**UNIVERSITÉ DE TECHNOLOGIE D’HAITI  
Faculté des Sciences de Genie Civil et d’achitecture  
Science informatique**

Sujet: Création d’une nouvelle machine virtuelle dans virtualBox

Créer un nouveau dépôt : TD

Preparer par: Djenou LACOMBE

Soumis au prof: Ismael SAINT AMOUR

Dans le cadre du cours de cyber sécurité

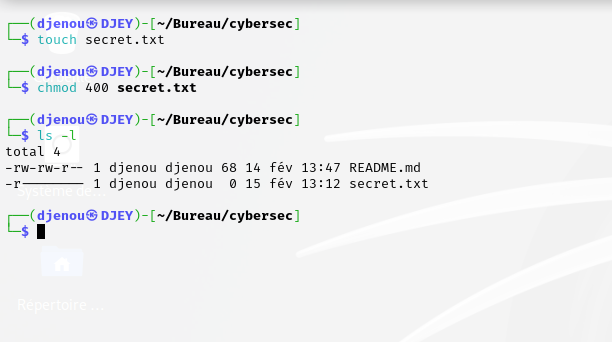
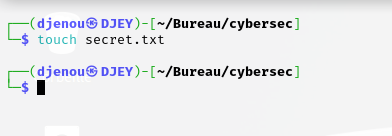
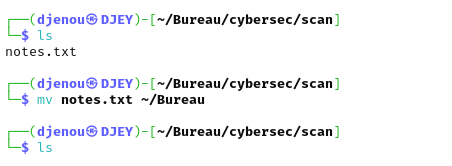
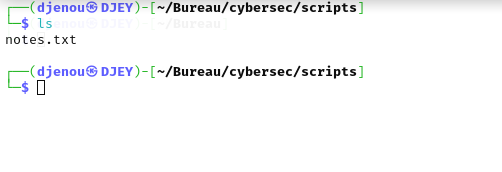
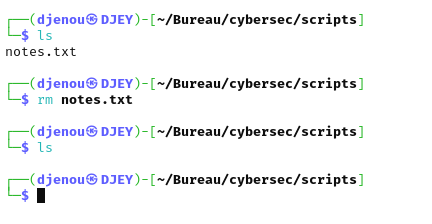
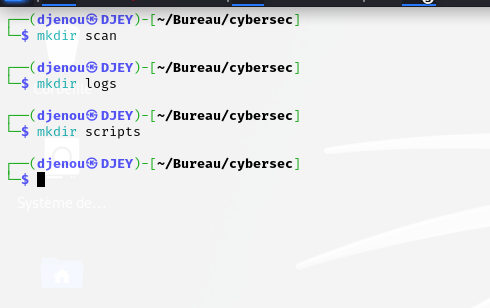
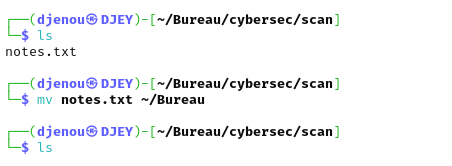
16 Fevrier 2025

**Étapes réalisée :**

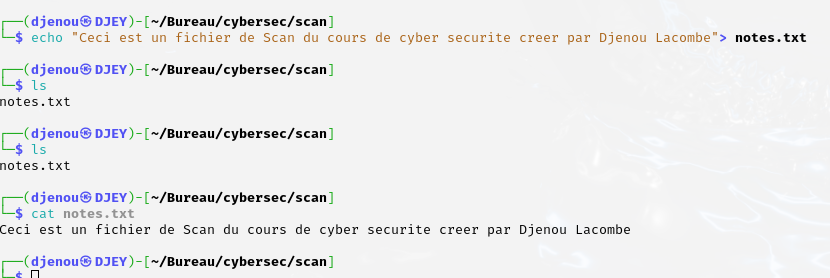
Créez un dossier cybersec avec trois sous-dossiers : scan , logs , script

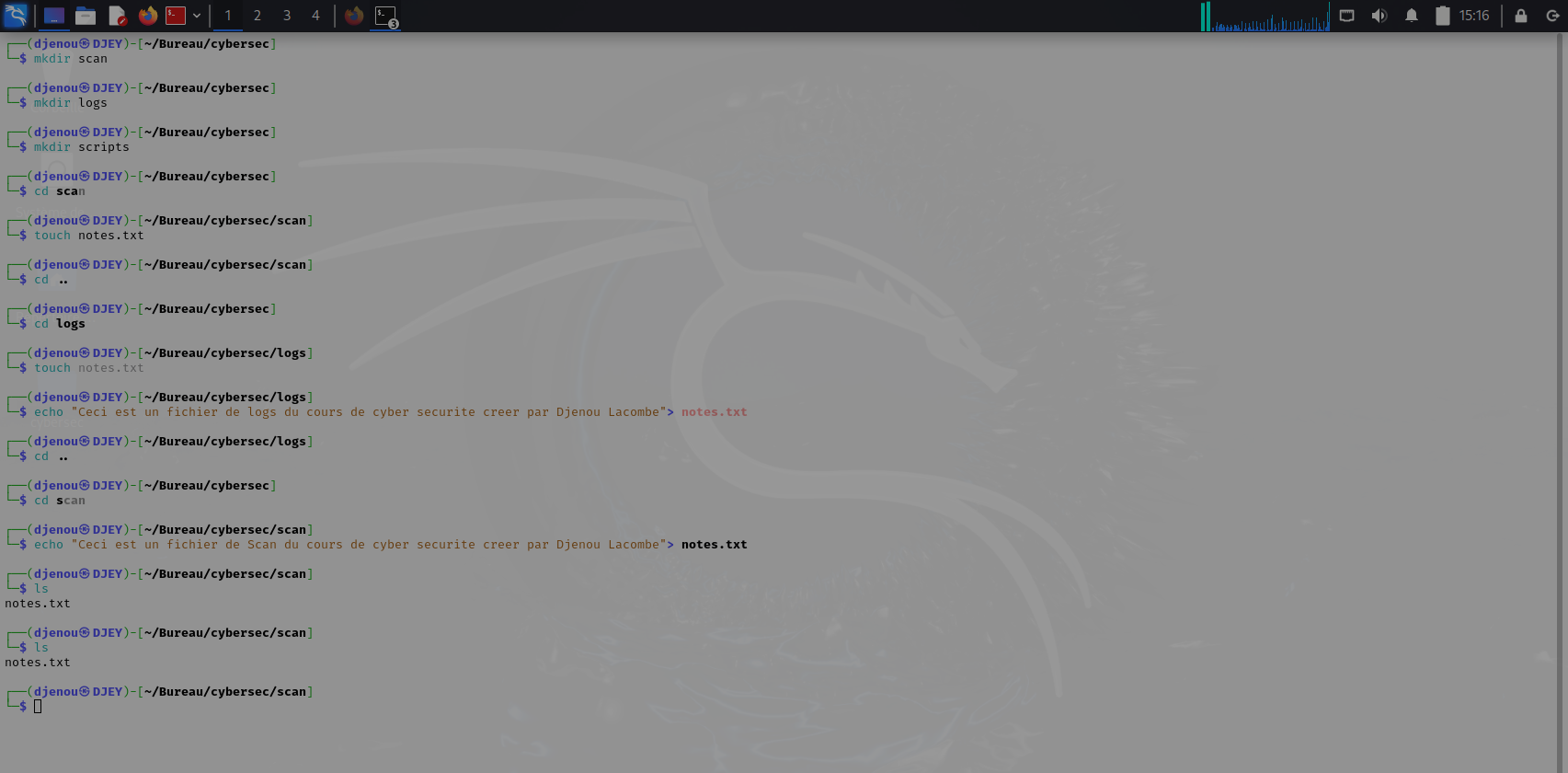
Après avoir installé kali linux sur une machine virtuelle avec virtualBox ou VMware, je commence par mettre à jour le système pour assurer son bon fonctionnement.

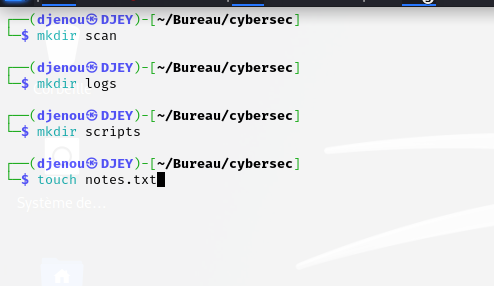
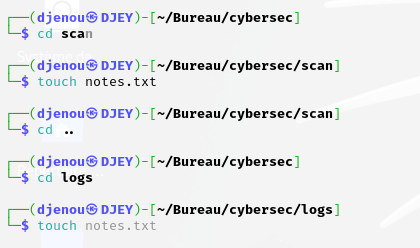
Ensuite, je crée une structure de dossiers organisée avec un repertoire cybersec contenant trois (3) sous-dossiers: scan, logs, scripts.



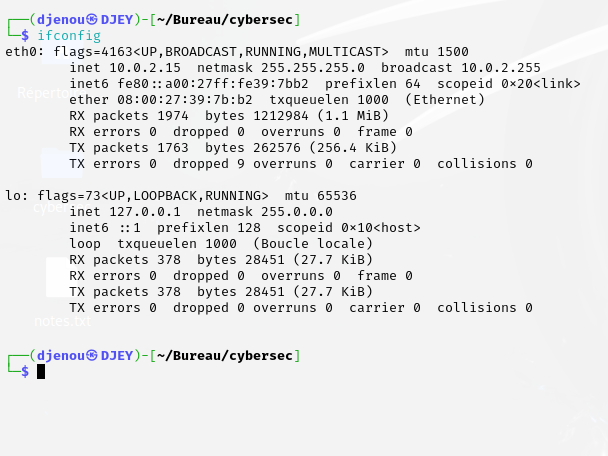
1. J’ajoute des fichiers texte, y insère du contenu, puis je les manipule en les copiant, déplacant et supprimant tout en verifiant chaque étape.







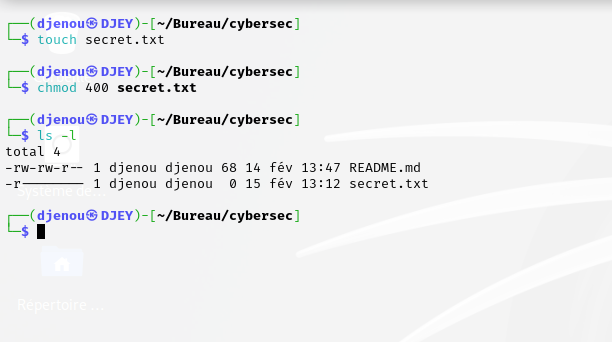
5. Scanner un réseau : ifconfig ou ip a : Affiche les informations réseau. Utilisez nmap pour scanner votre réseau local et identifier les appareils connectés. grep "motif" fichier.txt cat fichier.txt echo "Bonjour" > fichier.txt ps aux kill PID # Remplacez PID par l'ID du processus

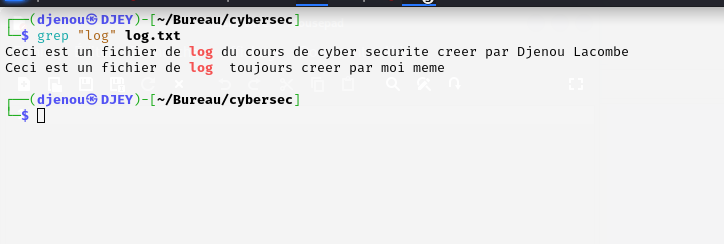


Utilisez nmap pour scanner votre réseau local et identifier les appareils connectés.



6. Manipuler les permissions : Créez un fichier secret.txt et changez ses permissions pour qu'il ne soit accessible qu'en lecture par le propriétaire.

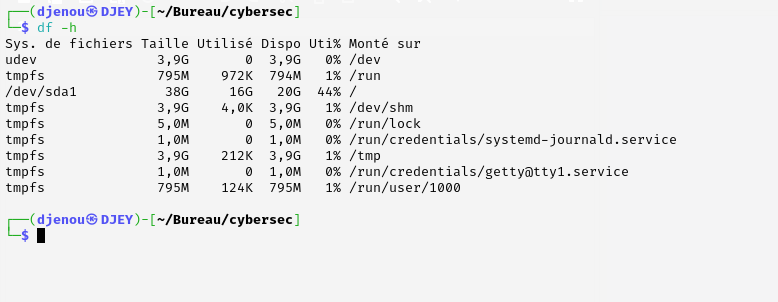


7. Utiliser grep : Créez un fichier log.txt avec des lignes de texte, puis utilisez grep pour rechercher un mot spécifique. 



j’explore les fonctionnalités de réseau en affichant les informations de connexion et en utilisant nmap pour la scanner mon reseau local et identifier les appareils conectés.

La commande **df -h** permet d'afficher l'espace disque disponible et utilisé sur les différentes partitions du système, avec une présentation en **format lisible par l'humain** (h pour "human-readable"



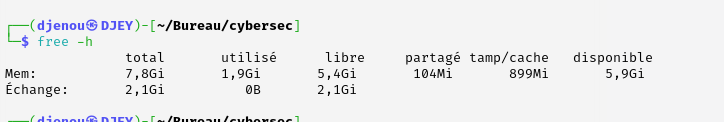
**du -sh : Afficher la taille d’un dossier ou fichier**

La commande **du -sh** permet de connaître **l’espace disque occupé** par un dossier ou un fichier, avec une taille **lisible par l’humain**.



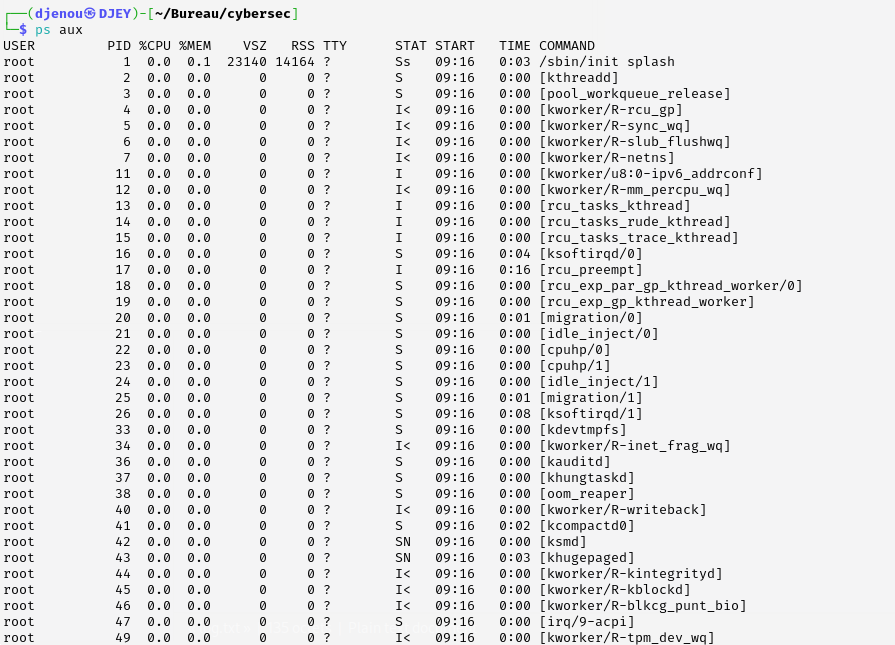
### free -h : Afficher l'utilisation de la mémoire (RAM)

La commande **free -h** permet de voir la mémoire **RAM** et l'espace **swap** utilisés et disponibles, en format **lisible par l'humain** (**Go, Mo, Ko**).



### ps aux : Afficher tous les processus en cours

La commande **ps aux** permet de **lister tous les processus** qui s'exécutent sur le système, avec des détails comme l'utilisateur, l'utilisation de la mémoire et du CPU, et la commande lancée.



### lspci : Afficher les périphériques PCI du système

La commande **lspci** permet de **lister tous les périphériques PCI** (Peripheral Component Interconnect) connectés à l’ordinateur, comme la carte graphique, la carte réseau, le contrôleur USB,



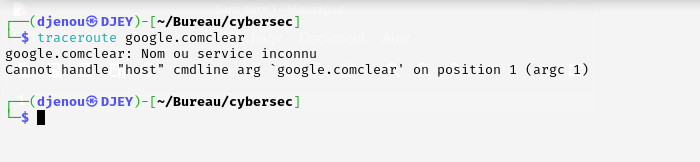
### sudo apt install traceroute : Installer l'outil traceroute sous Linux

La commande **sudo apt install traceroute** permet d'installer **l'outil traceroute** sur un système basé sur **Debian** (comme **Kali Linux, Ubuntu, Debian**).



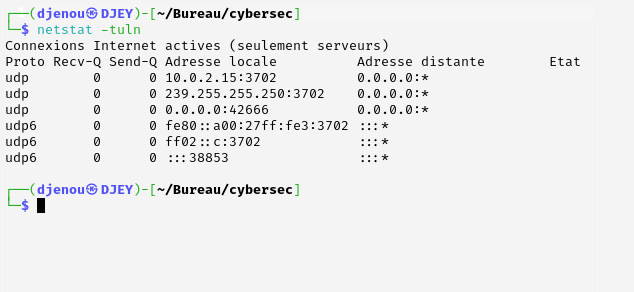
### traceroute google.com : Analyse du chemin emprunté par les paquets réseau

La commande **traceroute google.com** permet de déterminer **l’itinéraire suivi par les paquets** envoyés depuis l’ordinateur local jusqu’au serveur **Google**. Elle identifie **chaque routeur intermédiaire** traversé, ainsi que **le temps nécessaire** pour atteindre chaque point du réseau.



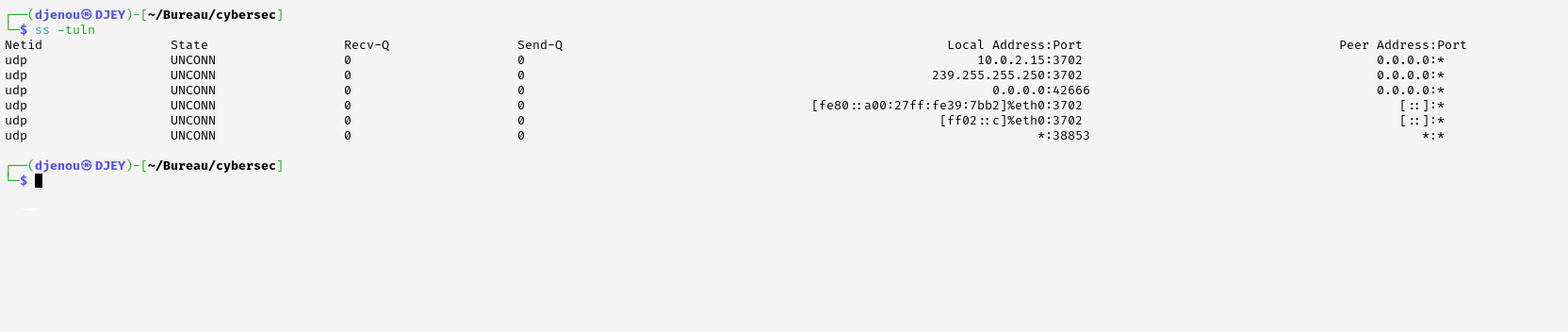
### netstat -tuln : Affichage des ports ouverts et des services en écoute

La commande **netstat -tuln** permet d’afficher **les ports réseau en écoute** sur un système ainsi que les services associés. Elle est particulièrement utile pour **analyser la sécurité d’un serveur** et vérifier les connexions entrantes potentielles.



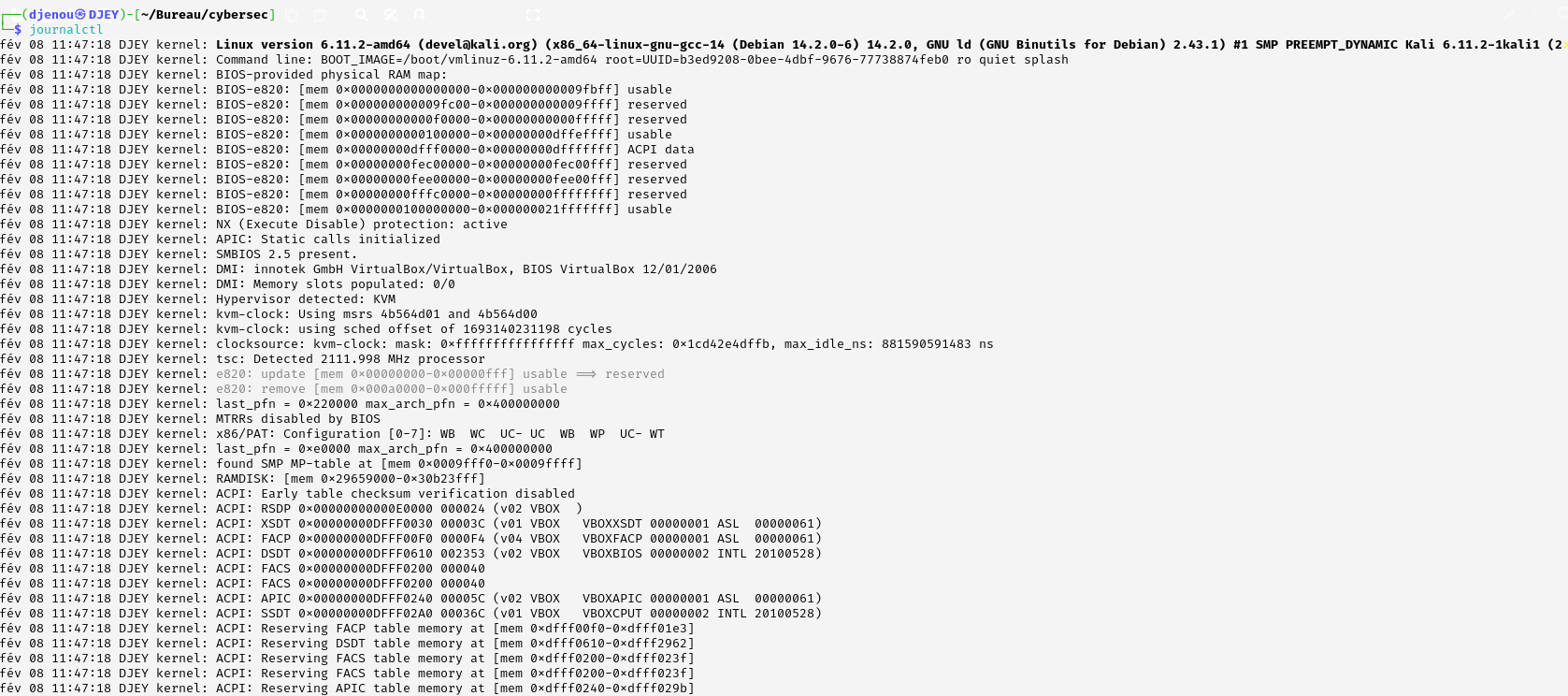
### ss -tuln : Affichage des ports ouverts et des services en écoute

La commande **ss -tuln** est une alternative moderne à netstat -tuln. Elle permet d’afficher **les ports en écoute** sur un système ainsi que les services qui les utilisent. Elle est **plus rapide et plus efficace** que netstat, car elle interroge directement les structures de données du noyau Linux.



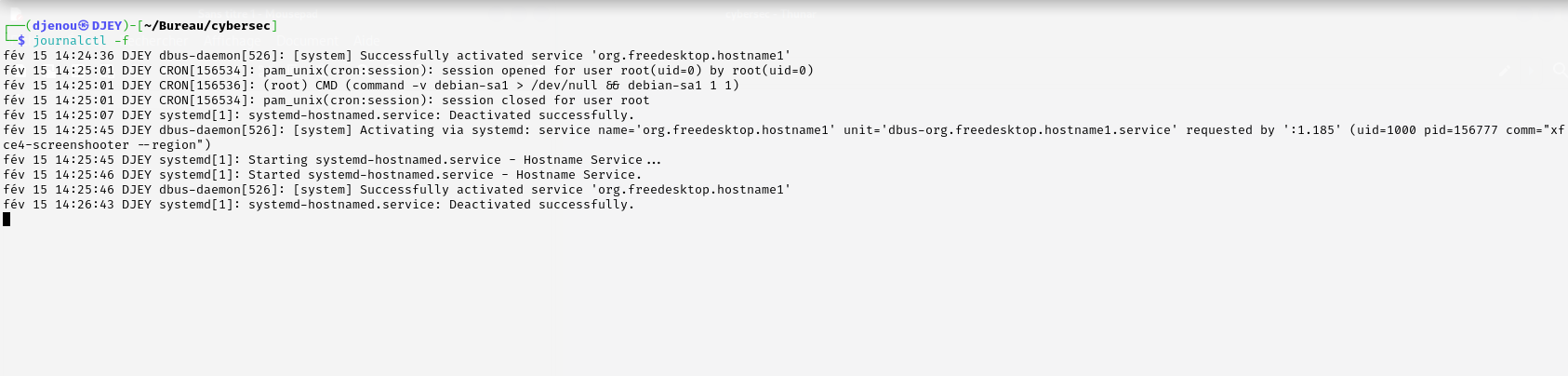
### journalctl : Afficher les journaux système sous Linux

La commande **journalctl** permet d’afficher les **journaux du système** sur les distributions Linux qui utilisent **systemd** comme système d'init. Elle permet de consulter, filtrer et analyser les **logs système**, les événements du noyau, les messages des services et des applications.



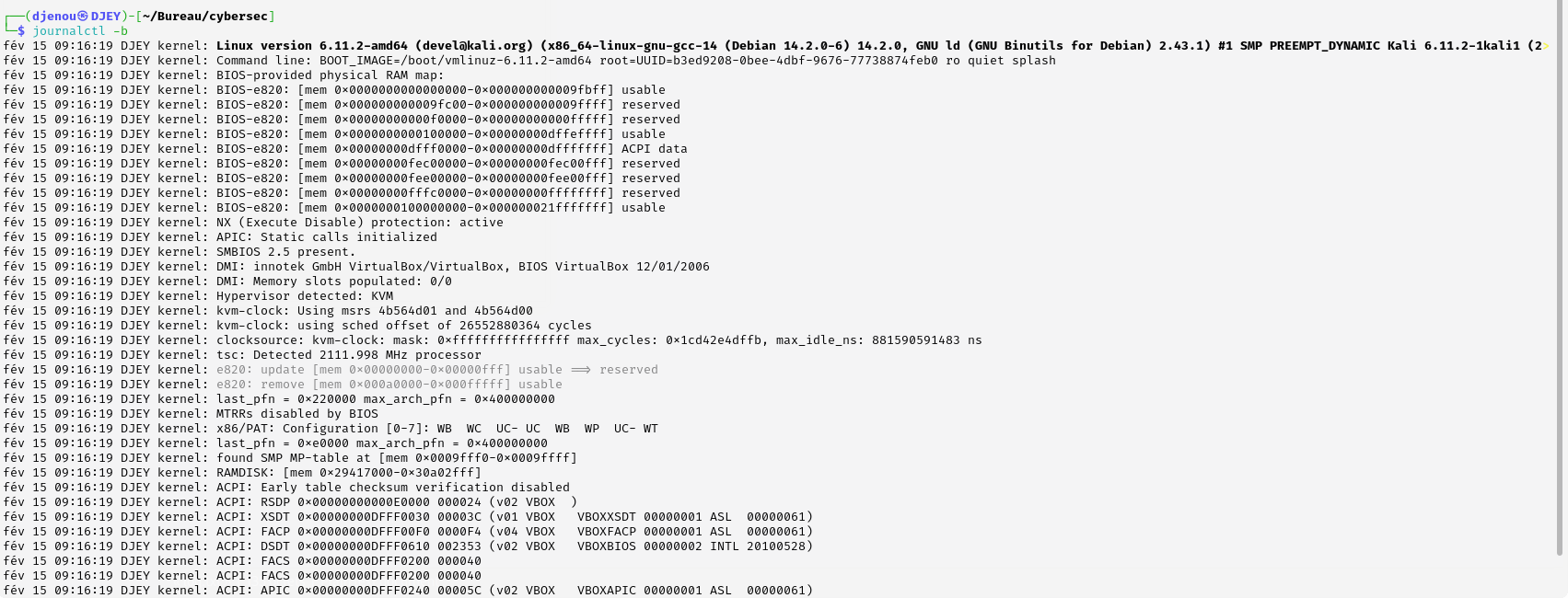
### journalctl -f : Suivi en temps réel des journaux système

La commande **journalctl -f** permet de suivre les journaux système en **temps réel**. Cela équivaut à utiliser la commande **tail -f** sur un fichier de logs, mais elle s'applique directement aux logs collectés par **systemd**. Cette commande est particulièrement utile pour **observer l’activité** du système pendant qu'il se déroule.



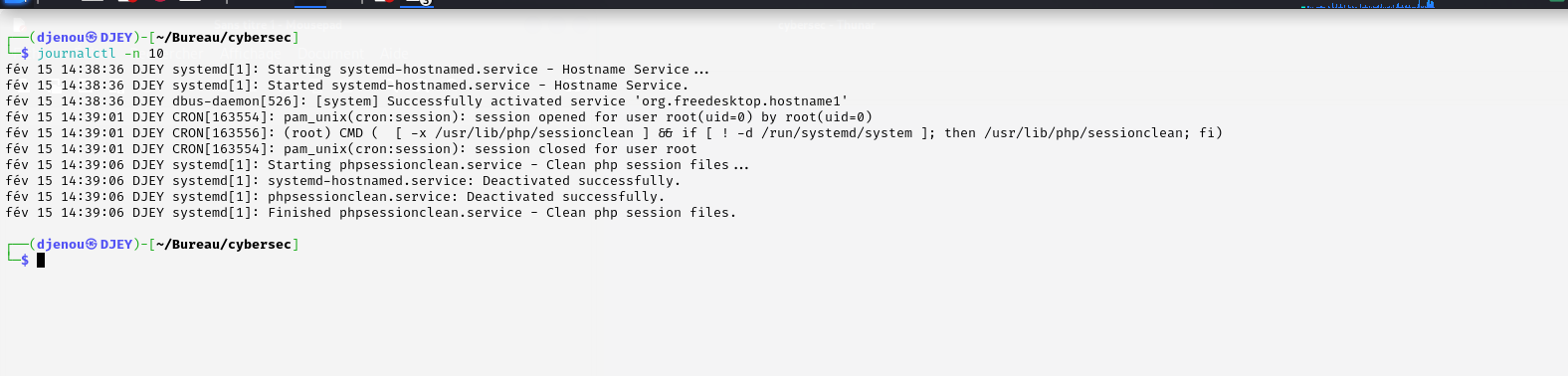
### journalctl -b : Afficher les journaux du démarrage actuel

La commande **journalctl -b** permet d'afficher les journaux du système **depuis le dernier démarrage**. Cela inclut tous les messages générés par **systemd**, les services, le noyau et d'autres applications depuis le dernier démarrage de la machine.



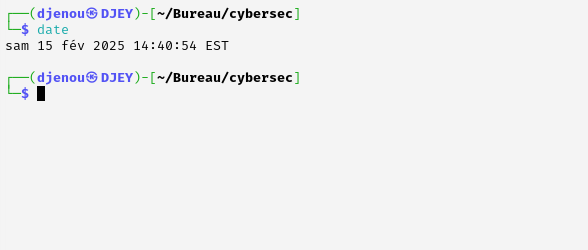
### journalctl -n 10 : Afficher les 10 derniers journaux

La commande **journalctl -n 10** permet d'afficher les **10 derniers journaux** enregistrés par **systemd**. Elle est utile pour obtenir rapidement un aperçu des dernières entrées dans les journaux système sans avoir à faire défiler tout l'historique des logs.



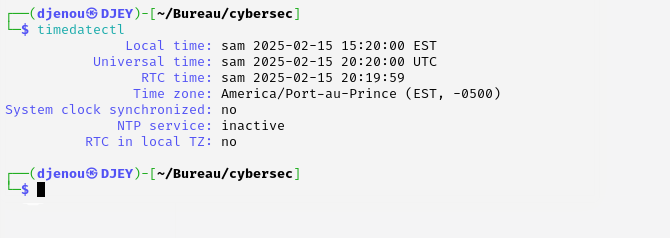
### date : Afficher ou définir la date et l'heure du système

La commande **date** permet d'afficher la **date et l'heure actuelles** du système. Elle peut également être utilisée pour **modifier la date et l'heure** du système si l'utilisateur dispose des privilèges nécessaires.



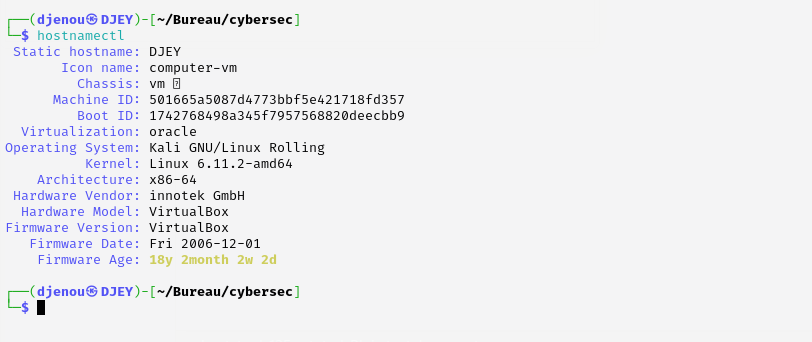
### timedatectl : Gérer la date, l'heure et le fuseau horaire du système

La commande **timedatectl** est utilisée pour afficher et modifier la **date, l'heure**, et le **fuseau horaire** sur les systèmes Linux qui utilisent **systemd**. Elle permet de configurer le temps système de manière centralisée

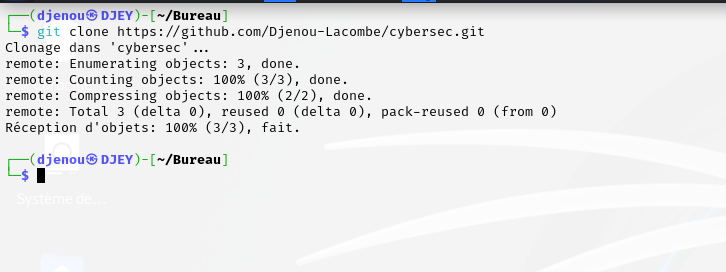
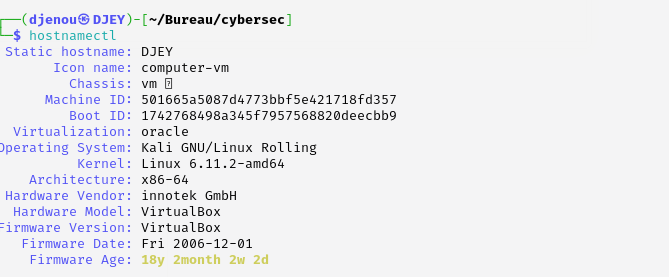


### hostnamectl : Gérer le nom d'hôte du système

La commande **hostnamectl** est utilisée pour afficher et modifier le **nom d'hôte** (hostname) d'un système Linux. Elle permet également de gérer certains paramètres liés au système, comme le **système d'exploitation**, le **type de machine**, et d'autres informations liées au réseau.



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



Ce travail me permet de me famliariser avec les comandes de gestion des fichier sous linux, ainsi qu’avec les outils de base en cybersécurité, essentiel pour les comprend l’arninistration systéme et annalyse réseau.

Au terme de cette série de tâches, plusieurs étapes clés ont été réalisées pour configurer et gérer un environnement Kali Linux. Voici les principaux points à retenir :

1. **Installation et configuration initiale de Kali Linux** :
   * Kali Linux a été installé avec succès, et le système a été mis à jour pour garantir une version à jour et fonctionnelle.
2. **Gestion des fichiers et des répertoires** :
   * Une structure de répertoires a été créée avec des sous-dossiers et des fichiers texte. Cela a permis de tester les commandes de gestion des fichiers, telles que la copie, le déplacement et la suppression.
   * L'organisation des fichiers a été suivie, et des vérifications ont été effectuées pour confirmer que les actions ont été réalisées correctement.
3. **Exploration des commandes réseau** :
   * Des commandes comme **nmap**, **ifconfig**, et **traceroute** ont été utilisées pour explorer le réseau, détecter les appareils connectés, et diagnostiquer la connectivité réseau.
   * Cela a permis de mieux comprendre la gestion réseau sous Linux, ce qui est essentiel dans un environnement de cybersécurité.
4. **Gestion du temps et du fuseau horaire** :
   * Des outils comme **timedatectl** et **hostnamectl** ont été utilisés pour configurer l'heure système et le nom d'hôte de la machine. Cela est crucial pour assurer la synchronisation correcte des systèmes et une gestion optimale des ressources.
5. **Apprentissage pratique et développement des compétences** :
   * La manipulation des commandes en ligne de commande sous Linux a renforcé la compréhension de la gestion des systèmes, notamment dans un environnement sécurisé et contrôlé comme Kali Linux.
   * L'exécution de ces tâches a permis de mieux appréhender les outils de gestion du système et des réseaux, essentiels pour toute personne travaillant dans le domaine de la cybersécurité.

En somme, cette tâche a permis non seulement de se familiariser avec l'environnement Kali Linux, mais aussi d'acquérir des compétences pratiques dans la gestion des fichiers, la configuration du système et l'analyse réseau. Ces compétences sont fondamentales pour tout travail en cybersécurité et en administration système.