

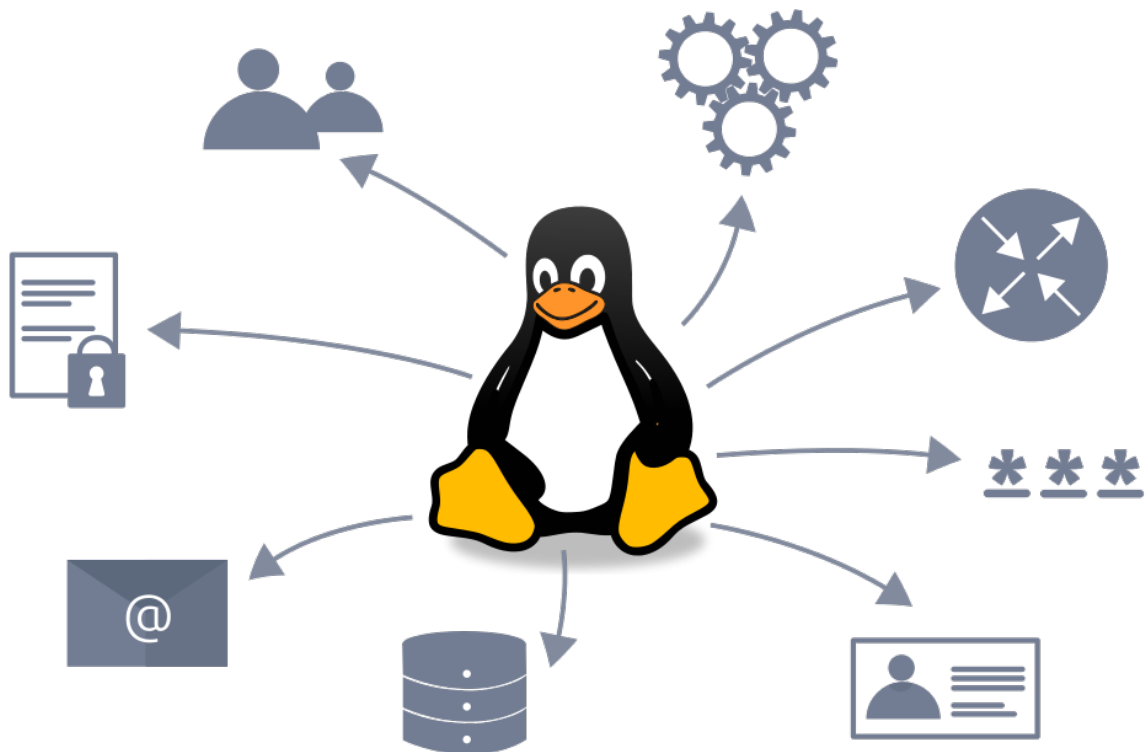
# Linux

- [\[Énumération/Linux\] Cheat-sheet](#)
- [\[Énumération/Linux\] Git-dumper](#)

# [Énumération/Linux] Cheat-sheet

## Introduction

Cette page va décrire différents procédés pour énumérer un système **Linux** qui pourraient vous servir.



## Manuel

### Afficher la version de l'OS

```
ls /etc/*-release
```

Par exemple sur **CentOS** :

```
cat /etc/os-release
```

## Afficher les utilisateurs / groupes / mots de passe

```
cat /etc/passwd
```

```
cat /etc/groups
```

```
cat /etc/shadow
```

Le fichier **shadow** est protégé en lecture par défaut et n'est pas accessible !

## Afficher les mails

```
ls -lh /var/mail/
```

## Afficher la liste des paquets

Sur les systèmes basés sur **Debian** :

```
dpkg -l
```

Et pour les systèmes basés sur **RedHat** :

```
rpm -qa
```

## Afficher les utilisateurs connectés

```
who
```

## Afficher la commande en cours d'exécution des utilisateurs connectés

```
w
```

## Afficher les dernières connexions d'utilisateurs

```
last
```

## Afficher les connexions actives

```
lsof -i [[:PORT]]
```

## Afficher l'arborescence des processus

```
ps axjf
```

# [Énumération/Linux] Git-dumper

## Introduction

Parfois, le site web que vous attaquez peut contenir un dépôt **Git**.

Dans ce cas, il peut être intéressant de le récupérer pour accéder au code source voire aux fichiers de configurations qui pourraient contenir des mots de passe ou autre.

## Git-dumper

Vous pouvez trouver le github de l'outil à cette adresse :

- <https://github.com/arthaud/git-dumper>

## Manuel

```
git-dumper <URL>/.git <OUTPUT_FOLDER>
```