

Universite de la technologie D Haiti

UNITECH

Nom :

Nozard

Prenom :

Placide

Prof : Ismael Saint Amour

Niveau : III

le 15/02/2025

Objectif :

ce Td est conçu pour permettre la virtualisation de kali linux et l'apprentissage des premières commandes est de vous familiariser avec l'environnement kali linux

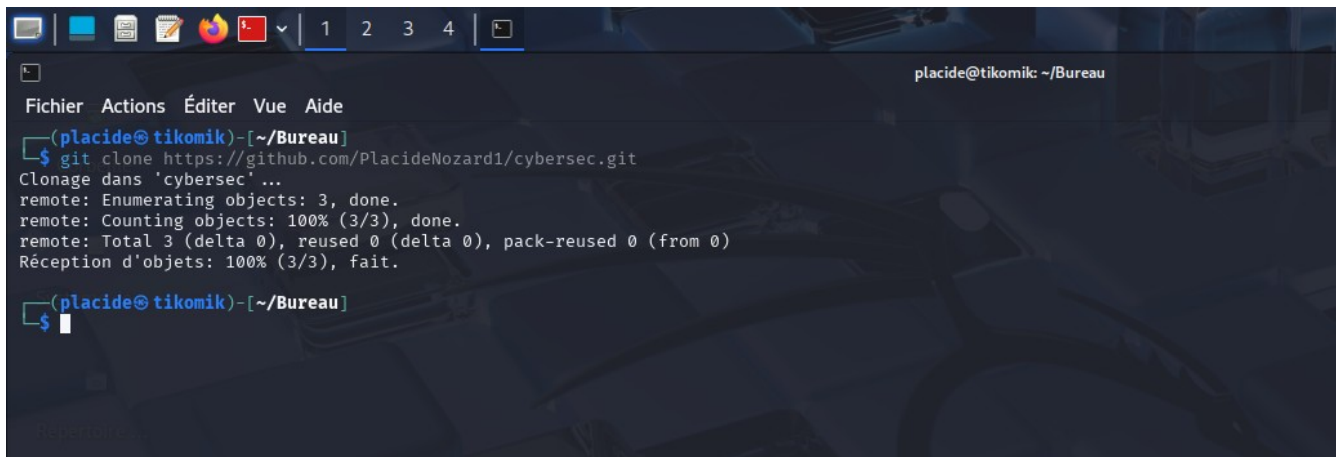
1. Apprendre les bases de kali linux

2. apprendre les commandes de bases pour naviger dans le système de fichiers

3. mettre à jour et configurer kali linux pour des tâches de cybersécurité

Étapes du TD

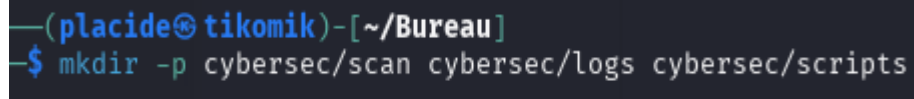
Pour cloner un dépôt git dans un dossier

A screenshot of a terminal window with a dark background. The window title is "placide@tikomik: ~/Bureau". The terminal shows the command `git clone https://github.com/PlacideNozard1/cybersec.git` being executed. The output shows the progress of cloning the repository, including enumerating and counting objects. The prompt `(placide@tikomik)-[~/Bureau]` is visible at the top of the terminal.

```
(placide@tikomik)-[~/Bureau]
$ git clone https://github.com/PlacideNozard1/cybersec.git
Clonage dans 'cybersec' ...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Réception d'objets: 100% (3/3), fait.

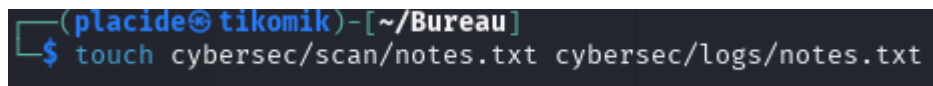
(placide@tikomik)-[~/Bureau]
$
```

pour créer un dossier

A terminal snippet showing the command `mkdir -p cybersec/scan cybersec/logs cybersec/scripts` being executed. The prompt `(placide@tikomik)-[~/Bureau]` is visible.

```
(placide@tikomik)-[~/Bureau]
$ mkdir -p cybersec/scan cybersec/logs cybersec/scripts
```

pour créer un dossier vide

A terminal snippet showing the command `touch cybersec/scan/notes.txt cybersec/logs/notes.txt` being executed. The prompt `(placide@tikomik)-[~/Bureau]` is visible.

```
(placide@tikomik)-[~/Bureau]
$ touch cybersec/scan/notes.txt cybersec/logs/notes.txt
```

pour ecrire un text dans un fichier

```
(placide@tikomik)-[~/Bureau]
$ echo "c'est mon fichier dans scan" > cybersec/scan/notes.txt

(placide@tikomik)-[~/Bureau]
$ echo "c'est mon fichier dans logs" > cybersec/logs/notes.txt
```

pour créer ou concatener des fichiers

```
(placide@tikomik)-[~/Bureau]
$ cat cybersec/scan/notes.txt
c'est mon fichier dans scan

(placide@tikomik)-[~/Bureau]
$ cat cybersec/logs/notes.txt
c'est mon fichier dans logs
```

pour copier des fichiers

```
(placide@tikomik)-[~/Bureau]
$ cp cybersec/scan/notes.txt cybersec/scripts
```

pour lister les fichiers

```
(placide@tikomik)-[~/Bureau]
$ ls cybersec/scripts
notes.txt
```

pour de deplaser des fichiers

```
(placide@tikomik)-[~/Bureau]
$ mv cybersec/scripts/notes.txt cybersec/scan
```

afficher la liste et repertoire dans le dossier scripts

```
(placide@tikomik)-[~/Bureau]
$ ls cybersec/scripts
```

pour supprimer des repertoires

```
(placide@tikomik)-[~/Bureau]
$ rm -r cybersec/scan cybersec/logs cybersec/scripts
```

liste des fichiers

```
(placide@tikomik)-[~/Bureau]
$ ls cybersec
README.md
```

afficher les informations relatives aux adresse ip

```
(placide@tikomik)-[~/Bureau]
$ 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 08:00:27:1c:26:24 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 81095sec preferred_lft 81095sec
    inet6 fd00::ebb5:f7c3:429b:6c1c/64 scope global temporary dynamic
        valid_lft 86232sec preferred_lft 14232sec
    inet6 fd00::a00:27ff:fe1c:2624/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86232sec preferred_lft 14232sec
    inet6 fe80::a00:27ff:fe1c:2624/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

pour scan de decouverte des hotes sur un reseaux

```
(placide@tikomik)-[~/Bureau]
$ nmap -sn 10.0.2.15/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 15:02 EST
Nmap scan report for 10.0.2.2
Host is up (0.00048s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00059s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.44 seconds
```

créer un fichier vide secret.txt

```
(placide@tikomik)-[~/Bureau]
$ touch secret.txt
```

modifie les permissions du fichier

```
(placide@tikomik)-[~/Bureau]
$ chmod 400 secret.txt
```

afficher les information detaillées

```
(placide@tikomik)-[~/Bureau]
$ ls -l secret.txt
-r----- 1 placide placide 0 15 fév 15:03 secret.txt
```

pour afficher espace disque utilise

```
(placide@tikomik)-[~/Bureau]
$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev                926M      0  926M   0% /dev
tmpfs               198M    1012K  197M   1% /run
/dev/sda1           38G      17G   19G  48% /
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    468K  987M   1% /tmp
tmpfs               1,0M      0    1,0M   0% /run/credentials/getty@tty1.service
tmpfs              198M    116K  198M   1% /run/user/1000
```

afficher la memoire

```
(placide@tikomik)-[~/Bureau]
$ free -h
               total        utilisé        libre       partagé  tamp/cache  disponible
Mem:           1,9Gi         1,3Gi         125Mi         46Mi         721Mi        617Mi
Échange:        2,0Gi         730Mi
```


liste de tout les processus

```
(placide@tikomik)-[~/Bureau]
$ ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root            1  0.7  0.5 23956 10672 ?        Ss   12:42   1:05 /sbin/init splash
root            2  0.0  0.0      0     0 ?        S    12:42   0:00 [kthreadd]
root            3  0.0  0.0      0     0 ?        S    12:42   0:00 [pool_workqueue_release]
root            4  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-rcu_gp]
root            5  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-sync_wq]
root            6  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-slub_flushwq]
root            7  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-netns]
root           12  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-mm_percpu_wq]
root           13  0.0  0.0      0     0 ?        I    12:42   0:00 [rcu_tasks_kthread]
root           14  0.0  0.0      0     0 ?        I    12:42   0:00 [rcu_tasks_rude_kthread]
root           15  0.0  0.0      0     0 ?        I    12:42   0:00 [rcu_tasks_trace_kthread]
root           16  0.1  0.0      0     0 ?        S    12:42   0:10 [ksoftirqd/0]
root           17  0.2  0.0      0     0 ?        I    12:42   0:19 [rcu_preempt]
root           18  0.0  0.0      0     0 ?        S    12:42   0:00 [rcu_exp_par_gp_kthread_worker/0]
root           19  0.0  0.0      0     0 ?        S    12:42   0:00 [rcu_exp_gp_kthread_worker]
root           20  0.0  0.0      0     0 ?        S    12:42   0:00 [migration/0]
root           21  0.0  0.0      0     0 ?        S    12:42   0:00 [idle_inject/0]
root           22  0.0  0.0      0     0 ?        S    12:42   0:00 [cpuhp/0]
root           24  0.0  0.0      0     0 ?        S    12:42   0:00 [kdevtmpfs]
root           25  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-inet_frag_wq]
root           27  0.0  0.0      0     0 ?        S    12:42   0:00 [kauditd]
root           28  0.0  0.0      0     0 ?        S    12:42   0:00 [khungtaskd]
root           29  0.0  0.0      0     0 ?        S    12:42   0:00 [oom_reaper]
root           31  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-writeback]
root           32  0.0  0.0      0     0 ?        S    12:42   0:06 [kcompactd0]
root           33  0.0  0.0      0     0 ?        SN   12:42   0:00 [ksmd]
root           34  0.0  0.0      0     0 ?        SN   12:42   0:01 [khugepaged]
root           35  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-kintegrityd]
root           36  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-kblockd]
root           37  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-blkcg_punt_bio]
root           38  0.0  0.0      0     0 ?        S    12:42   0:00 [irq/9-acpi]
root           39  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-tpm_dev_wq]
root           40  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-edac-poller]
root           41  0.0  0.0      0     0 ?        I<   12:42   0:00 [kworker/R-devfreq_wq]
root           42  0.0  0.0      0     0 ?        I<   12:42   0:01 [kworker/0:1H-kblockd]
root           43  0.1  0.0      0     0 ?        S    12:42   0:14 [kswapd0]
root           51  0.0  0.0      0     0 ?        I<   12:43   0:00 [kworker/R-kthrotld]
root           55  0.0  0.0      0     0 ?        I<   12:43   0:00 [kworker/R-acpi_thermal_pm]
```

afficher les informations sur le peripherique

```
(placide@tikomik)-[~/Bureau]
$ 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)
```

afficher des informations sur les connexions

```
(placide@tikomik)-[~/Bureau]
$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
udp 0 0 0.0.0.0:500 0.0.0.0:*
udp 0 0 10.0.2.15:3702 0.0.0.0:*
udp 0 0 239.255.255.250:3702 0.0.0.0:*
udp 0 0 0.0.0.0:35496 0.0.0.0:*
udp 0 0 0.0.0.0:48855 0.0.0.0:*
udp 0 0 0.0.0.0:4500 0.0.0.0:*
udp6 0 0 :::500 :::*
udp6 0 0 fe80::a00:27ff:fe1:3702 :::*
udp6 0 0 ff02::c:3702 :::*
udp6 0 0 :::35733 :::*
udp6 0 0 :::4500 :::*
```

afficher le nom hôte

```
(placide@tikomik)-[~]
$ hostnamectl
Static hostname: tikomik
Icon name: computer-vm
Chassis: vm
Machine ID: 741f76ffdd3b4731844f13ef60783ba2
Boot ID: ef5a0f9803864b109a296f4a8d683e7e
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 2d
```

n affiche aucune information

```
(placide@tikomik)-[~]
$ sudo hostnamectl set-hostname sumshine
[sudo] Mot de passe de placide :
Désolé, essayez de nouveau.
[sudo] Mot de passe de placide :

(placide@tikomik)-[~]
$ hostnamectl
Static hostname: sumshine
Icon name: computer-vm
Chassis: vm
Machine ID: 741f76ffdd3b4731844f13ef60783ba2
Boot ID: ef5a0f9803864b109a296f4a8d683e7e
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 2d
```

affiche et configurer le nom hôte

```
(placide@tikomik)-[~]
$ sudo hostnamectl set-hostname sumshine
[sudo] Mot de passe de placide :
Désolé, essayez de nouveau.
[sudo] Mot de passe de placide :
(placide@tikomik)-[~]
$ hostnamectl
Static hostname: sumshine
Icon name: computer-vm
Chassis: vm
Machine ID: 741f76ffdd3b4731844f13ef60783ba2
Boot ID: ef5a0f9803864b109a296f4a8d683e7e
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 2d
```

Conclusion

les commandes et outils que nous avons explorés offrent une grande flexibilité pour administrer et configurer un système Linux. Que ce soit pour la gestion des fichiers, la surveillance des ressources système, ou l'administration du réseau, chaque commande présente des fonctionnalités essentielles pour optimiser la gestion de l'ordinateur et la résolution des problèmes techniques.