Universite De Technologie D’haiti

(UNITECH)

**Faculte des sciences et Genies d’architectures**

**Matiere :** Cybersecurite

**Nom :** EXILIEN

**Prenom :** Wedson

**Professeur :** Ismael SAINT AMOUR

**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, de comprendre les bases de la virtualisation, et de maîtriser les commandes essentielles pour naviguer et interagir avec un système Linux.

Description des résultats de la tâche :

Création de la machine virtuelle et installation de Kali Linux :

Une nouvelle machine virtuelle a été configurée et Kali Linux a été installé avec succès via l’interface graphique.

Le système est pleinement fonctionnel après un redémarrage, prêt pour l'exécution des tâches.

Mise à jour du système :

La commande sudo apt update && sudo apt upgrade -y a permis de mettre à jour les paquets du système vers leurs dernières versions, garantissant ainsi la sécurité et la stabilité.

Création de la structure de dossiers :

Le dossier principal cybersec a été créé avec trois sous-dossiers : scan, logs, et scripts.

Deux fichiers notes.txt ont été créés dans les sous-dossiers scan et logs avec du contenu spécifique ajouté.

Le contenu des fichiers a été affiché avec succès, confirmant l'exactitude des informations.

Le fichier notes.txt a été copié correctement du dossier scan vers scripts, puis déplacé dans scan après vérification.

La suppression du fichier notes.txt dans scripts a été validée, montrant qu'il n'existe plus.

Enfin, les trois sous-dossiers ont été supprimés avec succès, confirmant un nettoyage complet de la structure.

Scan du réseau :

Les informations réseau locales ont été récupérées via ifconfig ou ip a, fournissant les adresses IP et les interfaces réseau.

Le scan du réseau local à l’aide de nmap a permis d’identifier les appareils connectés et d’afficher leurs adresses IP, les ports ouverts, et d'autres informations utiles.

Manipulation de fichiers et gestion des processus :

Les commandes grep, cat et echo ont permis de manipuler et d’afficher le contenu des fichiers.

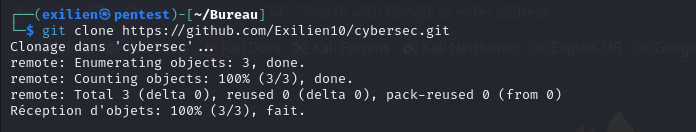
La liste des processus en cours a été affichée avec ps aux, et un processus spécifique a pu être terminé à l’aide de la commande kill.

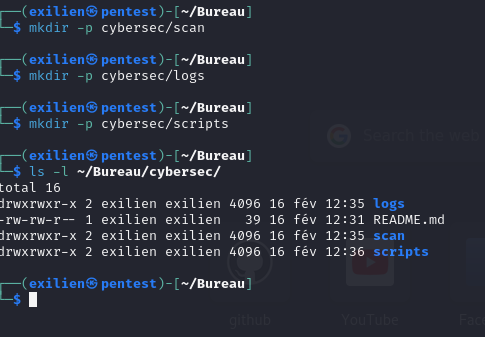
Gestion des permissions :

Un fichier secret.txt a été créé et ses permissions ont été modifiées pour être uniquement lisibles par le propriétaire (chmod 400).

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

Ajoutez un fichier notes.txt dans scan et logs .

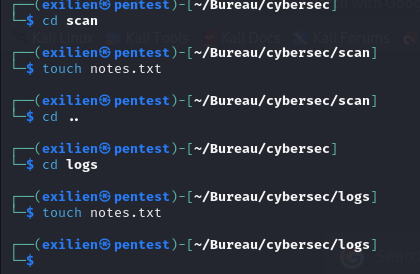




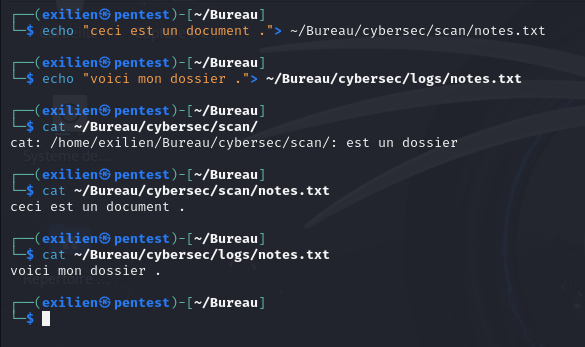
Ajoutez du contenu dans les fichiers textes ( notes.txt), puis affichez le contenu des fichiers.

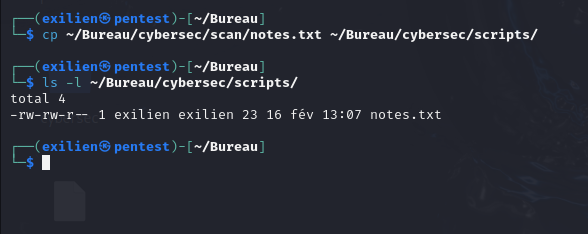
Copiez le fichier (notes.txt) dans le sous-dossier scripts .

vérifier si le fichiers a été copié.



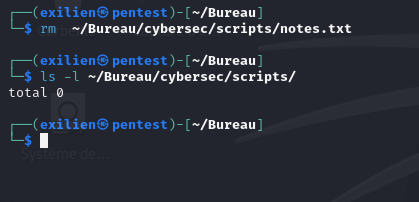
Déplacez le fichier (notes.txt) dans le sous-dossier scan .





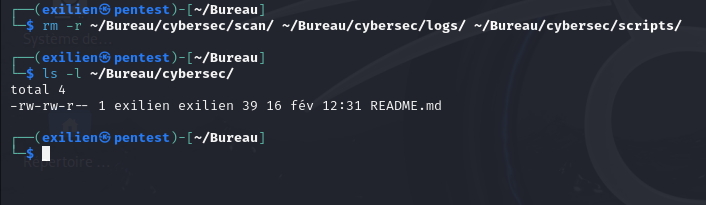
Supprimez le fichier (notes.txt)dans le sous-dossier scripts .

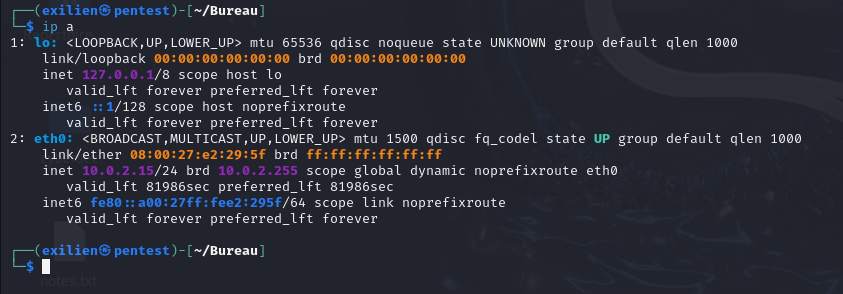
vérifier si le fichiers a été supprimé.

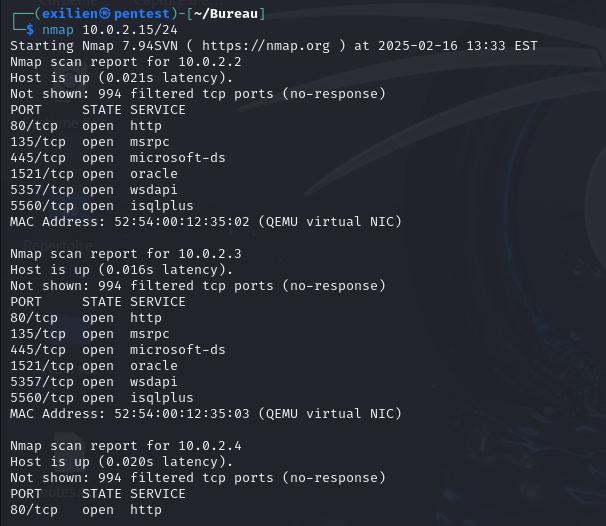


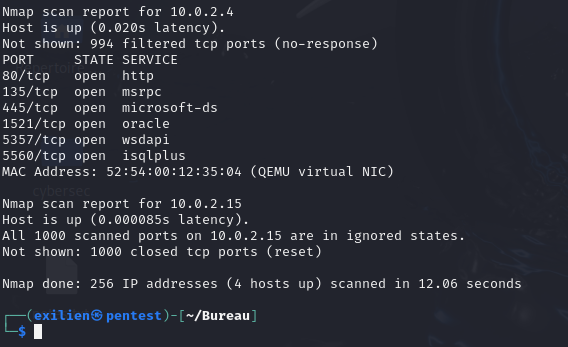
Supprimez les sous-dossiers : scan , logs , scripts.

vérifier si les sous-dossiers ont été supprimés.

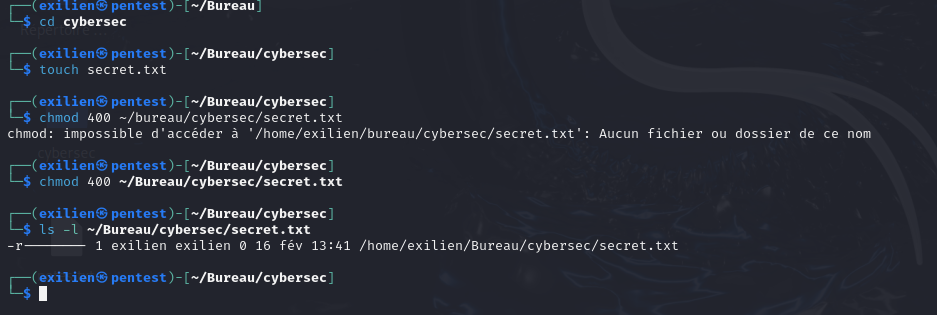


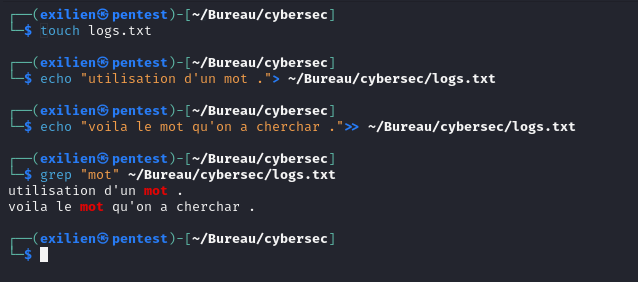
ifconfig ou ip a : Affiche les informations réseau. 

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



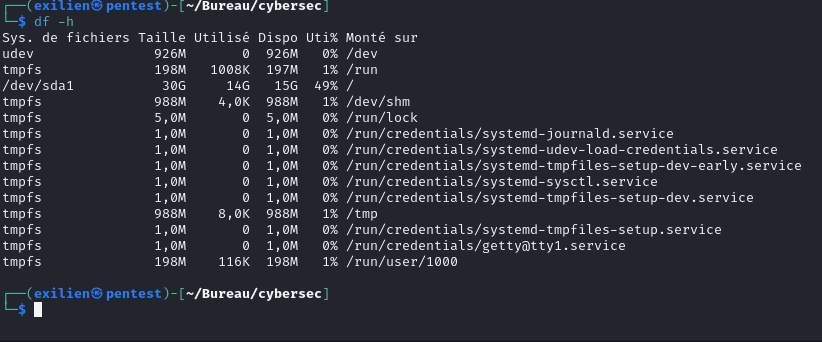
Créez un fichier secret.txt et changez ses permissions pour qu'il ne soit accessible qu'en lecture par le propriétaire.



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

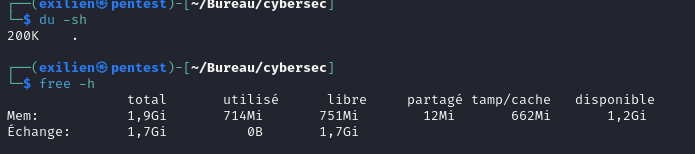
df : Affiche l'utilisation de l'espace disque.

-h : Affiche les informations dans un format lisible par l'humain (**h** pour "human-readable"), c'est-à-dire en Go, Mo, etc., au lieu de blocs en octets.



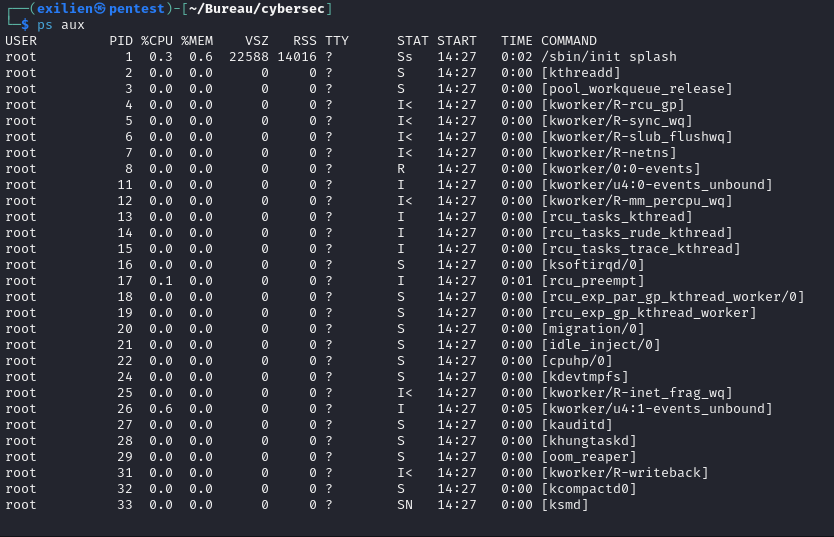
du : Signifie Disk Usage (utilisation du disque).

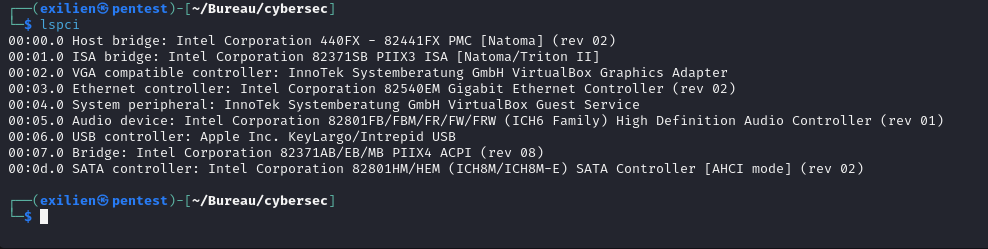
-s : Résumé (summary) – Affiche uniquement le total, sans détailler les sous-dossiers.

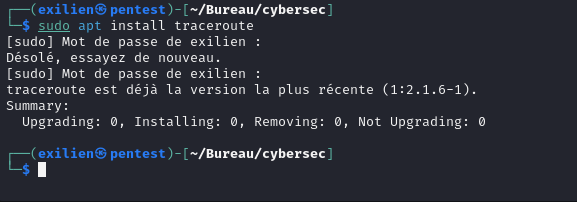
-h : Format lisible par l'humain (**h** pour "human-readable"), comme Ko, Mo, Go, etc. 

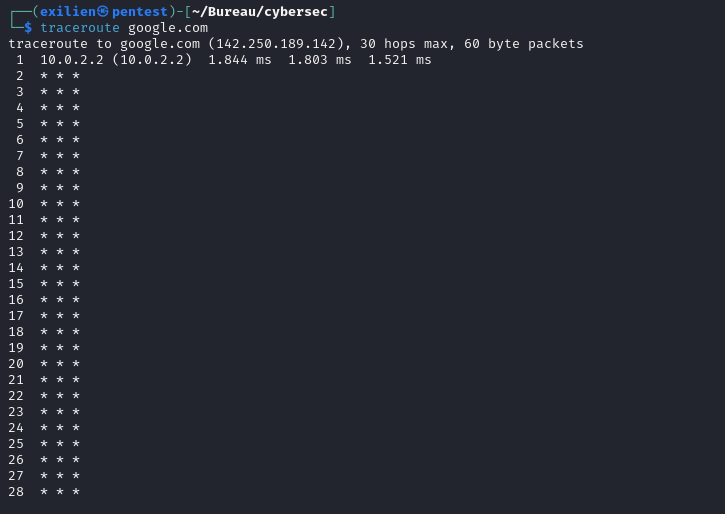
La commande **ps aux** sous Linux est utilisée pour afficher la **liste des processus en cours d'exécution** sur le système.

La commande **lspci** est utilisée pour lister **les périphériques connectés au bus PCI** de votre système (cartes graphiques, cartes réseau, contrôleurs USB, etc.).

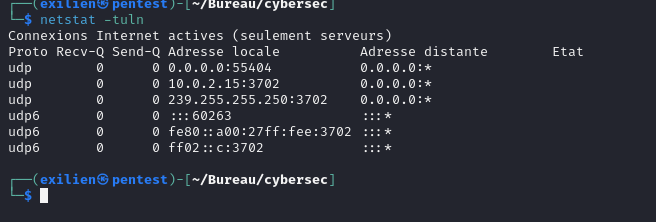




La commande **sudo apt install traceroute** installe **l'outil traceroute** sur votre machine pour vous permettre de diagnostiquer et visualiser les routes réseau suivies par vos paquets de données. 

La commande **traceroute google.com** est utilisée pour suivre le chemin emprunté par les paquets de données depuis votre ordinateur jusqu'à **google.com** (ou n'importe quel autre domaine) sur Internet. 

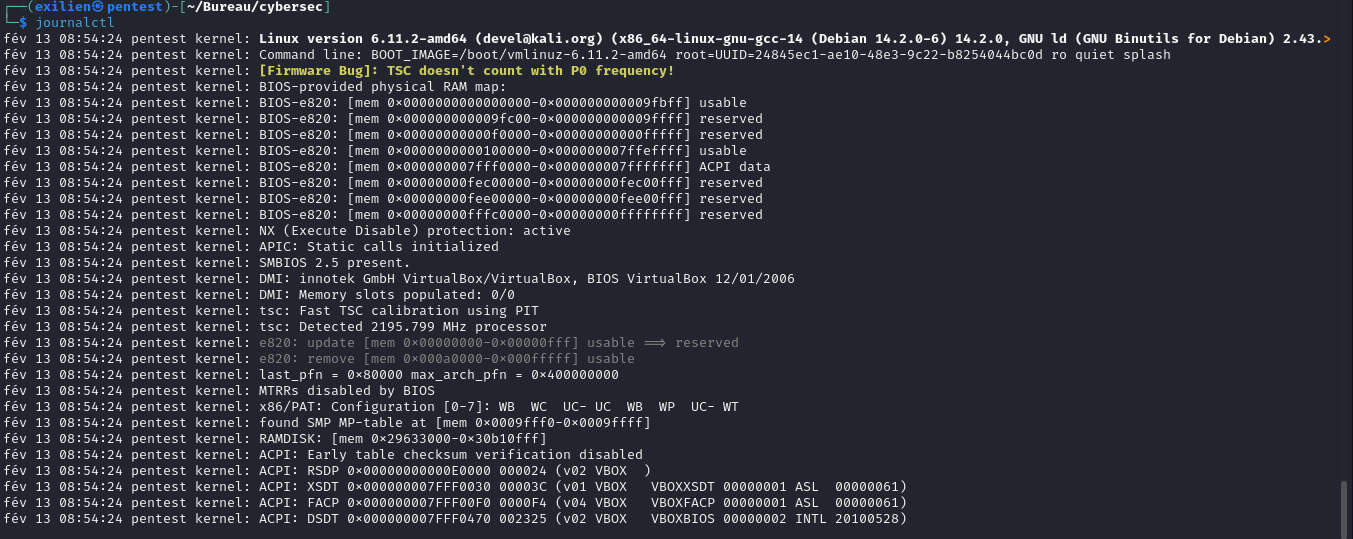
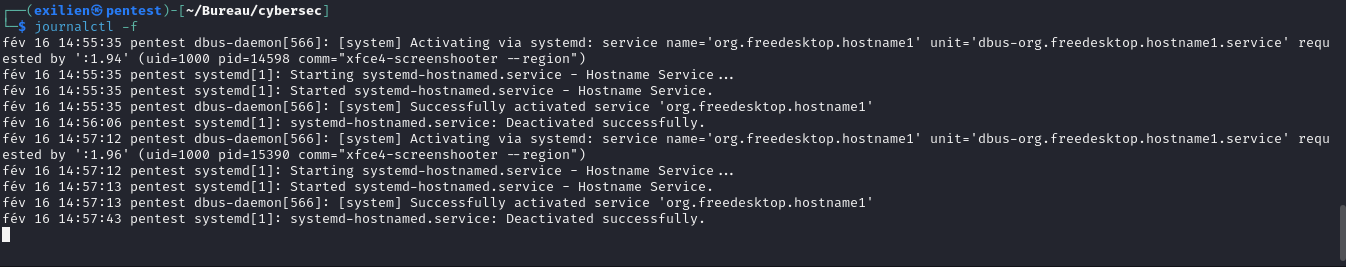
La commande **netstat -tuln** est utilisée pour afficher les **connexions réseau** et les **ports d'écoute** actifs sur votre machine.



La commande **ss -tuln** est utilisée pour afficher des informations sur les **connexions réseau** actives, de manière similaire à **netstat**, mais elle est plus rapide et plus moderne. **ss** (Socket Stat) est l'outil recommandé pour examiner les sockets réseau dans les systèmes modernes. 

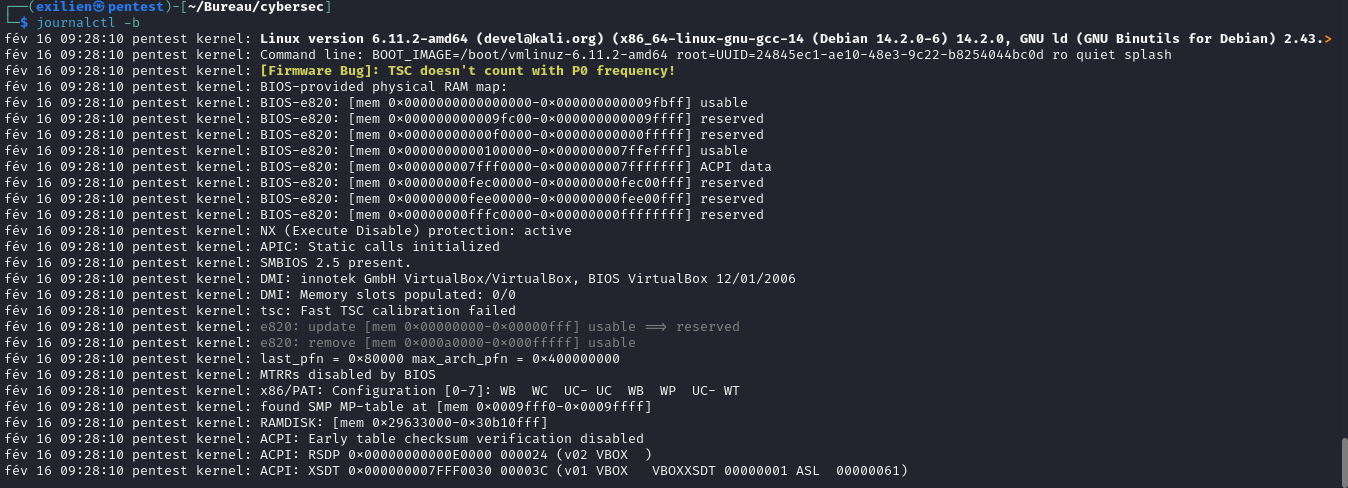
La commande **journalctl** est utilisée pour **afficher les journaux système** sur des systèmes utilisant **systemd**. Elle permet d'accéder aux logs générés par **systemd** (le gestionnaire de services du système), qui comprend des informations sur les services, les erreurs, les avertissements, etc.

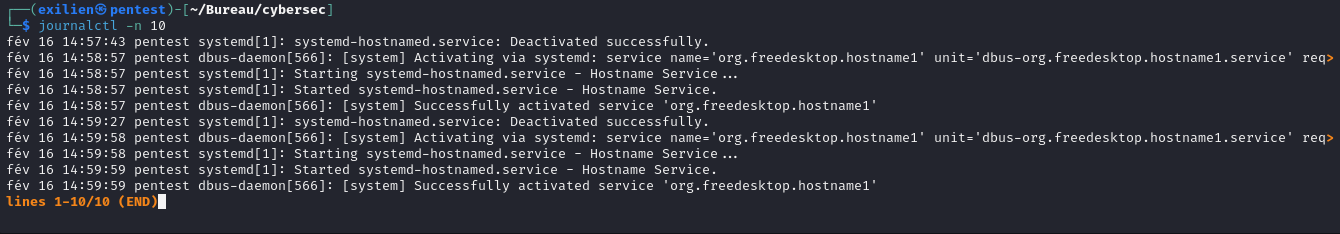
La commande **journalctl -f** est utilisée pour afficher les journaux **en temps réel** (comme la commande tail -f pour les fichiers). Cela permet de **suivre l'activité** des services système pendant leur exécution.

La commande **journalctl -b** est utilisée pour afficher les journaux **du dernier démarrage** du système. Cela permet de visualiser les événements enregistrés depuis que votre machine a été démarrée, y compris les messages du noyau, les services système et d'autres informations pertinentes.

La commande **journalctl -n 10** est utilisée pour afficher les **dernières 10 lignes** du journal. C'est un moyen rapide de voir les **derniers événements** enregistrés dans le journal sans avoir à parcourir l'ensemble du fichier.

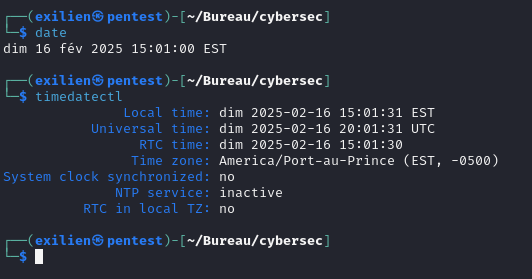


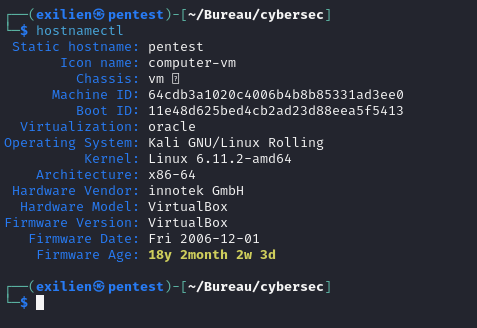


La commande **date** est utilisée pour afficher la **date et l'heure actuelles** du système dans un format lisible.

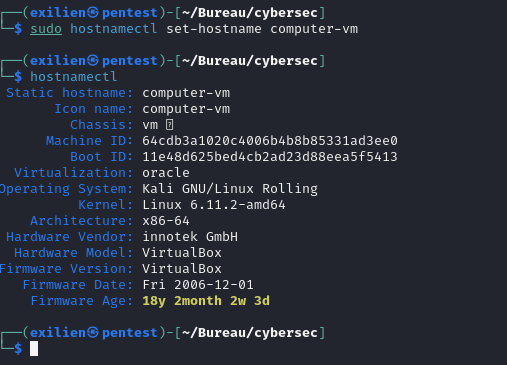
La commande **timedatectl** est utilisée pour **gérer et afficher** les **paramètres de date et d'heure** sur un système utilisant **systemd**.

La commande **hostnamectl** est utilisée pour **afficher ou configurer** le **nom d'hôte** de votre machine (le nom qui identifie l'ordinateur sur le réseau).





La commande **sudo hostnamectl set-hostname [nouveau\_nom]** est utilisée pour **changer le nom d'hôte** (hostname) de votre machine sous Linux.

. 

En un mot ,la tâche consistait à explorer et expliquer plusieurs commandes Linux qui sont essentielles pour la gestion et la configuration des systèmes.