UNIVERSITE DE TECHNOLOGIE D'HAITI

UNITECH

Faculte des sciences Informatique

Cours: Cyber Securite

Sujet: Traveaux Diriges de Systeme d;Exploitation kali Linux

Nom du Depot: cybersec

Preparer par : Judith MAXIME

Proposer par: Ismael SAINT AMOUR

15 /02/25

Description Des resultats de la Tache

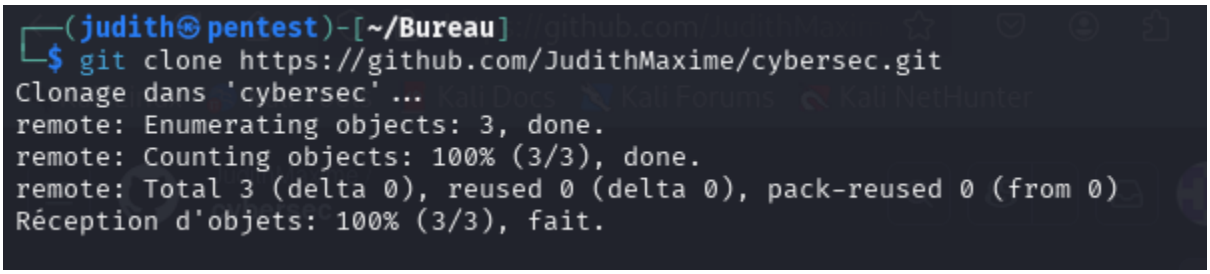
Les Etapes Realisees:

1.creation d'un depo GitHub

Nom:cybersec

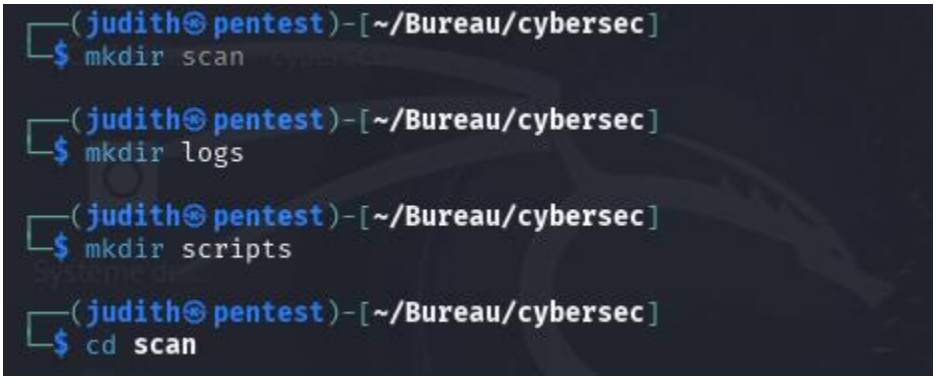
Description:Travauxdiriges de systemes d'exploitation Linux et de reseaux.

2.Clonage: qui permet de clone dans le repertoire local sur le bureau en utilisant la commande :

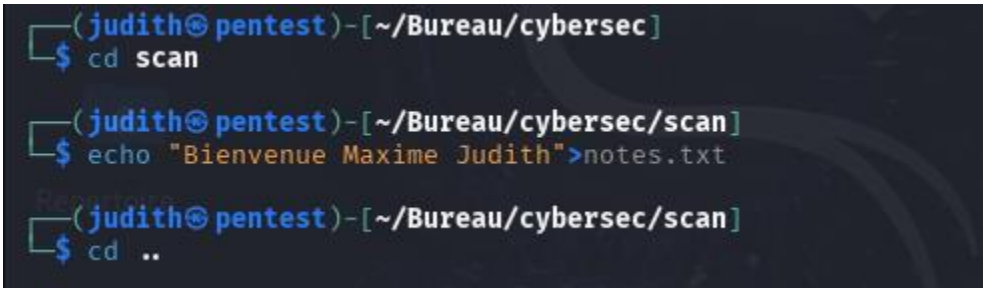


4.Creation de la structure de dossiers:

Creation des trois sous-Dossiers : scan,logs,scripts dans cybersec



Ajout d'un fichier notes.txt dans scan et logs.



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

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

┌──(judith㉿pentest)-[~/Bureau/cybersec/logs]
└─$ echo "Bienvenue Michel">notes.txt

┌──(judith㉿pentest)-[~/Bureau/cybersec/logs]
└─$ cat notes.txt
Bienvenue Michel
```

Copie du fichier (notes.txt dans le sous-dossier script.

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

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

┌──(judith㉿pentest)-[~/Bureau/cybersec/scan]
└─$ cat notes.txt
Bienvenue Maxime Judith
```

Verification du fichier qui a ete copie.

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

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

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

┌──(judith㉿pentest)-[~/Bureau/cybersec/scripts]
└─$ cat notes.txt
Bienvenue Maxime Judith
```

Deplacement du fichier (notes.txt) dans le sous-dossier scan.

```
┌──(judith㉿pentest)-[~/Bureau/cybersec/scripts]
└─$ rm notes.txt

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

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

Verification du fichier qui a ete supprime

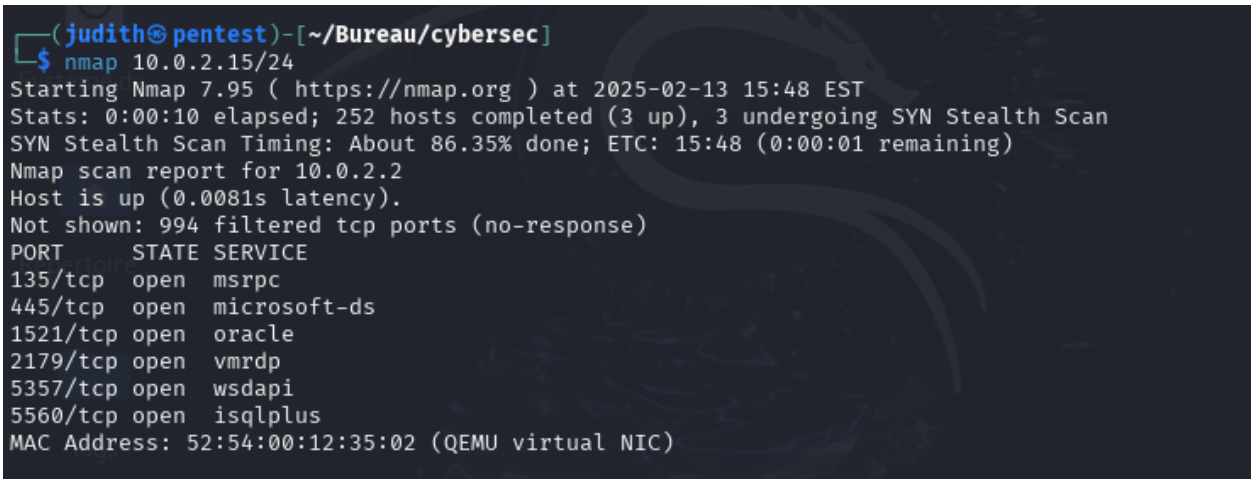
```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ rm -r  ~/Bureau/cybersec/scan/ ~/Bureau/cybersec/logs/ ~/Bureau/cybersec/scripts/

┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ ls -l
total 4
-rw-rw-r-- 1 judith judith 39 13 fév 14:54 README.md
```

5.scanner un reseau:

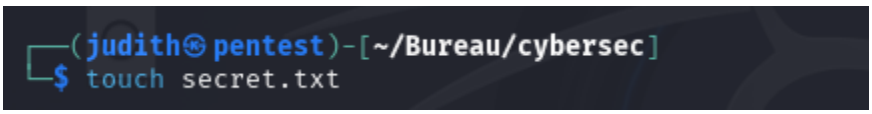
```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 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 08:00:27:78:09:b1 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 82708sec preferred_lft 82708sec
    inet6 fe80::a00:27ff:fe78:9b1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Utilisation de nmap pour scanner notre reseau local et l'identification des appareils connectes.



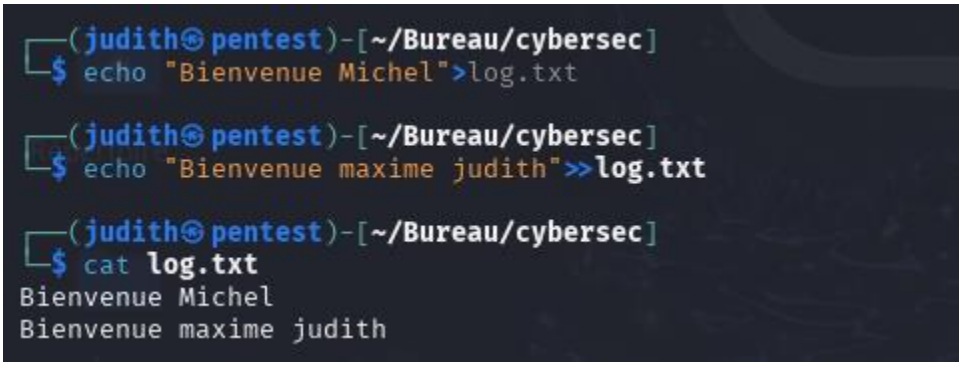
6- Manipulation des pernissions:

Creation du fichier secret.txt et changement de ses pernissions pour qu'il ne soit accessible qu'en lecture par le proprietaire.



7.Utilisation de grep:

Creation d'un fichier log.txt avec des lignes de texte, puis utilization grep pour rechercher un mot specifique.



8.Execution de ces commandes

Df -h

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                925M       0  925M   0% /dev
tmpfs               198M   1000K  197M   1% /run
/dev/sda1            19G     18G  114M 100% /
tmpfs               988M    4,0K  988M   1% /dev/shm
tmpfs               5,0M       0  5,0M   0% /run/lock
tmpfs               1,0M       0  1,0M   0% /run/credentials/systemd-journald.service
tmpfs               988M    8,0K  988M   1% /tmp
tmpfs               1,0M       0  1,0M   0% /run/credentials/getty@tty1.service
tmpfs               198M    116K  198M   1% /run/user/1000
```

Du –h

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ du -sh
200K    .
```

Free -h

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ free -h
               total        utilisé      libre     partagé tamp/cache   disponible
Mem:           1,9Gi        690Mi       984Mi        12Mi       450Mi       1,3Gi
Échange:       1,1Gi           0B       1,1Gi
```

Ps aux

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.4  0.6  22924 13956 ?        Ss   11:48   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    11:48   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    11:48   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   11:48   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   11:48   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   11:48   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   11:48   0:00 [kworker/R-netns]
root           9  0.2  0.0      0     0 ?        I    11:48   0:01 [kworker/0:1-events]
root          11  0.0  0.0      0     0 ?        I    11:48   0:00 [kworker/u4:0-events_unbound]
root          12  0.0  0.0      0     0 ?        I<   11:48   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    11:48   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    11:48   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    11:48   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    11:48   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    11:48   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    11:48   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          19  0.0  0.0      0     0 ?        S    11:48   0:00 [rcu_exp_gp_kthread_worker]
root          20  0.0  0.0      0     0 ?        S    11:48   0:00 [migration/0]
```

Lspci

```
┌──(judith㉿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)
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) USB2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)
```

Sudo apt install traceroute

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ sudo apt install traceroute
[sudo] Mot de passe de judith :
Désolé, essayez de nouveau.
[sudo] Mot de passe de judith :
Désolé, essayez de nouveau.
[sudo] Mot de passe de judith :
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  libconfig9           libgles1                   libhdf5-hl-100t64           libpaper1
  libbfio1           libdirectfb-1.7-7t64 libglvnd-core-dev          libjxl0.9                   libqt5×11extr
  libc++1-19         libegl-dev           libglvnd-dev               libmagickcore-6.q16-7-extra libsuperlu6
  libc++abi1-19      libfmt9              libgtksourceview-3.0-1     libmagickcore-6.q16-7t64    libtag1v5
  libcapstone4       libgl1-mesa-dev      libgtksourceview-3.0-common libmagickwand-6.q16-7t64   libtag1v5-van
  libconfig++9v5     libgles-dev          libgtksourceviewmm-3.0-0v5 libmbedcrypto7t64           libtagc0
Veuillez utiliser « sudo apt autoremove » pour les supprimer.

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

Traceroute google.com

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ traceroute google.com
traceroute to google.com (142.250.189.142), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  10.291 ms  9.573 ms  8.957 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
```

Netstat –tuln

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

Ss –tuln

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

Journalctl

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl
fév 07 13:21:02 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.
fév 07 13:21:02 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=7d4e6929-1dfd-46e7-b
fév 07 13:21:02 pentest kernel: BIOS-provided physical RAM map:
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x000000007fefffff] usable
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x000000007fff0000-0x000000007fffffff] ACPI data
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
fév 07 13:21:02 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
fév 07 13:21:02 pentest kernel: NX (Execute Disable) protection: active
fév 07 13:21:02 pentest kernel: APIC: Static calls initialized
fév 07 13:21:02 pentest kernel: SMBIOS 2.5 present.
fév 07 13:21:02 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
fév 07 13:21:02 pentest kernel: DMI: Memory slots populated: 0/0
fév 07 13:21:02 pentest kernel: Hypervisor detected: KVM
fév 07 13:21:02 pentest kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
fév 07 13:21:02 pentest kernel: kvm-clock: using sched offset of 3611360266582 cycles
```

Journalctl –f

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -f
fév 14 11:59:22 pentest sudo[5341]:   judith : TTY=pts/0 ; PWD=/home/judith/Bureau/cybersec ; USER=root ; COMMAND=
fév 14 11:59:22 pentest sudo[5341]: pam_unix(sudo:session): session opened for user root(uid=0) by judith(uid=1000
fév 14 11:59:24 pentest sudo[5341]: pam_unix(sudo:session): session closed for user root
fév 14 12:03:19 pentest systemd[1]: Starting systemd-tmpfiles-clean.service - Cleanup of Temporary Directories ...
fév 14 12:03:20 pentest systemd-tmpfiles[8387]: /usr/lib/tmpfiles.d/legacy.conf:14: Duplicate line for path "/run/
fév 14 12:03:20 pentest systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
fév 14 12:03:20 pentest systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories.
fév 14 12:05:01 pentest CRON[9232]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 14 12:05:01 pentest CRON[9234]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 14 12:05:01 pentest CRON[9232]: pam_unix(cron:session): session closed for user root
```

Journalctl –b

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -b
fév 14 11:48:13 pentest kernel: Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.
fév 14 11:48:13 pentest kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.2-amd64 root=UUID=7d4e6929-1dfd-46e7-b
fév 14 11:48:13 pentest kernel: BIOS-provided physical RAM map:
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x0000000000100000-0x000000007ffeffff] usable
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x000000007fff0000-0x000000007fffffff] ACPI data
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
fév 14 11:48:13 pentest kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
fév 14 11:48:13 pentest kernel: NX (Execute Disable) protection: active
fév 14 11:48:13 pentest kernel: APIC: Static calls initialized
fév 14 11:48:13 pentest kernel: SMBIOS 2.5 present.
fév 14 11:48:13 pentest kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
fév 14 11:48:13 pentest kernel: DMI: Memory slots populated: 0/0
fév 14 11:48:13 pentest kernel: Hypervisor detected: KVM
fév 14 11:48:13 pentest kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
```

Journalctl –n 10

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ journalctl -n 10
fév 14 12:03:20 pentest systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories.
fév 14 12:05:01 pentest CRON[9232]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 14 12:05:01 pentest CRON[9234]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
fév 14 12:05:01 pentest CRON[9232]: pam_unix(cron:session): session closed for user root
fév 14 12:09:01 pentest CRON[11167]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
fév 14 12:09:01 pentest CRON[11169]: (root) CMD (   [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/syst
fév 14 12:09:01 pentest CRON[11167]: pam_unix(cron:session): session closed for user root
fév 14 12:09:46 pentest systemd[1]: Starting phpsessionclean.service - Clean php session files...
fév 14 12:09:46 pentest systemd[1]: phpsessionclean.service: Deactivated successfully.
fév 14 12:09:46 pentest systemd[1]: Finished phpsessionclean.service - Clean php session files.
```

Date

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ date
ven 14 fév 2025 12:10:42 EST
```

timedatectl

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ timedatectl
               Local time: ven 2025-02-14 12:11:13 EST
           Universal time: ven 2025-02-14 17:11:13 UTC
                 RTC time: ven 2025-02-14 17:11:12
                Time zone: America/Port-au-Prince (EST, -0500)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

Hostnamectl

```
┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ hostnamectl
 Static hostname: pentest
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 4bc3aa5a65e045d0bce247ff88700c64
         Boot ID: f576f415d7f94ea1b806a816caea6338
  Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.11.2-amd64
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox
Firmware Version: VirtualBox
   Firmware Date: Fri 2006-12-01
    Firmware Age: 18y 2month 2w 1d
```

Sudo hostnamectl set-hostname wendell

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

┌──(judith㉿pentest)-[~/Bureau/cybersec]
└─$ hostnamectl
 Static hostname: wendell
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 4bc3aa5a65e045d0bce247ff88700c64
         Boot ID: f576f415d7f94ea1b806a816caea6338
  Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.11.2-amd64
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox
Firmware Version: VirtualBox
   Firmware Date: Fri 2006-12-01
    Firmware Age: 18y 2month 2w 1d
```

Les conclusions sur la tache accomplice.

4.pour conclure ce devoir me permet d’apprehender mieux l apprentissage du cours de securite informatique et surtout cela me mettre en chemin avec le linux ,c est par rapport avec ce devoir que j’ai decouvert ou je suis avec linux, bonne continutee professeur et merci beaucoup.