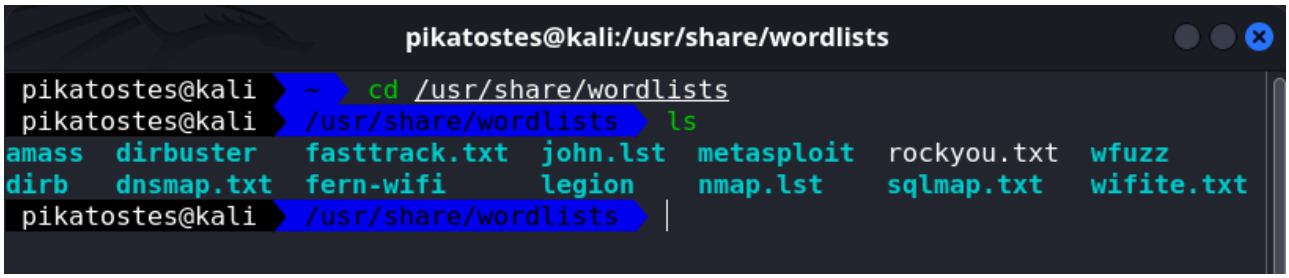
Práctica 01: Proceso de Cracking de Contraseñas con Hashcat

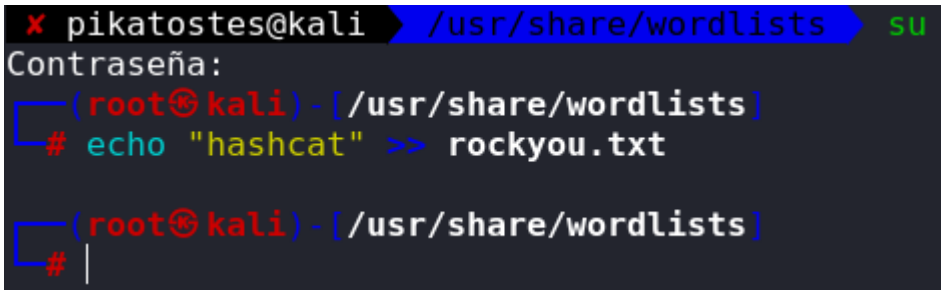
1. Preparación del Diccionario - Modificar rockyou.txt

Vamos a añadir la palabra `hashcat` a `rockyou.txt`.

1. En Kali, `rockyou.txt` ya viene instalado



2. Siendo superusuario, escribimos el siguiente comando



2. Descifrado de Hashes con Hashcat

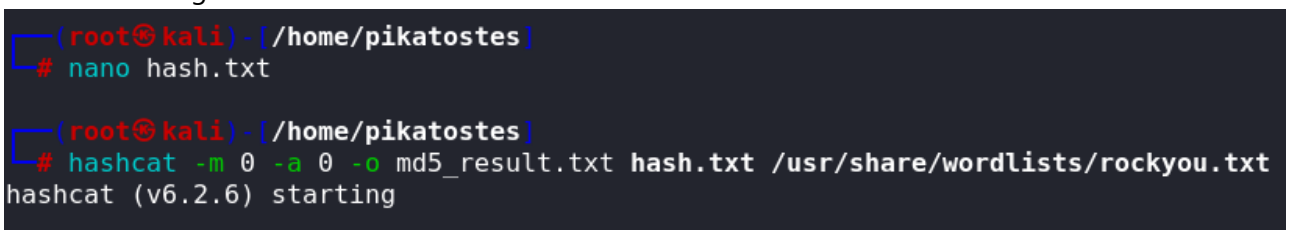
Hashcat es un potente descifrador de contraseñas que admite diferentes tipos de hash.

1. Descifrar Hash MD5

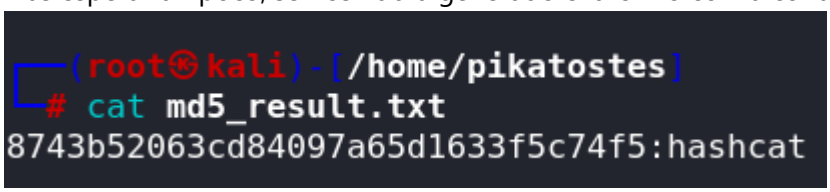
El hash a descifrar es el siguiente:

```
8743b52063cd84097a65d1633f5c74f5
```

1. Escribimos el siguiente comando:



2. Tras esperar un poco, se nos habrá generado el archivo con la contraseña crackeada:



2. Descifrar Hash NTLM

```
┌──(root㉿kali)-[/home/pikatostes]
└─# nano hash_ntlm.txt

┌──(root㉿kali)-[/home/pikatostes]
└─# cat hash_ntlm.txt
b4b9b02e6f09a9bd760f388b67351e2b
```

```
┌──(root㉿kali)-[/home/pikatostes]
└─# hashcat -m 1000 -a 0 -o ntlm_result.txt hash_ntlm.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
┌──(root㉿kali)-[/home/pikatostes]
└─# cat ntlm_result.txt
b4b9b02e6f09a9bd760f388b67351e2b:hashcat
```

3. Descifrar Hash NETNTLMv2

```
┌──(root㉿kali)-[/home/pikatostes]
└─# nano hash_netntlmv2.txt

┌──(root㉿kali)-[/home/pikatostes]
└─# cat hash_netntlmv2.txt
admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030
```

```
┌──(root㉿kali)-[/home/pikatostes]
└─# hashcat -m 5600 -a 0 -o netntlmv2_result.txt hash_netntlmv2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
┌──(root㉿kali)-[/home/pikatostes]
└─# cat netntlmv2_result.txt
ADMIN::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030:hashcat
```