

Hacking Windows 10 (et antérieur)

Règles

- "Saisie utilisateur"
- 'Élément cliquable/sélectionnable'
- Nom de fichier, dossier ou autre
- <Élément à remplacer>

lien, raccourci clavier et phrase de demande de saisie

commande, extrait code et extrait de fichier

Table des matières

- [Hacking Windows 10 \(et antérieur\)](#)
 - [Règles](#)
 - [Table des matières](#)
 - [Déverrouiller le compte administrateur](#)
 - [Première méthode \(Testé sur Windows 10 22h2 sur VirtualBox\)](#)
 - [Deuxième méthode \(Testé sur Windows 10 22h2 sur VirtualBox\)](#)

Déverrouiller le compte administrateur

Première méthode (Testé sur Windows 10 22h2 sur VirtualBox)

- cliquer sur le bouton d'alimentation dans le coin inférieur droit, puis de maintenir la touche Maj enfoncée tout en cliquant sur le bouton Redémarrer.
- cliquer sur 'Dépannage' > 'puis sur Options avancées' > 'Outils de redémarrage système'
- Cliquer sur 'Vous avez oublié votre mot de passe ou vous ne voyez pas votre compte ?'

Deuxième méthode (Testé sur Windows 10 22h2 sur VirtualBox)

- démarrer en mode sans échec
 - cliquer sur le bouton d'alimentation dans le coin inférieur droit, puis de maintenir la touche Maj enfoncée tout en cliquant sur le bouton Redémarrer.
 - cliquer sur 'Dépannage' > 'puis sur Options avancées' > 'Paramètres'
 - Cliquer sur 'Redémarrer'
 - Appuyer sur la touche 'f4' pour démarrer en mode sans échec ('fn' + 'f4' si 'f4' seul ne fonctionne pas)

à partir de là, j'ai déjà accès à windows, mais je devrais refaire la manipulation à chaque fois que je veux accéder à windows. Pour palier à ce problème, je vais créer un compte administrateur.

- Ouvrir une invite de commande en tant qu'administrateur
- Créer un nouveau compte

```
net user /add [nom du compte] [mot de passe]
```

- Ajouter le compte au groupe administrateur

```
net localgroup administrateurs [nom du compte] /add
```

=====

on peut ajouter n'importe quel programme dans

'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' pour qu'il se lance au démarrage de windows

- allez dans les clés de registre
- modifier la clé ``
- remplacer le fichier `` par le fichier `cmd.exe`