Text

Description automatically generated with low confidence

Shape

Description automatically generated

|  |
| --- |
| Cheat sheet Linux |

Sylvain Depasse

1-19-2023

**Introduction**Ce document est donc un ‘aide-mémoire’ ou cheat sheet visant à vous épauler lors de manipulation linux. Chaque étape est documentée et illustrée de façon à permettre une entière compréhension. Néanmoins, il est sujet à être modifié, à évoluer.  
Retenez que certaines tâches devront être accomplies sous ‘root’

**Elévation de privilèges**Afin de vous approprier les droit admin (root sous linux) il vous sera nécessaire d’ouvrir une invite de commande (via votre clavier par exemple ‘**ctrl+alt+t’)**   
  
Dans celui-ci vous taperez la commande suivante  
  
$su  
  
Suivie du mdp valide pour l’élévation.  
  
// Effectivement, il sera plus efficace d’effectuer une élévation dès le début des opérations.

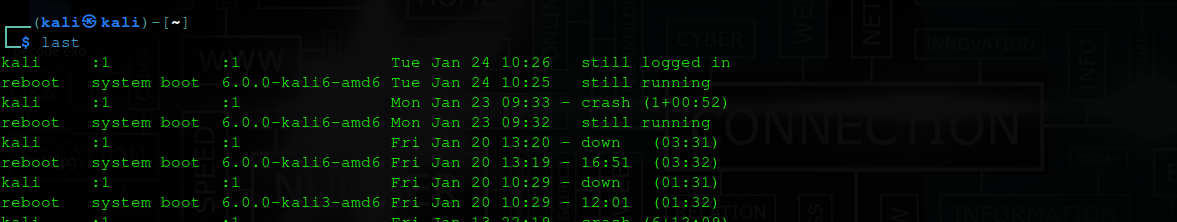
**Liés aux utilisateurs**

Dernières connexion

# lastlog



# last

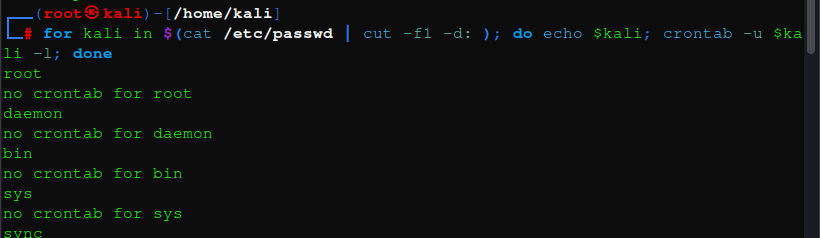


Utilisateur avec des shells de connexion

# cat /etc/passwd | grep sh$ //SCREEN

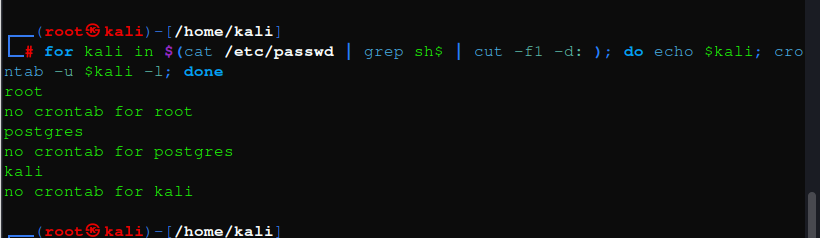
Lister les taches planifiées des utilisateur

# for user in $(cat /etc/passwd | cut -f1 -d: ); do echo $user; crontab -u $user -l; done



> utilisateurs avec shells

# for user in $(cat /etc/passwd | grep sh$ | cut -f1 -d: ); do echo $user; crontab -u $user -l; done



Clé SSH autorisées

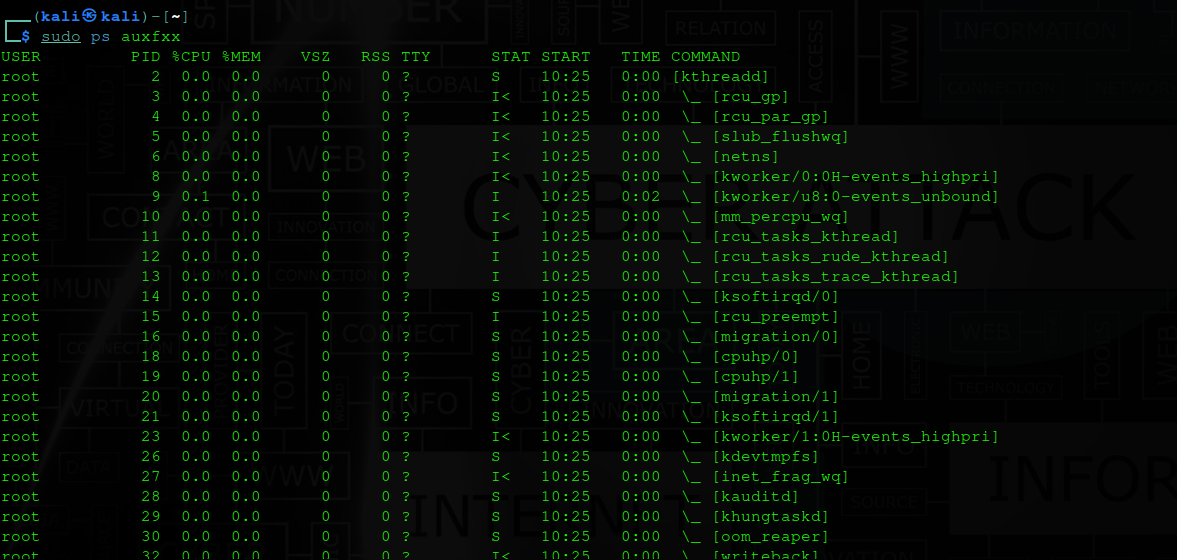
# find / -type f -name authorized\_keys 2</dev/null



**Processus et mise en réseau**

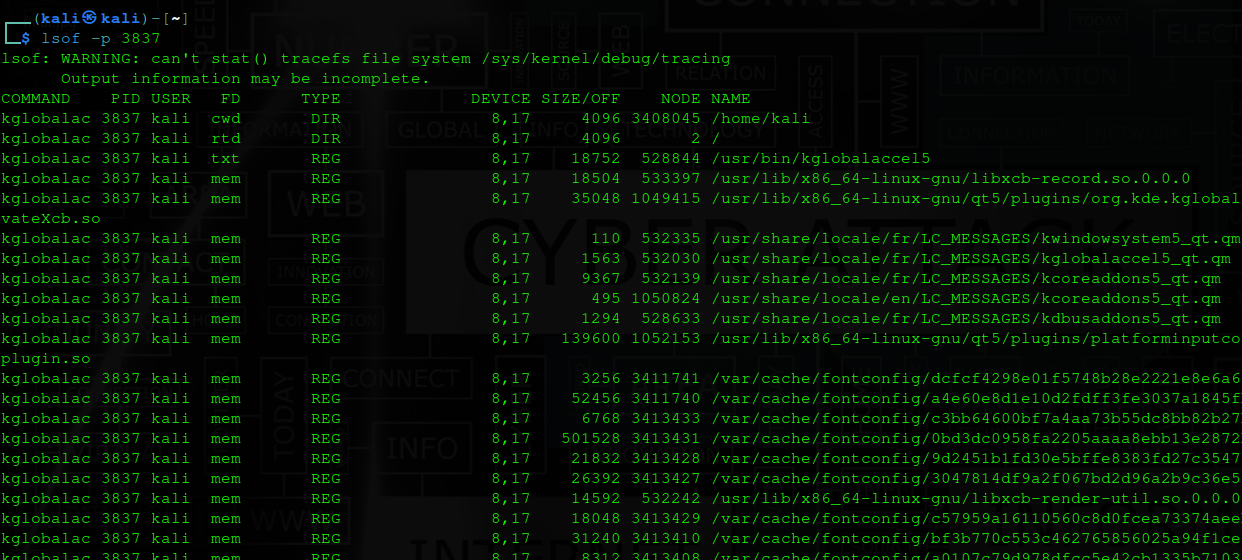
Afficher l'arborescence des processus avec nom d'utilisateur, TTY et sortie large.

# ps auxfww



Détails du processus

# lsof -p [pid]



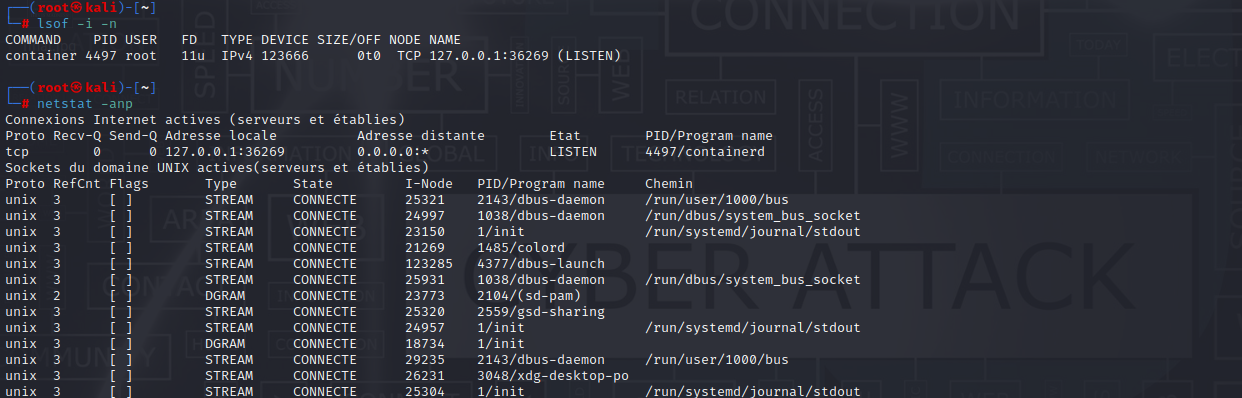
Pour arrêter un processus en court.

# kill [process id]

Afficher toutes les connexions ne résout pas les noms (IP uniquement)

# lsof -i -n

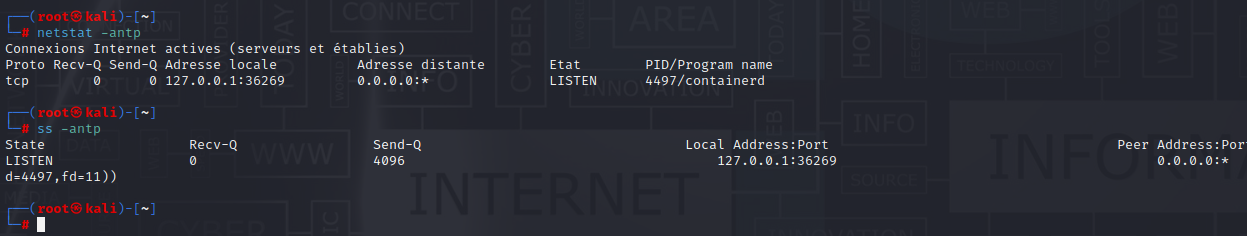
# netstat -anp



> Look for tcp only

# netstat -antp

# ss -antp



Lister tous les services

# service --status-all

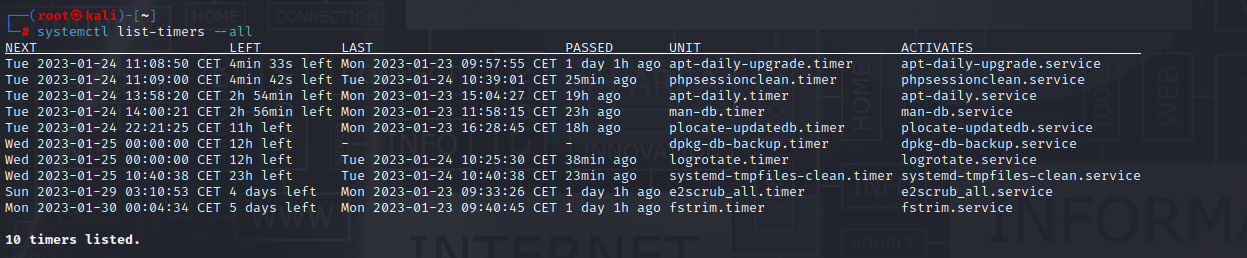


Répertorier les règles de pare-feu

# iptables --list-rules //pas compris??

Lister tous les minuteurs

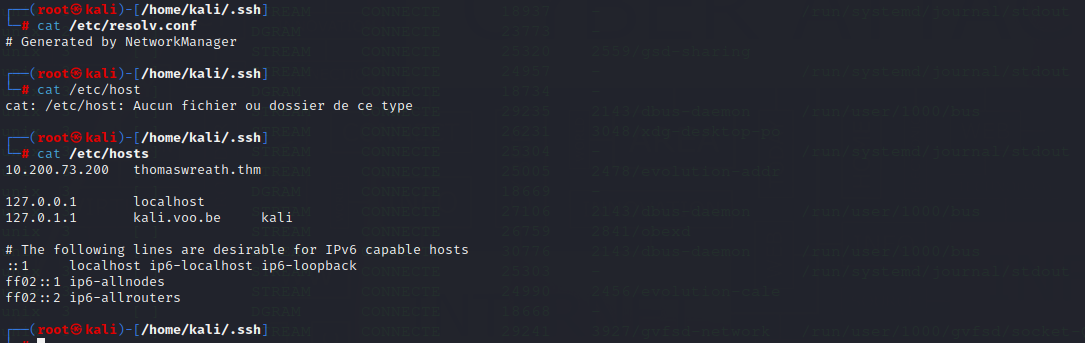
# systemctl list-timers –all



Consultez ces fichiers pour voir si le DNS a été empoisonné.

# cat /etc/hosts

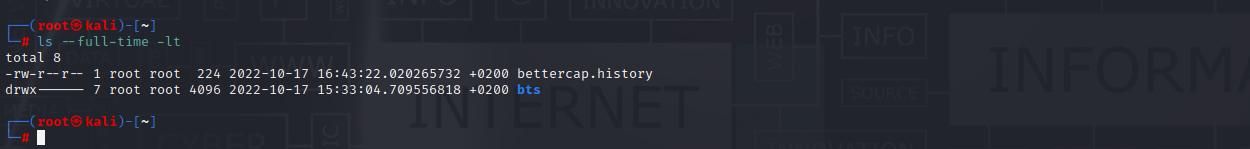
# cat /etc/resolv.conf



**Fichiers et dossiers**

Afficher la liste des fichiers et des dossiers avec un horodatage nano, trier par heure de modification (la plus récente).

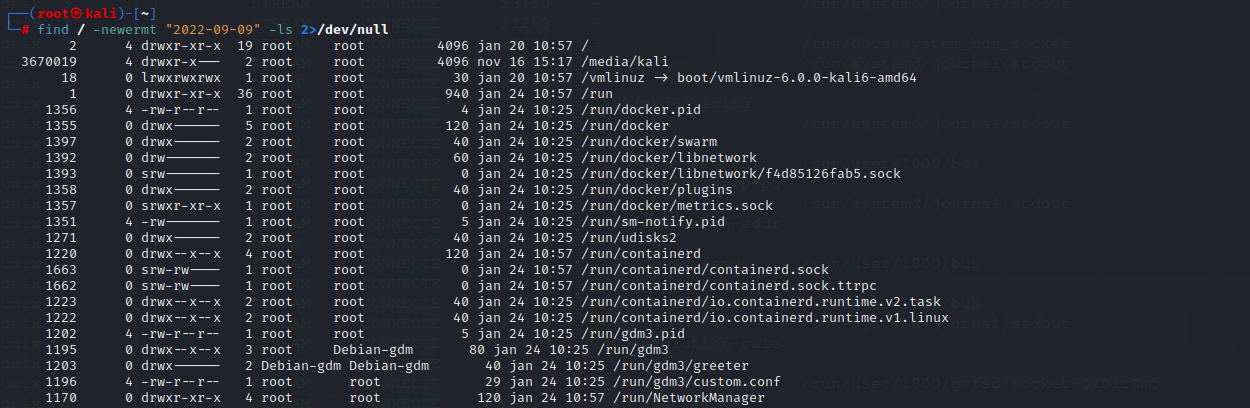
# ls --full-time -lt



Répertorier tous les fichiers qui ont été modifiés à une date/heure spécifique.

> Liste les fichiers qui ont été modifiés le 2021-06-16 (AAAA-MM-JJ)

# find / -newermt "2022-09-09" -ls 2>/dev/null



> Liste les fichiers qui ont été modifiés le 2021-05-01 jusqu'au 2021-05-09 (il y a 9 jours)

# find / -newermt "2022-05-01" ! -newermt "2022-05-10" -ls 2>/dev/null

> Liste les fichiers qui ont été modifiés le 2021-05-01 jusqu'au 2021-05-09 (il y a 9 jours) + ajouter un filtre

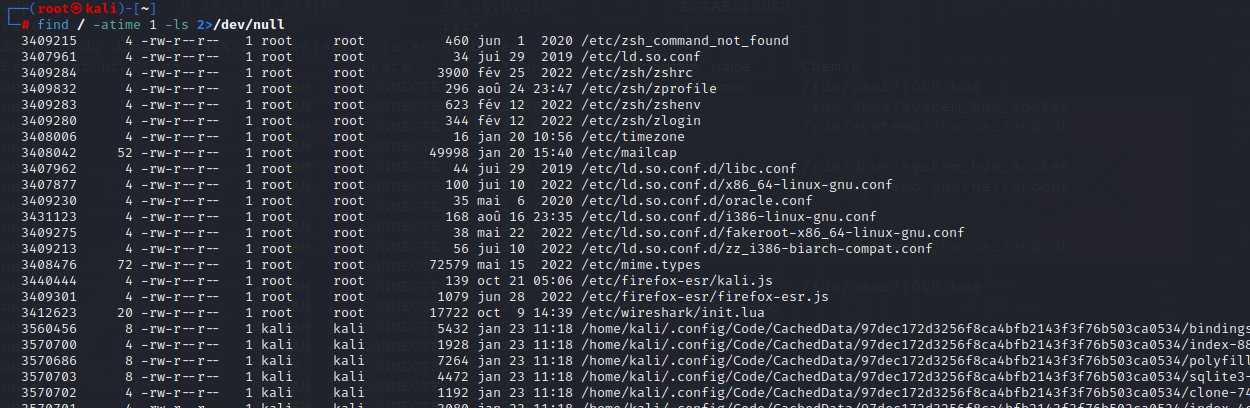
# find / -newermt "2022-05-01" ! -newermt "2022-05-10" -ls 2>/dev/null | grep -v 'filterone\|filtertwo'

> Liste des fichiers modifiés entre 01h00 et 07h00 le 16 juin 2021.

# find / -newermt "2022-06-16 01:00:00" ! -newermt "2022-06-16 07:00:00" -ls 2>/dev/null

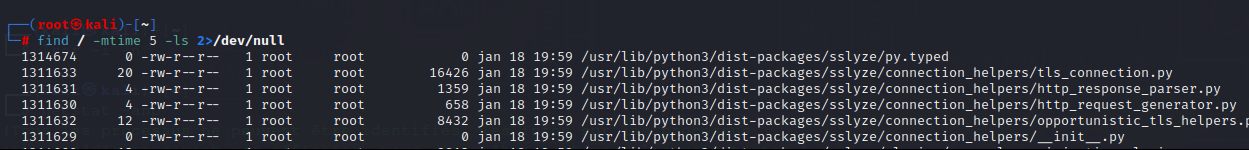
> Liste les fichiers qui ont été consultés il y a exactement 1 jour.

# find / -atime 1 -ls 2>/dev/null



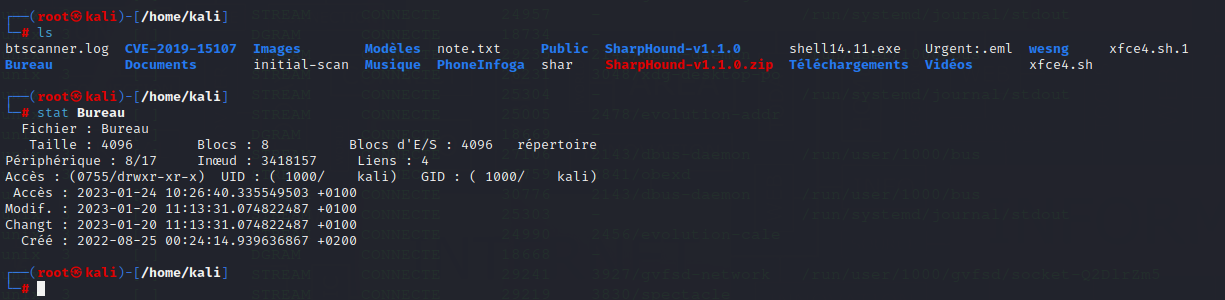
> Liste les fichiers qui ont été modifiés au cours des 5 derniers jours.

# find / -mtime 5 -ls 2>/dev/null

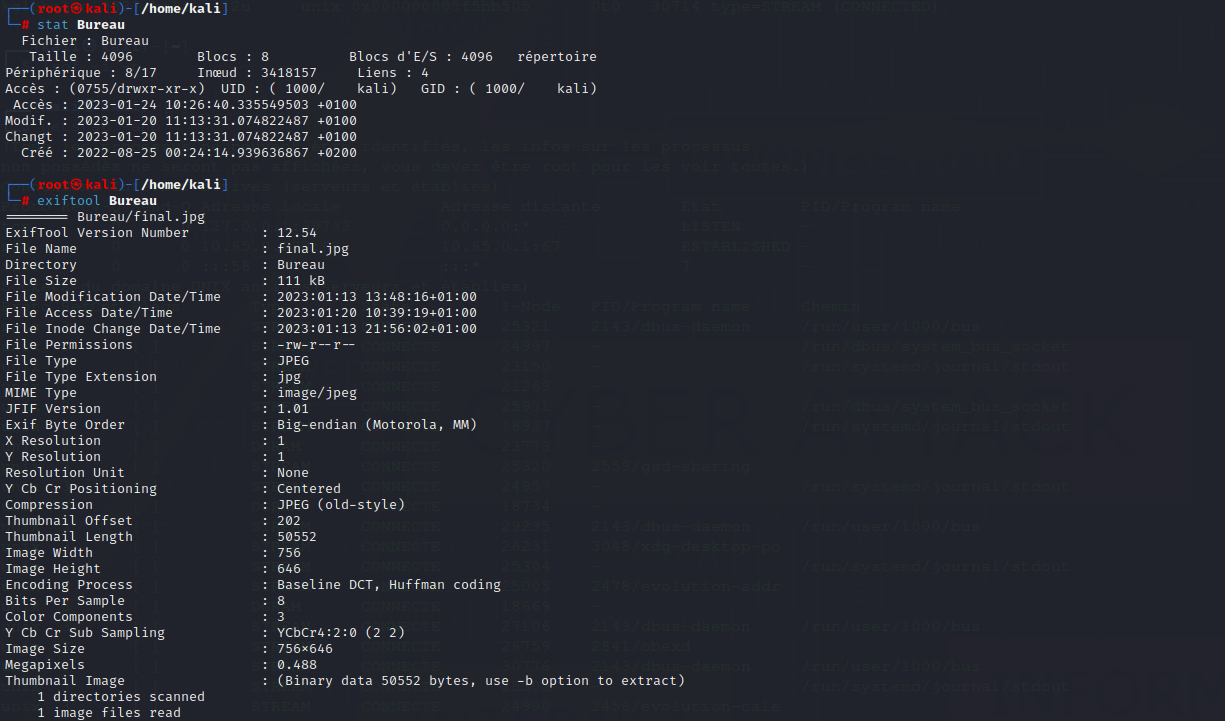


Consultation de dossier

# stat [file]



# exiftool [file]



Observer les changements dans les fichiers

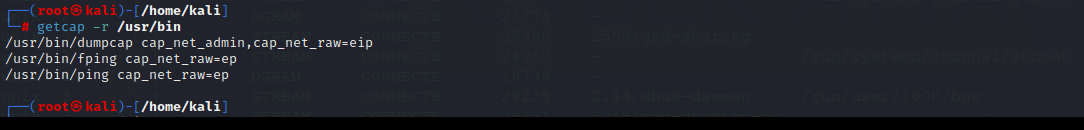
# find . -type f -exec md5sum {} \; | awk '{print $1}' | sort | uniq -c | grep ' 1 ' | awk '{print $2}'  
 // pas compris??

Chercher cap\_setuid+epen capacités binaires

# getcap -r /usr/bin/

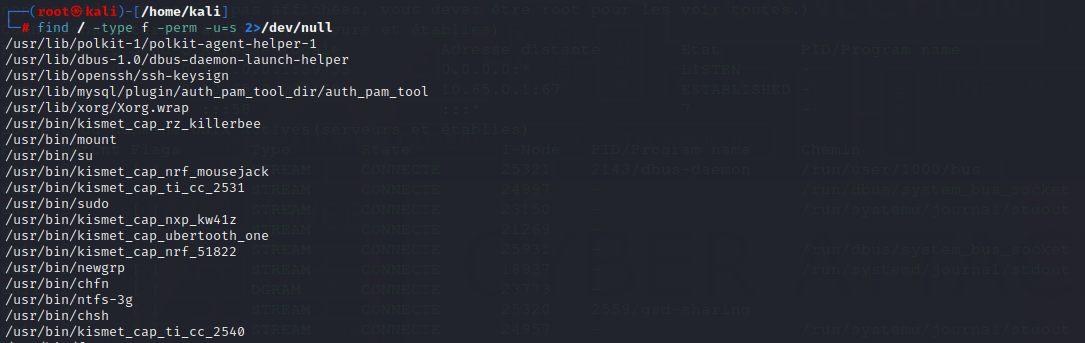
# getcap -r /bin/

# getcap -r / 2>/dev/null



Fail Perm

# find / -type f -perm -u=s 2>/dev/null



Audit des journaux

> 3eme partie

# aureport –tty

// contrôle install

**Zones de persistance**

Répertoires :

/etc/cron\*/

/etc/incron.d/\*

/etc/init.d/\*

/etc/rc\*.d/\*

/etc/systemd/system/\*

/etc/update.d/\*

/var/spool/cron/\*

/var/spool/incron/\*

/var/run/motd.d/\*

Des dossiers:

/etc/passwd

/etc/sudoers

/home/<user>/.ssh/authorized\_keys

/home/<user>/.bashrc