

CracktheHash

En este reto nos embarcaremos en la magia de identificar los hash y crackearlos

Nivel 1:

1. 48bb6e862e54f2a795ffc4e541caed4d

para esto lo primero será identificar , la naturaleza del mismo , utilizaremos una herramienta llamada hash identifier:

```
(viernez13㉿kali)-[~]
$ hash-identifier
#####
#          v1.2 #
# By Zion3R #
# www.Blackploit.com #
# Root@Blackploit.com #
#####
HASH: 48bb6e862e54f2a795ffc4e541caed4d
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Possible MD5 ;D

para crackear MD5 se utiliza hashcat

como es parte de un ctf y las preguntas dicen que se debe ocupar rockyou utilizaremos este metodo
hashcat -m 0 Valor del hash /usr/share/wordlists/rockyou.txt

```

(viernez13㉿kali)-[~]
$ hashcat -m 0 48bb6e862e54f2a795ffc4e541caed4d /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-sandybridge-AMD A10-7860K Radeon R7, 12 Compute Cores 4C+8G, 2251/4566 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient ... █

```

la hemos crackeado!

```

Dictionary cache hit:
* Filename .. : /usr/share/wordlists/rockyou.txt
* Passwords.. : 14344385
* Bytes..... : 139921507
* Keyspace .. : 14344385

48bb6e862e54f2a795ffc4e541caed4d:easy

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 0 (MD5)
Hash.Target...: 48bb6e862e54f2a795ffc4e541caed4d
Time.Started...: Mon Feb  5 00:21:03 2024 (0 secs)
Time.Estimated.: Mon Feb  5 00:21:03 2024 (0 secs)
Kernel.Feature ..: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 868.3 kH/s (0.32ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 173056/14344385 (1.21%)
Rejected.....: 0/173056 (0.00%)
Restore.Point...: 172032/14344385 (1.20%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: florida69 → convict1
Hardware.Mon.#1..: Util: 52%

Started: Mon Feb  5 00:20:22 2024
Stopped: Mon Feb  5 00:21:05 2024

```

es easy!

Segundo nivel!

2. CBFDAC6008F9CAB4083784CBD1874F76618D2A97

D: identificamos

```
(viernez13㉿kali)-[~]
$ hash-identifierd for this attack: 0 MB
#####
Dic#ionary cache hit:
* F#lenA\.\.\.\sr/share/wordlists/\w\you.txt
* P#sswo\ld\.\.\.\4\44385
* B#tes..\.\.: 139\21\07\.
* K#yspace..\.\4\4\5\.
#
48b#6e862e54\2a\%f\%e5\%a\%d:es\y
#
Session.....: hashcat
Status.....: Cracked
Hash.....:
Hash.Target....: 48b6e862e54f2a795fffc4e541caed4d
THASH:tCBFDAC6008F9CAB4083784CBD1874F76618D2A97secs)
Time.Estimated ...: Mon Feb 5 00:21:03 2024 (0 secs)
PossibleHashes...: Pure Kernel
[+]sSHA-1e.....: File (/usr/share/wordlists/rockyou.txt)
[+]sMySQL5e-.SHA-1(SHA-1($pass))
```

de seguro en esta parte se podrían preguntar como se puede saber el modulo a ejecutar , se puede adquirir desde acá : https://hashcat.net/wiki/doku.php?id=example_hashes

en el caso de Sha1 ,es este:

100 SHA1 b89eaac7e61417341b710b727768294d0e6a277b

probamos el comando :

```
hashcat -m 100 CBFDAC6008F9CAB4083784CBD1874F76618D2A97 /usr/share/wordlists/rockyou.txt
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels/can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See#the above message to find out about the exact limits.

#
# Watchdog: Temperature abort trigger set to 90c
# Host memory required for this attack: 0 MB
#
Dictionary cache hit:
* Filename...: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
*#Bytes.CFEDAE6139921507083784CBD1874F76618D2A97
* Keyspace .. : 14344385
Possible Hashes:
cbfdac6008f9cab4083784cbd1874f76618d2a97:password123
[+] MySQL5 - SHA-1(SHA-1($pass))
Session.....: hashcat
Status.....: Possible.Us:hCracked
HashMode.160....: 100 (SHA1)
HashWTarget60....: cbfdac6008f9cab4083784cbd1874f76618d2a97
TimeStarted50....: Mon Feb  5 00:26:28 2024 (0 secs)
TimeEstimated...: Mon Feb  5 00:26:28 2024 (0 secs)
Kernel.FeatureHMAC:Pure Kernel
Guess.Base.160(WMACFile (/usr/share/wordlists/rockyou.txt)
Guess.Queue.50(WMAC):1/1 (100.00%)
Speed.#1(MNGS): 915.8 kH/s (0.23ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered(MNGS): 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress($pass.$$:l2048/14344385 (0.01%)
Rejected($salt.$$:s0/2048 (0.00%)
Restore Point..md:(1024/14344385 (0.01%)
Restore Sub.#1 .md:(Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine:1 Device)Generator
Candidates.#1...:1kuciing →alovers1))
Hardware.Mon.#1...:Util: 54%
```

password123

Nivel 3!

3. 1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032
mismo procedimiento :
acá hay un truquito , SHA-256 es SHA2-256

1400 SHA2-256 127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2cab935

password , letmein

Avancemos al siguiente Nivel.

4. \$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkjkUlypTsgbX1H68wsRom

acá se pone más compleja la pista , debido a que hash-identifier , no detecta el hash!

HASH: \$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom
Not Found.

HASH: [REDACTED]

buscando en internet llegué a esto buscando la naturaleza del resultado , llegue a una pagina donde muestran diferentes algoritmos :

<https://www.onlinehashcrack.com/hash-acceptance.php>

The screenshot shows the homepage of onlinehashcrack.com. The top navigation bar includes links for HOME, PASSWORD RECOVERY, HOW TO?, FREE TOOLS, ALGORITHMS, ABOUT, and CONTACT. The main section is titled "PASSWORD HASH IDENTIFICATION" and contains a sub-instruction: "Enter your unknown hash and we will try to identify it, we support over 250 hash types." Below this is a text input field containing the hash value: "\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkjkUlypTsgbX1H68wsR". To the right of the input field, under the heading "Result:", it says "Your hash may be one of the following:" followed by a list: - Blowfish(OpenBSD) - Woltlab Burning Board 4.x - bcrypt.

Enter a hash to identify:

```
$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkjkUlypTsgbX1H68wsR
```

Result:

Your hash may be one of the following:

- Blowfish(OpenBSD)
- Woltlab Burning Board 4.x
- bcrypt

Example Hash Inputs

Blowfish(OpenBsd)

```
hashcat -m 3200 "\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkjkUlypTsgbX1H68wsRom" /usr/share/wordlists/rockyou.txt
```

acá habrá que separar la codificación lo que hice fue ponerle \ antes de cada \$ para que sea reconocido.

y haremos una trampa , debido a que si usamos rockyou completo tardará app 27 días en crackearla xD

como sabemos que la clave de la primera es de 4 digitos convertiremos rockyou en un diccionario de solo 4 caracteres alfanumericos.

para esto , primero creamos el dicc

```
awk 'length==4' /usr/share/wordlists/rockyou.txt > /home/viernez13/f4letrasrock.txt
```

luego lanzaremos el hashcat

```
hashcat -m 3200 "\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkjkUlypTsgbX1H68wsRom" /home/viernez13/f4letrasrock.txt
```

```

[+] sha1(sha1($pass).$salt)
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => hashcat -m 3200 "
$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom:bleh
[+] sha1(sha1($pass))
Session1(strtotime(hashcatame)).$pass)
Status.....: Cracked
HashMode:3200 (bcrypt9$2*$, Blowfish (Unix))46683D7B336B63032
Hash.Target....: $2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX ... 8wsRom
Time.Started....: Mon Feb  5 02:13:03 2024 (1 min, 51 secs)
Time.Estimated ...: Mon Feb  5 02:14:54 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.....: File (/home/viernez13/f4letrasrock.txt)
Guess.Queue: 1/1 (100.00%)
Speed.#1.P.34.11.94   6 H/s (5.61ms) @ Accel:2 Loops:32 Thr:1 Vec:1
Recovered.256....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.256....: 652/18152 (3.59%)
Rejected.256(HMAC): 0/652 (0.00%)
Restore.Point(WMAt): 648/18152 (3.57%)
Restore.Sub.#1(WMAt): Salt:0 Amplifier:0-1 Iteration:4064-4096
Candidate.Engine: Device Generator
Candidates.#1.:;ableh → 9876
Hardware.Mon.#1.:;pUtil: 89%
Started: Mon Feb  5 02:12:52 2024 5ieeUznr71EeNkJkUlypTsgbX1H68wsRom
Stopped: Mon Feb  5 02:14:56 2024
Not Found.
(viernez13㉿kali)-[~]
└─$:

```

luego de unos minutos , hemos conseguido la clave!! ;D

nivel5

traté de identificar el hash resultando en un MD5 lo cual no era , por lo cual fui por la vía fácil , me fui a crackstation y fue correcto era un md4

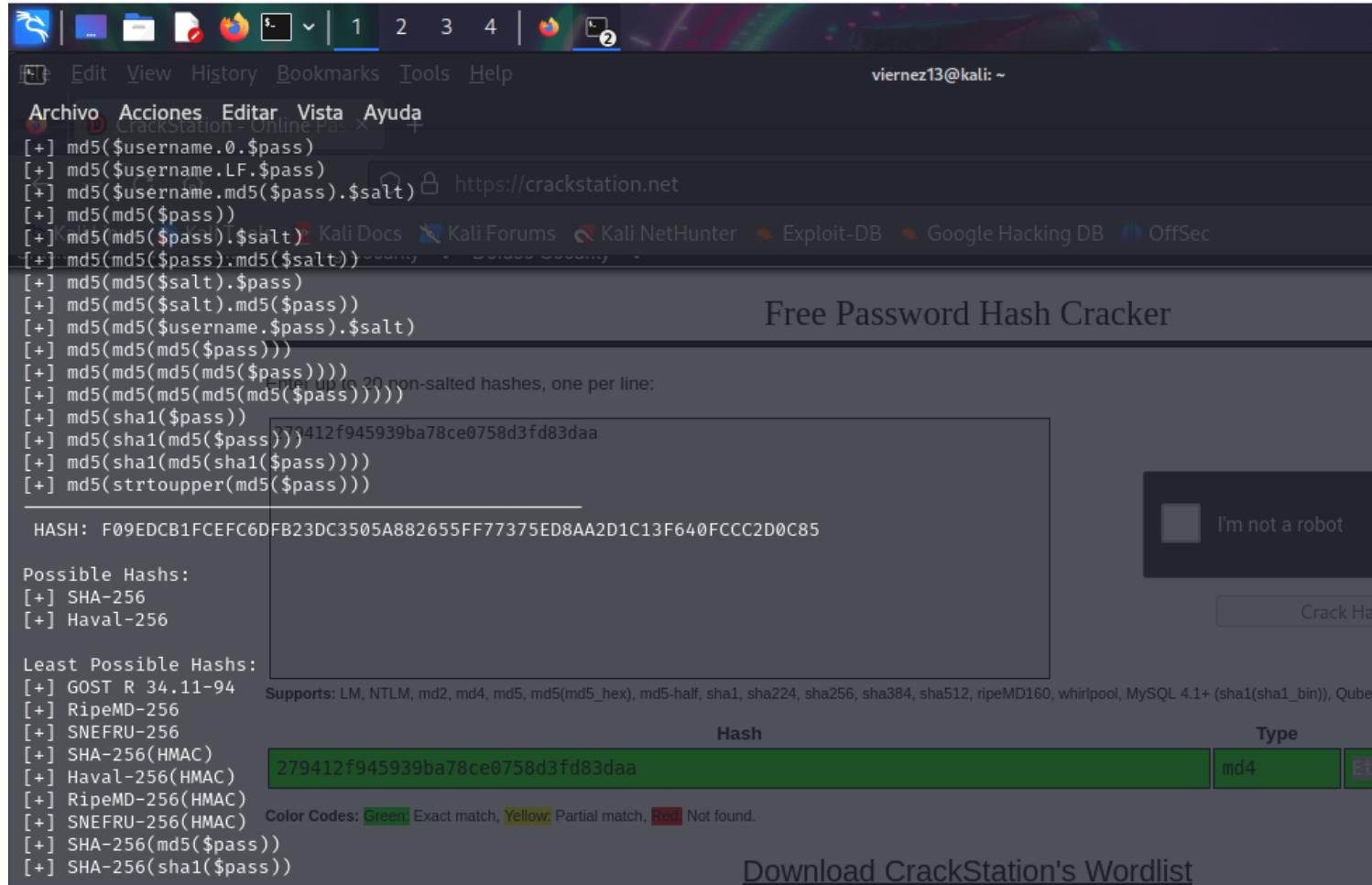
Hash	Type	Result
279412f945939ba78ce0758d3fd83daa	md4	Eternity22

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

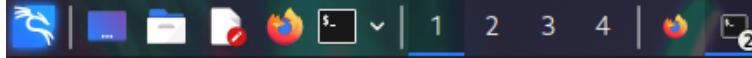
2 Tarea , nivel 1

F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85

fue reconocido como sha-256
es el modulo 1400 , hacemos la magia



Archivo Máquina Ver Entrada Dispositivos Ayuda



Edit View History Bookmarks Tools Help

viernez13@kali: ~

Archivo Acciones Editar Vista Ayuda

Host memory required for this attack: 0 MB
<https://crackstation.net>

Dictionary cache hit:

- * Filename...: /usr/share/wordlists/rockyou.txt
- * Passwords.: 14344385
- * Bytes.....: 139921507
- * Keyspace .. : 14344385

Free Password Hash Cracker

f09edcb1fcefc6dfb23dc3505a882655ff77375ed8aa2d1c13f640fcc2d0c85:paule

Session.....: hashcat

Status.....: Cracked

Hash.Mode.....: 1400 {SHA2-256}

Hash.Target.....: f09edcb1fcefc6dfb23dc3505a882655ff77375ed8aa2d1c13f ... 2d0c85

Time.Started....: Mon Feb 5 02:26:44 2024 (0 secs)

Time.Estimated ... : Mon Feb 5 02:26:44 2024 (0 secs)

Kernel.Feature ... : Pure Kernel

Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)

Guess.Queue.....: 1/1 (100.00%)

Speed.#1.....: 666.7 kH/s (0.77ms) @ Accel:512 Loops:1 Thr:1 Vec:8

Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)

Progress.....: 78848/14344385 (0.55%)

Rejected.....: 0/78848 (0.00%)

Restore.Point....: 77824/14344385 (0.54%)

Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1

Candidate.Engine.: Device Generator

Hash

Candidates.#1....: superm → jasons1

Hardware.Mon.#1..: Util: 54%

Started: Mon Feb 5 02:26:43 2024 Exact match, Yellow Partial match, Red Not found.

Stopped: Mon Feb 5 02:26:46 2024

Nivel 2

1DFECA0C002AE40B8619ECF94819CC1B

Probé MD5 sin resultado

```
*+Create more (work)items to make use of your parallelization power:
[+] https://hashcat.net/faq/morework
[+] RipeMD-128(HMAC)
Approaching final keyspace - workload adjusted.
[+] SNEFRU-128(HMAC)
Session.....: hashcat
Status....:128(WM4:)Exhausted
Hash.Mode....:0 (MD5)
Hash.Target....:1dfeca0c002ae40b8619ecf94819cc1b
Time.Started....:Mon Feb 5 02:32:06 2024 (10 secs)
Time.Estimated...:Mon Feb 5 02:32:16 2024 (0 secs)
Kernel.Feature....:Pure Kernel
Guess.Base....:File(/usr/share/wordlists/rockyou.txt)
Guess.Queue....:1/1(100.00%)
Speed.#1.....:1345.8kh/s (0.28ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered....:0/1(0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....:14344385/14344385 (100.00%)
Rejected.....:0/14344385 (0.00%)
Restore.Point....:14344385/14344385 (100.00%)
Restore.Sub.#1...:Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.:Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..:Util: 42%
[+] md5($salt,$pass)
Started:Mon Feb 5 02:32:04 2024
Stopped:Mon Feb 5 02:32:18 2024
[+] md5($salt,$pass))
```

Probé MD4 sin resultado

```
[+] This has a drastic speed impact but can be better for specific attacks.
[+] Typical scenarios are a small wordlist but a large ruleset.
[+] RipeMD-128(HMAC)
*+ Update your backend API runtime / driver the right way:
[+] https://hashcat.net/faq/wrongdriver
[+] Tiger-128
*+ Create more work items to make use of your parallelization power:
[+] https://hashcat.net/faq/morework
[+] md5($salt.$pass)
Approaching final keyspace - workload adjusted.
[+] md5($salt.$pass.$username)
Session.....: hashcat
Status.....: Exhausted
HashMode: alt.md5:$900s(MD4)t)
Hash.Target: $1dfeca0c002ae40b8619ecf94819cc1b
Time.Started: Mon Feb 5 02:34:40 2024 (11 secs)
Time.Estimated: Mon Feb 5 02:34:51 2024 (0 secs)
Kernel.FeatureName:@PuresKernel
Guess.Base.Username:!/Filea(/usr/share/wordlists/rockyou.txt)
Guess.Queue.Username: m1/1$(100.00%)lt)
Speed.#1.....: 1214.4 KH/s (0.22ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Points.....: 14344385/14344385 (100.00%)
Restore.Sub.#1.....: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine: aDevice Generator
Candidates:#1d5(m:$HEX[206b7269734656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon#1.m$Util:$68%))
[+] md5($salt.$pass))
Started: Mon Feb 5 02:34:38 2024
Stopped: Mon Feb 5 02:34:53 2024
```

el reconocimiento que podrán ser posibles otros..

```
PossibleHashes: all keyspace - workload adjusted.
[+] MD5
[+] sDomain.Cached:Credentials - MD4(MD4(($pass)).(strtolower($username)))
Status.....: Exhausted
LeastMPossibleHashes: 0 (MD4)
[+] hRAadmin tv2.x...: 1dfeca0c002ae40b8619ecf94819cc1b
[+] eNTLMrted.....: Mon Feb 5 02:34:40 2024 (11 secs)
```

probaré con NTLM
modo de ntlm es 1000

1000	NTLM	b4b9b02e6f09a9bd760f388b67351e2b
------	------	----------------------------------

hashcat -m 1000 1DFECA0C002AE40B8619ECF94819CC1B /usr/share/wordlists/rockyou.txt

```
(viernez13㉿kali)-[~]
└─$ hashcat -m 1000 1dFeca0c002AE40B8619ECF94819CC1B /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-sandybridge-AMD A10-7860K Radeon R7, 12 Compute Cores 4C+8G, 2251/4566 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient ...
```

era NTLM

```
Dictionary cache hit:
* Filename .. : /usr/share/wordlists/rockyou.txt
* Passwords.. : 14344385
* Bytes..... : 139921507
* Keyspace .. : 14344385

1dFeca0c002ae40B8619ecf94819cc1b:n63umy8lkf4i

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 1000 (NTLM)
Hash.Target...: 1dFeca0c002ae40B8619ecf94819cc1b
Time.Started...: Mon Feb  5 02:39:06 2024 (4 secs)
Time.Estimated ...: Mon Feb  5 02:39:10 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1495.6 kH/s (0.24ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 5239808/14344385 (36.53%)
Rejected.....: 0/5239808 (0.00%)
Restore.Point...: 5238784/14344385 (36.52%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: n6ri2fdkgm9y → n4athan5
Hardware.Mon.#1..: Util: 43%

Started: Mon Feb  5 02:38:27 2024
Stopped: Mon Feb  5 02:39:11 2024
```

```
(viernez13㉿kali)-[~]
└─$
```

nivel3

Hash: \$6\$aReallyHardSalt\$6WKUTqzq.UQQmmr0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxlf.hsGpS41BqMhSrHVXgMp djS6xeKZAs02.

Salt: aReallyHardSalt

acá se complica un poco la cosa , ya comenzamos a tener salt...

pero ¿qué es un salt?

Salt es un número de dígitos aleatorios que se le agrega a la contraseña ya sea al principio o al final y que el usuario no conocerá. Con esto, la contraseña se hace de mayor longitud y por lo tanto más compleja, de esta manera será mucho más difícil encontrar el hash en una tabla y más aún obtener la contraseña, ya que está combinada con el salt.

De esta manera, el salt constituye un método de seguridad que los sistemas deben usar para la protección de las contraseñas.

Identificamos el cifrado :

PASSWORD HASH IDENTIFICATION

Enter your unknown hash and we will try to identify it, we support over 250 hash types.

Enter a hash to identify:

\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHvXgMpjdjS6xeKZAs02.

Result:

Your hash may be one of the following:
- SHA-512 Crypt

ahora buscaremos el módulo , podemos hacerlo con hashid

```
hashid -m "\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHvXgMpjdjS6xeKZAs02."
```

```
Analyzing '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHvXgMpjdjS6xeKZAs02.'
```

se les recuerda separar , siempre antes de un \$ con un \

```
(viernez13㉿kali)-[~]
$ hashid -m "\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHvXgMpjdjS6xeKZAs02."
Analyzing '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHvXgMpjdjS6xeKZAs02.' 
[+] SHA-512 Crypt [Hashcat Mode: 1800]
```

el crackeo de SHA-512 puede ser tardío por lo cual aplicaremos la misma trampa que hicimos hace unos niveles atrás

son 6 dígitos

Answer format: *****

6

Submit

```
awk 'length==6' /usr/share/wordlists/rockyou.txt > /home/viernez13/f6letrasrock.txt
```

```
hashcat -m 1800 "\$6\$aReallyHardSalt\$6WKUTqzq.UQQmmr0p/  
T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpds6xeKZAs02." /home/viernez13/  
f6letrasrock.txt
```

```
Archivo Acciones Editar Vista Ayuda  
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)  
Progress.....: 581696/1949273 (29.84%)  
Rejected.....: 0/581696 (0.00%)  
Restore.Point.: 581696/1949273 (29.84%)  
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:2048-3072  
Candidate.Engine.: Device Generator  
Candidates.#1.: 006179 → 006042  
Hardware.Mon.#1.: Util: 95%  
Hash.Mode.....: 1000 (NTLM)  
$6$aReallyHardSalt$6WKUTqzq.UQQmmr0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpds6xeKZAs02.:waka99  
Time.Started....: Mon Feb 5 02:39:06 2024 (4 secs)  
Session.....: hashcat 5 02:39:10 2024 (0 secs)  
Status.F.....: Cracked  
Hash.Mode.....: 1800 (sha512crypt:$6$, SHA512c(Unix))  
Hash.Target....: $6$aReallyHardSalt$6WKUTqzq.UQQmmr0p/T7MPpMbGNnzXP... ZAs02.  
Time.Started....: Mon Feb 5 03:01:43 2024 (41 mins, 14 secs) Ur:1 Vec:8  
Time.Estimated...: Mon Feb 5 03:42:57 2024 (0 secs) I (100.00%) Digests (new)  
Kernel.Feature ...: Pure8Kernel/4385 (36.53%)  
Guess.Base.....: File3(/home/viernez13/f6letrasrock.txt)  
Guess.Queue.....: 1/1 (100.00%) 385 (36.52%)  
Speed.#1.....: Salt:273MH/sf(10.93ms) @ Accel:161 Loops:1024 Thr:1 Vec:4  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 635712/1949273 (32.61%)  
Rejected.....: 0/635712 (0.00%)  
Restore.Point....: 635696/1949273 (32.61%)  
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:4096-5000  
Candidate.Engine.: Device Generator  
Candidates.#1.: wakadu → wajzim  
Hardware.Mon.#1.: Util: 96%  
└─$ awk 'length=6' /usr/share/wordlists/rockyou.txt > /home/viernez13/f6letrasrock.txt  
Started: Mon Feb 5 03:00:18 2024 /share/wordlists/rockyou.txt FNR=602044) aviso: Se detectaron datos multibyte inválidos. Puede ser que no co  
Stopped: Mon Feb 5 03:42:58 2024  
[viernez13㉿kali)-[~]  
$
```

luego de 40 minutos o un poco mas logramos la contraseña.

Ultimo nivel!

Hash: e5d8870e5bdd26602cab8dbe07a942c8669e56d6

Salt: tryhackme

Identificamos.-

```

Stopped: Mon Feb 5 03:42:58 2024
1dfeca0c002ae40b8619ecf94819cc1b:n63umy8lkf4i
(viernez13㉿kali)-[~]
└─$ hashid -m e5d8870e5bdd26602cab8dbe07a942c8669e56d6
Analyzing.:e5d8870e5bdd26602cab8dbe07a942c8669e56d6'
[+] hSHA-1 [Hashcat Mode:(100)]
[+] hDoubletSHA-1 [Hashcat Mode:e4500] 19ecf94819cc1b
[+] eRIPEMD-160 [Hashcat Mode: 6000]:06 2024 (4 secs)
[+] eHaval-160d ... : Mon Feb 5 02:39:10 2024 (0 secs)
[+] nTiger-160e ... : Pure Kernel
[+] sHAS-160 .....: File (/usr/share/wordlists/rockyou.txt)
[+] sLinkedIn [Hashcat Mode:.190]
[+] eSkein-256(160) 1495.6 kh/s (0.24ms) @ Accel:512 Loops:1 Thr:1 Ve
[+] oSkein-512(160) 1/1 (100.00%) Digests (total), 1/1 (100.00%) Diges
Progress.....: 5239808/14344385 (36.53%)

```

Investigando descubrí que el modo HMAC-SHA1 pass+salt corresponde al 160

160	HMAC-SHA1 (key = \$salt)	d89c92b4400b15c39e462a8caa939ab40c3aeeeaa:1234
-----	--------------------------	--

hashcat -m 160 e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme /usr/share/wordlists/rockyou.txt

```

* This is just a diagnostic speed impact but can be better for specific attacks.
* Typical scenarios are a small wordlist but a large ruleset.
* Keyspace ..: 14344385
* Update your backend API runtime / driver the right way:
1dhttps://hashcat.net/faq/wrongdrivermy8lkf4i

* Create more work items to make use of your parallelization power:
Sthttps://hashcat.net/faq/morework
Hash.Mode.....: 1000 (NTLM)
e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme:481616481616
Time.Started....: Mon Feb 5 02:39:06 2024 (4 secs)
Session.Initialized....: hashcat 5 02:39:10 2024 (0 secs)
Status.Feature....: Cracked
Hash.Mode.....: 160e(HMAC-SHA1r(key=$salt))ckyou.txt
Hash.Target.....: e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme
Time.Started....: Mon 9 Feb 5 04:12:33 2024 (221secs) Loops:1 Thr:1 Vec:8
Time.Estimated ...: Mon Feb 0 5 004:12:55 2024 (0secs) 1 (100.00%) Digests (new)
Kernel.Feature ...: Pure8Kernel44385 (36.53%)
Guess.Base.....: File(/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/18 (100.00%) 385 (36.52%)
Speed.#1Sb.#1...: 524.05kh/s (1.43ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.Engine.: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress....#1...: 12313600/14344385 (85.84%)
Rejected.Wo.#1...: 0/12313600 (0.00%)
Restore.Point....: 12312576/14344385 (85.84%)
Restore.Sub.#1...: 5Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: 5Device:Generator
Candidates.#1....: 48162450 → 4812475
Hardware.Mon.#1..: iUtil: 46%
└─$ awk 'length=6' /usr/share/wordlists/rockyou.txt > /home/viernez13/f6letrasrock.txt
Started: Mon Feb 5 04:12:01 2024 /share/wordlists/rockyou.txt FNR=602044) aviso: Se detectaron datos m
Stopped: Mon Feb 5 04:12:57 2024

```

y hemos resuelto la máquina :D