



CENTRE UNIVERSITAIRE INFORMATIQUE

GESTION DES RISQUES, CYCLE DE VIE DE L'INFORMATION
ET HACKING ÉTHIQUE

Rapport practical - Hash cracking

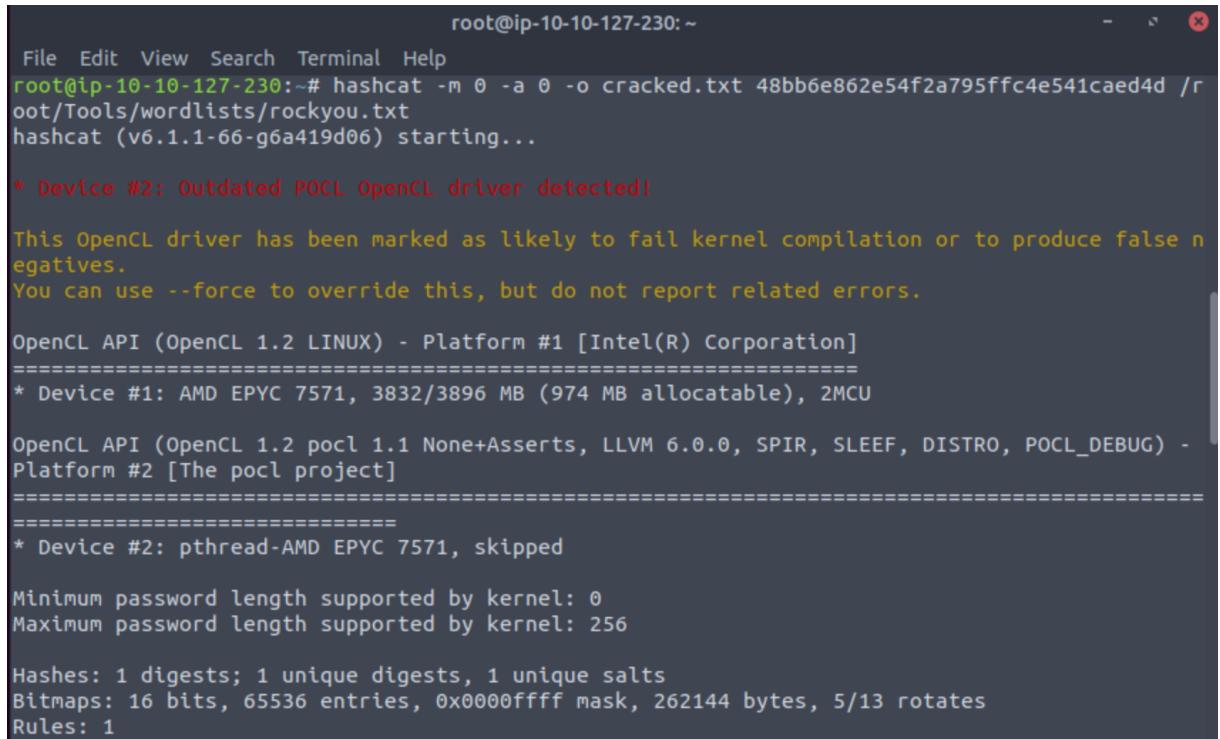
Étudiant :

Senou ronald ALOHOUTADE

1 level 1

1.1 48bb6e862e54f2a795ffc4e541caed4d

Pour casser le hash, je vais d'abord essayer de déterminer son type en utilisant un outil approprié, puis utiliser les paramètres correspondants avec Hashcat pour casser le hash. Dans ce cas, le hash est de type MD5, donc voici la commande que je vais utiliser pour tenter de casser le hash :



```
root@ip-10-10-127-230:~#
File Edit View Search Terminal Help
root@ip-10-10-127-230:~# hashcat -m 0 -a 0 -o cracked.txt 48bb6e862e54f2a795ffc4e541caed4d /r
oot/Tools/wordlists/rockyou.txt
hashcat (v6.1.1-66-g6a419d06) starting...

* Device #2: Outdated POCL OpenCL driver detected!

This OpenCL driver has been marked as likely to fail kernel compilation or to produce false negatives.
You can use --force to override this, but do not report related errors.

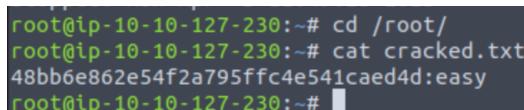
OpenCL API (OpenCL 1.2 LINUX) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: AMD EPYC 7571, 3832/3896 MB (974 MB allocatable), 2MCU

OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEP, DISTRO, POCL_DEBUG) -
Platform #2 [The pocl project]
=====
* Device #2: pthread-AMD EPYC 7571, skipped

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
```

J'ai utilisé l'outil Hashcat avec le fichier rockyou.txt pour casser le hash, et j'ai redirigé le résultat vers le fichier "cracked.txt".



```
root@ip-10-10-127-230:~# cd /root/
root@ip-10-10-127-230:~# cat cracked.txt
48bb6e862e54f2a795ffc4e541caed4d:easy
root@ip-10-10-127-230:~#
```

En analysant la capture, on peut constater que le mot de passe du hash est : "easy".

1.2 CBFDAC6008F9CAB4083784CBD1874F76618D2A97

J'ai utilisé la même méthode que pour le premier hash, mais cette fois-ci j'ai d'abord utilisé l'outil "hashid" pour déterminer le type de hash, qui est du type SHA-1.

```
root@ip-10-10-163-219:~#
File Edit View Search Terminal Help
root@ip-10-10-163-219:~# hashid -m 'CBFDAC6008F9CAB4083784CBD1874F76618D2A97'
Analyzing 'CBFDAC6008F9CAB4083784CBD1874F76618D2A97'
[+] SHA-1 [Hashcat Mode: 100]
[+] Double SHA-1 [Hashcat Mode: 4500]
[+] RIPEMD-160 [Hashcat Mode: 6000]
[+] Haval-160
[+] Tiger-160
[+] HAS-160
[+] LinkedIn [Hashcat Mode: 190]
[+] Skein-256(160)
[+] Skein-512(160)
root@ip-10-10-163-219:~# hashcat -m 100 -a 0 sha1.txt CBFDAC6008F9CAB4083784CBD1
874F76618D2A97 /root/Tools/wordlists/rockyou.txt
hashcat (v6.1.1-66-g6a419d06) starting...

CBFDAC6008F9CAB4083784CBD1874F76618D2A97: No such file or directory

Started: Mon Apr  3 13:13:22 2023
Stopped: Mon Apr  3 13:13:22 2023
root@ip-10-10-163-219:~# hashcat -m 100 -a 0 -o sha1.txt CBFDAC6008F9CAB4083784C
BD1874F76618D2A97 /root/Tools/wordlists/rockyou.txt
hashcat (v6.1.1-66-g6a419d06) starting...

* Device #2: Outdated POCL OpenCL driver detected!
```

```
root@ip-10-10-163-219:~# ls
Desktop      HashTag-master.zip  Postman  sha1.txt
Downloads    Instructions       Rooms    thinclient_drives
HashTag-master Pictures         Scripts  Tools
root@ip-10-10-163-219:~# cat sha1.txt
cbfdac6008f9cab4083784cbd1874f76618d2a97:password123
root@ip-10-10-163-219:~#
```

En analysant la capture, on peut constater que le mot de passe du hash est : "password123".

1.3 1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7

J'ai utilisé la même méthode que pour le hash précédent, mais cette fois-ci le type de hash est SHA-256.

```
root@ip-10-10-163-219:~# hashid -m '1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4
FC946683D7B336B63032'
Analyzing '1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032'
[+] Snefru-256
[+] SHA-256 [Hashcat Mode: 1400]
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94 [Hashcat Mode: 6900]
[+] GOST CryptoPro S-Box
[+] SHA3-256 [Hashcat Mode: 5000]
[+] Skein-256
[+] Skein-512(256)
root@ip-10-10-163-219:~#
```

```
root@ip-10-10-163-219:~#
File Edit View Search Terminal Help
* Keyspace...: 14344384

Session.....: hashcat
Status.....: Cracked
Hash.Name....: SHA2-256
Hash.Target...: 1c8bfe8f801d79745c4631d09fff36c82aa37fc4cce4fc946683d7b336b63032
Time.Started...: Mon Apr 3 13:26:22 2023 (1 sec)
Time.Estimated...: Mon Apr 3 13:26:23 2023 (0 secs)
Guess.Base....: File (/root/Tools/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 1114.1 kH/s (1.23ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 2048/14344384 (0.01%)
Rejected.....: 0/2048 (0.00%)
Restore.Point...: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: 123456 -> lovers1

Started: Mon Apr 3 13:26:01 2023
Stopped: Mon Apr 3 13:26:24 2023
root@ip-10-10-163-219:~# cat sha256.txt
1c8bfe8f801d79745c4631d09fff36c82aa37fc4cce4fc946683d7b336b63032:letmein
root@ip-10-10-163-219:~#
```

De la deuxième capture on constate que le mot de passe du hash est : "letmein".

1.4 2y12Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRo

J'ai utilisé la même méthode que pour le hash précédent, mais cette fois-ci le type de hash est Bcrypt. J'ai lancé la même commande pour casser le mot de passe, mais le processus affiche cette fois-ci une durée de 26 jours et 14 heures pour casser le mot de passe de ce hash.

```
root@ip-10-10-177-164:~# hashcat -a 0 -m 3200 '$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom' /  
root/Tools/wordlists/rockyou.txt  
hashcat (v6.1.1-66-g6a419d06) starting...
```

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s  
  
Session.....: hashcat  
Status.....: Running  
Hash.Name....: bcrypt $2*$, Blowfish (Unix)  
Hash.Target...: $2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX...8wsRom  
Time.Started...: Fri Apr 14 00:43:56 2023 (27 secs)  
Time.Estimated...: Wed May 10 15:00:05 2023 (26 days, 14 hours)  
Guess.Base....: File (/root/Tools/wordlists/rockyou.txt)  
Guess.Queue....: 1/1 (100.00%)  
Speed.#1.....: 6 H/s (9.86ms) @ Accel:16 Loops:8 Thr:1 Vec:8  
Recovered.....: 0/1 (0.00%) Digests  
Progress.....: 160/14344384 (0.00%)  
Rejected.....: 0/160 (0.00%)  
Restore.Point...: 160/14344384 (0.00%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:832-840  
Candidates.#1...: ginger -> november  
  
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>
```

Afin de réduire le temps nécessaire pour cracker le mot de passe, je vais filtrer le fichier "rockyou" en ne gardant que les mots de passe ayant une longueur de 4 caractères, puis rediriger les résultats vers un autre fichier.

```
root@ip-10-10-177-164:~# grep '^....$' /usr/share/wordlists/rockyou.txt > rockyou1.txt  
root@ip-10-10-177-164:~# hashcat -a 0 -m 3200 '$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom' /  
root/rockyou1.txt  
hashcat (v6.1.1-66-g6a419d06) starting...  
  
* Device #2: Outdated POCL OpenCL driver detected!  
  
This OpenCL driver has been marked as likely to fail kernel compilation or to produce false negatives.  
You can use --force to override this, but do not report related errors.  
  
OpenCL API (OpenCL 1.2 LINUX) - Platform #1 [Intel(R) Corporation]  
=====  
* Device #1: AMD EPYC 7571, 3832/3896 MB (974 MB allocatable), 2MCU  
  
OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEF, DISTRO, POCL DEBUG) - Platform #2 [The
```

```
$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom:bleh  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Name....: bcrypt $2*$, Blowfish (Unix)  
Hash.Target...: $2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX...8wsRom  
Time.Started...: Fri Apr 14 00:46:32 2023 (1 min, 46 secs)  
Time.Estimated...: Fri Apr 14 00:48:18 2023 (0 secs)  
Guess.Base....: File (/root/rockyou1.txt)  
Guess.Queue....: 1/1 (100.00%)  
Speed.#1.....: 6 H/s (10.01ms) @ Accel:4 Loops:32 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests  
Progress.....: 656/18152 (3.61%)  
Rejected.....: 0/656 (0.00%)  
Restore.Point...: 648/18152 (3.57%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4064-4096  
Candidates.#1...: bleh -> 2123  
  
Started: Fri Apr 14 00:45:44 2023  
Stopped: Fri Apr 14 00:48:20 2023  
root@ip-10-10-177-164:~#
```

Grâce à cette méthode, j'ai pu réduire le temps nécessaire pour casser le hash, et le

mot de passe a finalement été trouvé : "bleh".

1.5 279412f945939ba78ce0758d3fd83daa

Pour ce hash qui est du type MD4, j'ai utilisé un outil en ligne parce que je n'arrivais pas à le casser avec Hashcat.

```
root@ip-10-10-39-98: ~
File Edit View Search Terminal Help
* Runtime...: 10 secs

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Name....: MD4
Hash.Target....: 279412f945939ba78ce0758d3fd83daa
Time.Started....: Fri Apr 14 19:05:13 2023 (6 secs)
Time.Estimated...: Fri Apr 14 19:05:19 2023 (0 secs)
Guess.Base.....: File (/root/Tools/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2554.2 kH/s (0.36ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests
Progress.....: 14344384/14344384 (100.00%)
Rejected.....: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[206b6d3831303838] -> $HEX[042a0337c2a156616d6f732103]

Started: Fri Apr 14 19:04:16 2023
Stopped: Fri Apr 14 19:05:21 2023
root@ip-10-10-39-98:~# hashcat -a 0 -m 900 '279412f945939ba78ce0758d3fd83daa' /root/Tools/wordlists/rockyou.txt
```

Enter up to 20 non-salted hashes, one per line:

279412f945939ba78ce0758d3fd83daa

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
279412f945939ba78ce0758d3fd83daa	md4	Eternity22

En analysant la capture, on peut constater que le mot de passe du hash est : "Eternity22"

2 Level 2

2.1 F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F6

J'ai suivi la même démarche à celle de la partie 1.

```
root@ip-10-10-235-63:~# hashid -m 'F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85'
Analyzing 'F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85'
[+] Snelru-256
[+] SHA-256 [Hashcat Mode: 1400]
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94 [Hashcat Mode: 6900]
[+] GOST CryptoPro S-Box
[+] SHA3-256 [Hashcat Mode: 5000]
[+] Skein-256
[+] Skein-512(256)
root@ip-10-10-235-63:~# hashcat -m 1400 'F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85' /root/Tools/wordlists/rockyou.txt
hashcat (v6.1.1-66-g6a419d06) starting...

* Device #2: Outdated POCL OpenCL driver detected!

This OpenCL driver has been marked as likely to fail kernel compilation or to produce false negatives.
You can use --force to override this, but do not report related errors.

OpenCL API (OpenCL 1.2 LINUX) - Platform #1 [Intel(R) Corporation]
=====
```

```
f09edcb1fcef6dfb23dc3505a882655ff77375ed8aa2d1c13f640fccc2d0c85:paule

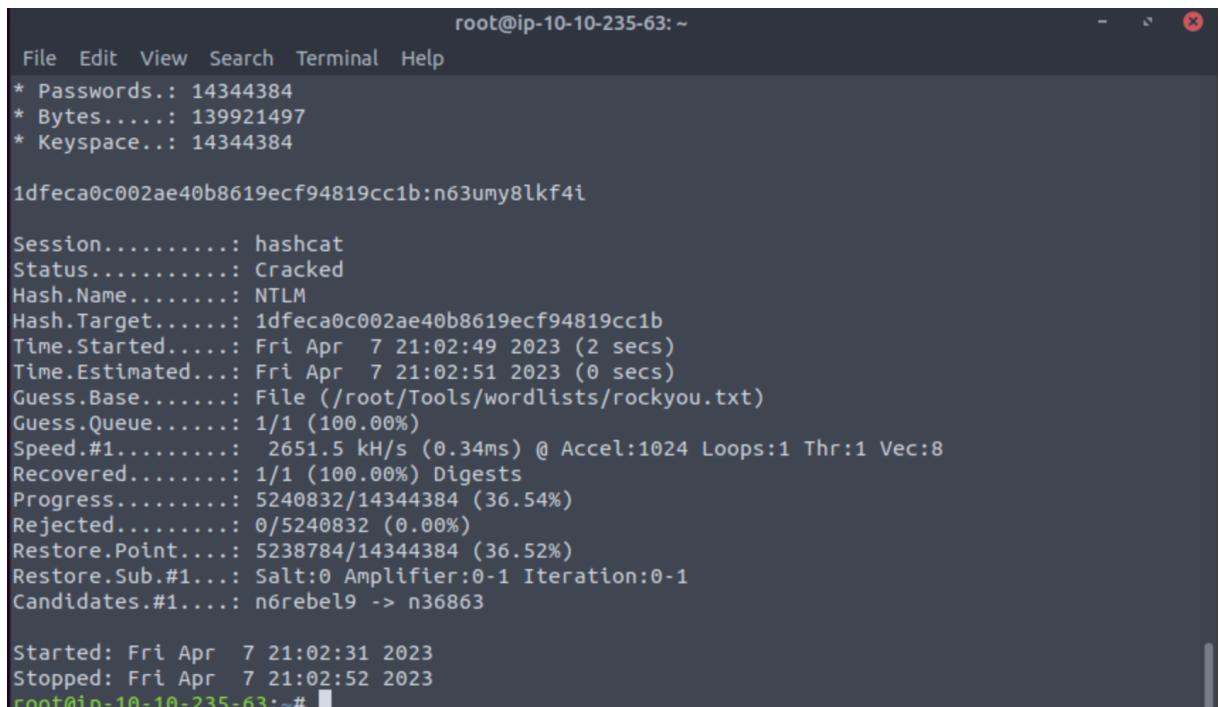
Session.....: hashcat
Status.....: Cracked
Hash.Name....: SHA2-256
Hash.Target...: f09edcb1fcef6dfb23dc3505a882655ff77375ed8aa2d1c13f...2d0c85
Time.Started...: Fri Apr 7 20:58:50 2023 (0 secs)
Time.Estimated...: Fri Apr 7 20:58:50 2023 (0 secs)
Guess.Base....: File (/root/Tools/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 1188.5 kH/s (1.18ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 79872/14344384 (0.56%)
Rejected.....: 0/79872 (0.00%)
Restore.Point...: 77824/14344384 (0.54%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: superhot -> Bryan

Started: Fri Apr 7 20:58:32 2023
Stopped: Fri Apr 7 20:58:51 2023
root@ip-10-10-235-63:~#
```

En analysant la capture, on peut constater que le mot de passe du hash est : "paule".

2.2 1DFECA0C002AE40B8619ECF94819CC1B

J'ai utilisé la même méthode, sauf qu'ici on m'a donné le type de hash. J'ai juste cherché le mode de hash pour pouvoir exécuter la commande hashcat.



```
root@ip-10-10-235-63: ~
File Edit View Search Terminal Help
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace...: 14344384

1dfeca0c002ae40b8619ecf94819cc1b:n63umy8lkf4i

Session.....: hashcat
Status.....: Cracked
Hash.Name....: NTLM
Hash.Target....: 1dfeca0c002ae40b8619ecf94819cc1b
Time.Started....: Fri Apr 7 21:02:49 2023 (2 secs)
Time.Estimated....: Fri Apr 7 21:02:51 2023 (0 secs)
Guess.Base.....: File (/root/Tools/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2651.5 kH/s (0.34ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 5240832/14344384 (36.54%)
Rejected.....: 0/5240832 (0.00%)
Restore.Point....: 5238784/14344384 (36.52%)
Restore.Sub.#1....: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: n6rebel9 -> n36863

Started: Fri Apr 7 21:02:31 2023
Stopped: Fri Apr 7 21:02:52 2023
root@ip-10-10-235-63:~#
```

De la capture on constate que le mot de passe du hash est : "n63umy8lkf4i".

2.3 6aReallyHardSalt6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi⁴ / Salt : aReallyHardSalt

j'ai procédé à la même démarche avec celle du 04 ième hash du level 1 pour vitre casser le hash.

```
root@ip-10-10-90-100:~  
File Edit View Search Terminal Help  
Stopped: Thu Apr 13 23:48:50 2023  
root@ip-10-10-90-100:~# grep '^.....$' /usr/share/wordlists/rockyou.txt > rocky  
ou-6.txt  
root@ip-10-10-90-100:~# hashcat -a 0 -m 1800 '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMp djS6xeKZAs02.' /root/r  
ockyou-6.txt  
hashcat (v6.1.1-66-g6a419d06) starting...  
  
* Device #2: Outdated POCL OpenCL driver detected!  
  
This OpenCL driver has been marked as likely to fail kernel compilation or to pr  
oduce false negatives.  
You can use --force to override this, but do not report related errors.  
  
OpenCL API (OpenCL 1.2 LINUX) - Platform #1 [Intel(R) Corporation]  
=====  
* Device #1: AMD EPYC 7571, 3832/3896 MB (974 MB allocatable), 2MCU  
  
OpenCL API (OpenCL 1.2 pocl 1.1 None+Asserts, LLVM 6.0.0, SPIR, SLEEF, DISTRO, P  
OCL_DEBUG) - Platform #2 [The pocl project]  
=====  
=====  
* Device #2: pthread-AMD EPYC 7571, skipped
```

```
root@ip-10-10-90-100:~  
File Edit View Search Terminal Help  
Candidates.#1....: yaypee -> yayill  
  
$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41  
BqMhSrHVXgMp djS6xeKZAs02.:waka99  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Name....: sha512crypt $6$, SHA512 (Unix)  
Hash.Target....: $6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXP...ZAs02.  
Time.Started....: Thu Apr 13 23:50:54 2023 (31 mins, 35 secs)  
Time.Estimated...: Fri Apr 14 00:22:29 2023 (0 secs)  
Guess.Base.....: File (/root/rockyou-6.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 336 H/s (9.30ms) @ Accel:32 Loops:256 Thr:1 Vec:4  
Recovered.....: 1/1 (100.00%) Digests  
Progress.....: 635712/1949232 (32.61%)  
Rejected.....: 0/635712 (0.00%)  
Restore.Point....: 635648/1949232 (32.61%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000  
Candidates.#1....: wakero -> wajhik  
  
Started: Thu Apr 13 23:50:52 2023  
Stopped: Fri Apr 14 00:22:30 2023  
root@ip-10-10-90-100:~#
```

En analysant la capture, on peut constaterDe la deuxième capture on constate que le

mot de passe du hash est : "waka99".

2.4 e5d8870e5bdd26602cab8dbe07a942c8669e56d6 :tryhackme

J'ai utilisé la même méthode, sauf qu'ici on m'a donné le salt. Pour cela, j'ai créé un fichier dans lequel j'ai copié le hash suivi du salt, en les séparant par un " :". Ensuite, j'ai lancé la commande hashcat sur ce fichier.

```
root@ip-10-10-173-247: ~
File Edit View Search Terminal Help
* Bytes.....: 139921497
* Keyspace...: 14344384

e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme:481616481616

Session.....: hashcat
Status.....: Cracked
Hash.Name....: HMAC-SHA1 (key = $salt)
Hash.Target...: e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme
Time.Started...: Sat Apr  8 11:46:33 2023 (11 secs)
Time.Estimated.: Sat Apr  8 11:46:44 2023 (0 secs)
Guess.Base....: File (/root/Tools/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 1094.8 kH/s (1.43ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 12314624/14344384 (85.85%)
Rejected.....: 0/12314624 (0.00%)
Restore.Point...: 12312576/14344384 (85.84%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: 48162440 -> 4811011016

Started: Sat Apr  8 11:46:15 2023
Stopped: Sat Apr  8 11:46:45 2023
root@ip-10-10-173-247:~#
```

En analysant la capture, on peut constater que le mot de passe correspondant au hash est : "481616481616".

