262983 whiskermenu Menu Whisker Afficher un menu p
wills1    1053  0.3  1.8 279992 18828 ?        Sl   13:36   0:14 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libcpugraph.so 13 27262988 cpugraph Graphique processeur Représentation
wills1    1054  0.0  1.4 410672 14552 ?        Sl   13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 14 27262989 systray Greffon de barre d'état Fournit des él
wills1    1055  0.2  1.7 338940 17072 ?        Sl   13:36   0:09 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libgenmon.so 15 27262990 genmon Moniteur générique Afficher la sortie d'
wills1    1056  0.0  2.1 459988 21592 ?        Sl   13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 16 27262991 pulseaudio Greffon PulseAudio Ajuste
wills1    1057  0.0  2.2 459988 21984 ?        Sl   13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 17 27262992 notification-plugin Greffon de not
wills1    1058  0.0  2.2 386832 22696 ?        Sl   13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 18 27262993 power-manager-plugin Greffon du gest
wills1    1060  0.0  1.8 386640 18524 ?        Sl   13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 22 27262994 actions Boutons d'action Déconnexion, verrouil
wills1    1094  0.0  1.5 407528 15576 ?        Ssl  13:36   0:00 /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
root      1096  0.0  0.9 317920  9848 ?        Ssl  13:36   0:00 /usr/libexec/upowerd
wills1    1121  0.0  1.7 263224 17600 ?        Sl   13:36   0:00 xfce4-power-manager --restart --sm-client-id 292ea27bf-c9db-4de9-80b6-8c0beaa4f550
wills1    1150  0.0  1.2 426316 12760 ?        Ssl  13:36   0:00 /usr/libexec/gvfs-udisks2-volume-monitor
root      1154  0.0  0.9 469256  9116 ?        Ssl  13:36   0:00 /usr/libexec/udisks2/udisksd
wills1    1172  0.0  0.8 389216  8344 ?        Ssl  13:36   0:00 /usr/libexec/gvfs-afc-volume-monitor
wills1    1178  0.0  0.6 308808  6624 ?        Ssl  13:36   0:00 /usr/libexec/gvfs-gphoto2-volume-monitor
wills1    1187  0.0  0.6 307784  6524 ?        Ssl  13:36   0:00 /usr/libexec/gvfs-goa-volume-monitor
wills1    1193  0.0  0.6 307852  6616 ?        Ssl  13:36   0:00 /usr/libexec/gvfs-mtp-volume-monitor
wills1    1203  0.0  2.1  64108 20924 ?        S    13:36   0:00 /usr/bin/python3 /usr/share/system-config-printer/applet.py
wills1    1205  0.0  0.6 308344  6156 ?        Sl   13:36   0:00 /usr/libexec/geoclue-2.0/demos/agent
wills1    1207  0.0  3.7 527624 36680 ?        Sl   13:36   0:01 /usr/bin/python3 /usr/bin/blueman-applet
wills1    1240  0.0  0.8 594972  8128 ?        Sl   13:36   0:00 xiccd
wills1    1244  0.0  1.1 256876 11748 ?        Sl   13:36   0:00 /usr/libexec/polkit-mate-authentication-agent-1
wills1    1248  0.0  1.5 336256 15436 ?        Sl   13:36   0:00 light-locker
wills1    1261  0.0  2.3 622628 23780 ?        Sl   13:36   0:00 nm-applet
wills1    1262  0.0  0.5 230560  5880 ?        Ssl  13:36   0:00 /usr/libexec/dconf-service
wills1    1279  0.0  0.8 534320  8732 ?        Sl   13:36   0:00 /usr/libexec/gvfsd-trash --spawner :1.22 /org/gtk/gvfs/exec_spaw/0
colord    1280  0.0  1.3 315716 13012 ?        Ssl  13:36   0:00 /usr/libexec/colord
wills1    1299  0.0  0.6 234408  6596 ?        Ssl  13:36   0:00 /usr/libexec/gvfsd-metadata
wills1    1421  0.0  0.6  46384  6880 ?        Ss   13:36   0:00 /usr/libexec/bluetooth/obexd
wills1    1835  0.1  7.0 466920 69760 ?        Sl   13:37   0:06 /usr/bin/qterminal
wills1    1846  0.2  0.6  11280  6612 pts/0    Ss   13:37   0:09 /usr/bin/zsh
root      8169  0.0  0.0      0     0 ?        I    13:49   0:00 [kworker/u4:0-events_unbound]
root     23767  0.0  0.0      0     0 ?        I    14:20   0:00 [kworker/u4:2]
root     32361  0.0  0.0      0     0 ?        I    14:28   0:00 [kworker/0:2]
wills1   32874  133  0.3   8512  3932 pts/0    R+   14:39   0:00 ps aux

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

journalctl -n 10

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -n 10
fév 12 14:39:42 pentest systemd[1]: Finished phpsessionclean.service - Clean php session files.
fév 12 14:42:44 pentest sudo[34474]:   wills1 : TTY=pts/0 ; PWD=/home/wills1/Bureau/cybersec ; USER=root ; COMMAND=/usr/bin/apt install traceroute
fév 12 14:42:44 pentest sudo[34474]: pam_unix(sudo:session): session opened for user root(uid=0) by wills1(uid=1000)
fév 12 14:42:46 pentest sudo[34474]: pam_unix(sudo:session): session closed for user root
fév 12 14:45:01 pentest CRON[35713]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 12 14:45:01 pentest CRON[35714]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 12 14:45:01 pentest CRON[35713]: pam_unix(cron:session): session closed for user root
fév 12 14:55:01 pentest CRON[40568]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 12 14:55:01 pentest CRON[40569]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 12 14:55:01 pentest CRON[40568]: pam_unix(cron:session): session closed for user root

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

date

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ date
mer 12 fév 2025 14:58:51 EST

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

timedatectl

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ timedatectl
               Local time: mer 2025-02-12 14:59:18 EST
           Universal time: mer 2025-02-12 19:59:18 UTC
                 RTC time: mer 2025-02-12 19:59:17
                Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

hostnamectl

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ hostnamectl
 Static hostname: pentest
       Icon name: computer-vm
         Chassis: vm 
      Machine ID: d0dcec37b9f94e4382461e05b041cb8a
         Boot ID: d5079bd72918400e8f322bbad7b573cd
  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 1w 6d

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```

Pour changer le nom d'hôte, vous pouvez utiliser la commande suivante sudo hostnamectl set-hostname [nouveau_nom]

```
┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$ sudo hostnamectl set-hostname [Edhersen]
[sudo] Mot de passe de wills1 :

┌──(wills1㉿pentest)-[~/Bureau/cybersec]
└─$
```