
TryHackMe - Crack the hash Room Writeup

Motasm Elsayed



Contents

Introduction	2
Online Hash Cracking Tools	3
Task 1: Level 1 Hashes	3
Task 2: Level 2 Hashes	5
Level 2 - Hash 1	6
Level 2 - Hash 2	7
Level 2 - Hash 3	9
Level 2 - Hash 4	10
Conclusion	12



Figure 1: Challenge official cover

Challenge description: This challenge tests your knowledge of identifying and analyzing password hashes, cracking password hashes using online tools, and conducting password-dictionary attacks using tools such as Hashcat and John The Ripper.

Challenge category: Cryptography - Password Cracking - Password Dictionary Attacks

Challenge link: [Crack the hash](#)

Introduction

Mastering the craft of conducting password-cracking attacks with diverse tools and techniques is a paramount skill for every penetration tester. Beyond mere unauthorized access, this proficiency is a linchpin in understanding and fortifying digital security. It serves as a crucial dimension of a penetration tester's toolkit, allowing them to uncover vulnerabilities within systems, assess the robustness of cryptographic defenses, and ultimately enhance the overall resilience of an organization's cybersecurity posture. In the dynamic landscape of cyber threats, the ability to proficiently navigate and decrypt passwords is not just a tactical advantage but a strategic imperative, reinforcing the pentester's capability to identify and mitigate potential points of exploitation. So let's delve into these challenge questions together!

Online Hash Cracking Tools

When it comes to cracking password hashes in the hope of retrieving the password value of the hash, it's a good practice to start by making use of **online hash cracking tools** as these tools have massive pre-computed lookup tables to crack password hashes and it's more likely to find the hash value, if it's there, in less than a second, on the other hand, using tools like **Hashcat** or **John The Ripper** to crack the password hash using brute-force attacks or even password-dictionary attacks may take longer.

Task 1: Level 1 Hashes

As we said above, it's a good practice to first look for the hash values on online hash-cracking tools or databases, let's try to crack the hash values in Task 1.

There are a lot of online hash-cracking tools out there we can use, but to name a few, the following websites are some of the most popular ones:

- <https://crackstation.net/>
- <https://hashes.com/en/decrypt/hash>
- <https://md5hashing.net/>
- <https://www.onlinehashcrack.com/>

Throughout this writeup, we are gonna use <https://crackstation.net/> and <https://hashes.com/en/decrypt/hash>.

Well, let's open them and then copy and paste all the hash values in task 1, but make sure to write one hash per line.

CrackStation

Defuse.ca · Twitter

CrackStation ▾ Password Hashing Security ▾ Defuse Security ▾

Free Password Hash Cracker

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

```
48bb6e862e54f2a795ffc4e541caed4d
C8FDAC6008F9CAB4083784C8D1874F76618D2A97
1C8BF8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D78336B63032
$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom
279412f945939ba78ce0758d3fd83daa
```

☐ I'm not a robot
[Privacy](#) · [Terms](#)

Crack Hashes

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
48bb6e862e54f2a795ffc4e541caed4d	md5	easy
C8FDAC6008F9CAB4083784C8D1874F76618D2A97	sha1	password123
1C8BF8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D78336B63032	sha256	letmein
\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom	Unknown	Unrecognized hash format.
279412f945939ba78ce0758d3fd83daa	md4	Eternity22

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

[Download CrackStation's Wordlist](#)

Figure 2: Cracking Level 1 hashes using CrackStation

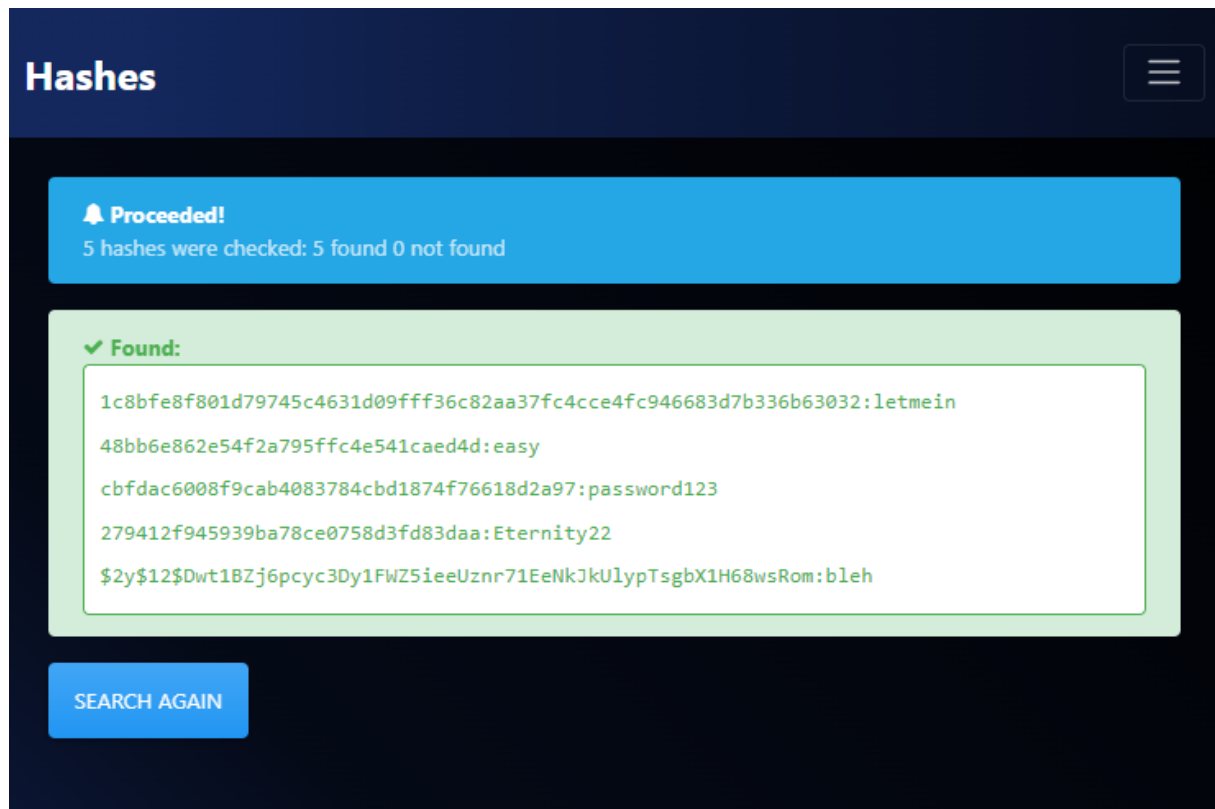


Figure 3: Cracking Level 1 hashes using Hashes.com

Well done! As you see, we retrieved all the passwords by using online hash-cracking tools! You may also have noticed that CrackStation could not retrieve the password of the hash number 4, but we were able to retrieve it using hashes.com. So keep in mind to try different tools.

Task 2: Level 2 Hashes

In task 2 we will not use online hash cracking tools just to get familiar with the manual process of cracking hashes and start using tools such as **Hash-Identifier** to identify hash type and **Hashcat** to conduct password-dictionary attacks. So let's get started!

The following are the steps we will follow to find the password from its hash value using Hashcat:

1. Identify the hash type using tools such as Hash-Identifier, Hashid, or any online hash identifier tool
2. Find the corresponding Hashcat "Hash-Mode" value from the following website <https://hashcat.net/wiki/doku.p> to use it when running **Hashcat**

3. Save the hash value in a text file
4. Run **Hashcat** to conduct a password-dictionary attack

So keep these steps in mind as we will keep using them till the end of this writeup!

Level 2 - Hash 1

1. Identifying the hash using the **Hash-Identifier** tool

```
HASH: F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85

Possible Hashs:
[+] SHA-256
[+] Haval-256
```

Figure 4: Identifying the hash using Hash-Identifier tool

2. Finding the “Hash-Mode” value

From the following website “https://hashcat.net/wiki/doku.php?id=example_hashes”, the value is 1400

3. Saving the hash value in a text file using the following command:

```
1 $ echo -n '
    F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85' >
    hash.txt
```

4. Running **Hashcat** using the following command:

```
1 $ hashcat -m 1400 -d 1 hash.txt /usr/share/wordlists/rockyou.txt
```

```
f09edcb1fcefcb6dfb23dc3505a882655ff77375ed8aa2d1c13f640fccc2d0c85:paule

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: f09edcb1fcefcb6dfb23dc3505a882655ff77375ed8aa2d1c13f...2d0c85
Time.Started.....: Sun Mar  3 12:17:27 2024 (1 sec)
Time.Estimated...: Sun Mar  3 12:17:28 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 35854.2 kH/s (3.18ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 1310720/14344384 (9.14%)
Rejected.....: 0/1310720 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> saytown
Hardware.Mon.#1..: Temp: 46c Util: 43% Core:1815MHz Mem:6100MHz Bus:8

Started: Sun Mar  3 12:17:22 2024
Stopped: Sun Mar  3 12:17:28 2024
```

Figure 5: Cracked Password

Level 2 - Hash 2

1. Identifying the hash using https://hashes.com/en/tools/hash_identifier

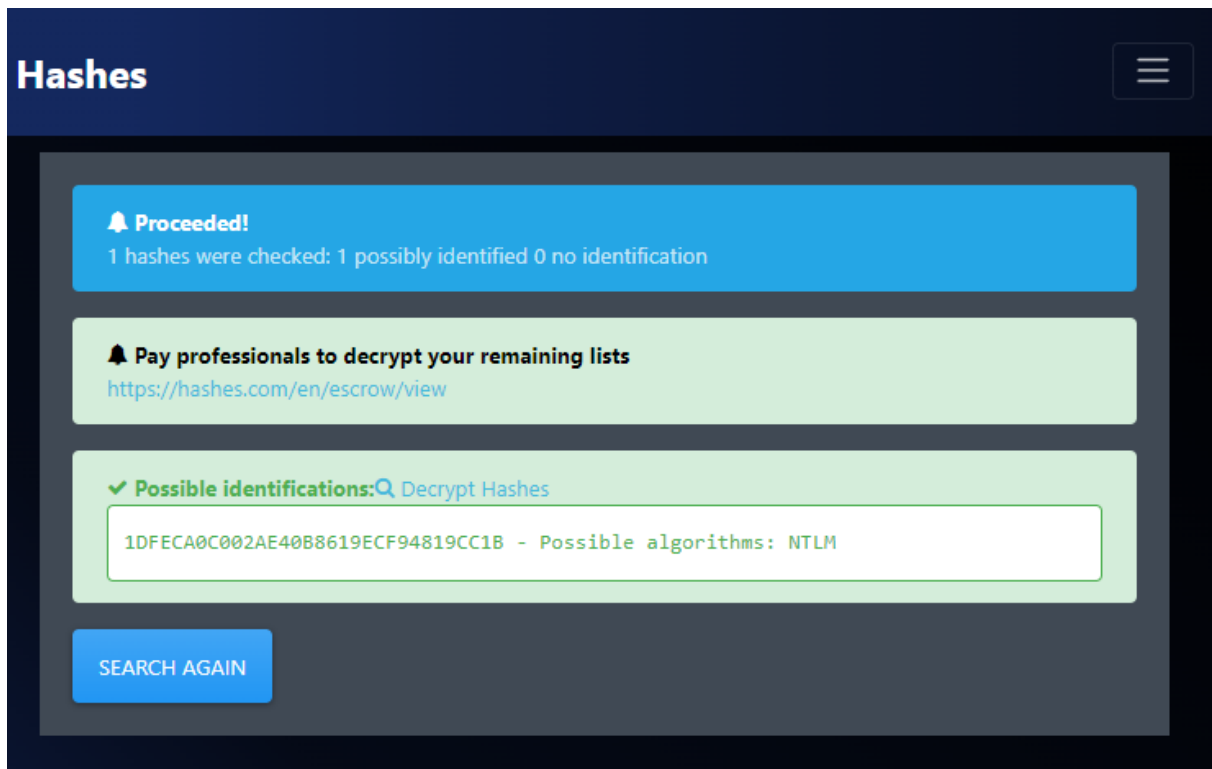


Figure 6: Identifying the hash using Hashes.com tool

2. Finding the “Hash-Mode” value

From the following website “https://hashcat.net/wiki/doku.php?id=example_hashes”, the value is 1000

3. Saving the hash value in a text file using the following command:

```
1 $ echo -n '1DFECA0C002AE40B8619ECF94819CC1B' > hash.txt
```

4. Running **Hashcat** using the following command:

```
1 $ hashcat -m 1000 -d 1 hash.txt /usr/share/wordlists/rockyou.txt
```

```
1dfeca0c002ae40b8619ecf94819cc1b:n63umy8lkf4i

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: 1dfeca0c002ae40b8619ecf94819cc1b
Time.Started.....: Sun Mar  3 12:22:59 2024 (1 sec)
Time.Estimated...: Sun Mar  3 12:23:00 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 15681.8 kH/s (3.21ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 5242880/14344384 (36.55%)
Rejected.....: 0/5242880 (0.00%)
Restore.Point....: 3932160/14344384 (27.41%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: seaford12 -> nlckos
Hardware.Mon.#1..: Temp: 47c Util: 38% Core:1875MHz Mem:6100MHz Bus:8

Started: Sun Mar  3 12:22:54 2024
Stopped: Sun Mar  3 12:23:00 2024
```

Figure 7: Cracked Password

Level 2 - Hash 3

1. Identifying the hash using https://hashes.com/en/tools/hash_identifier

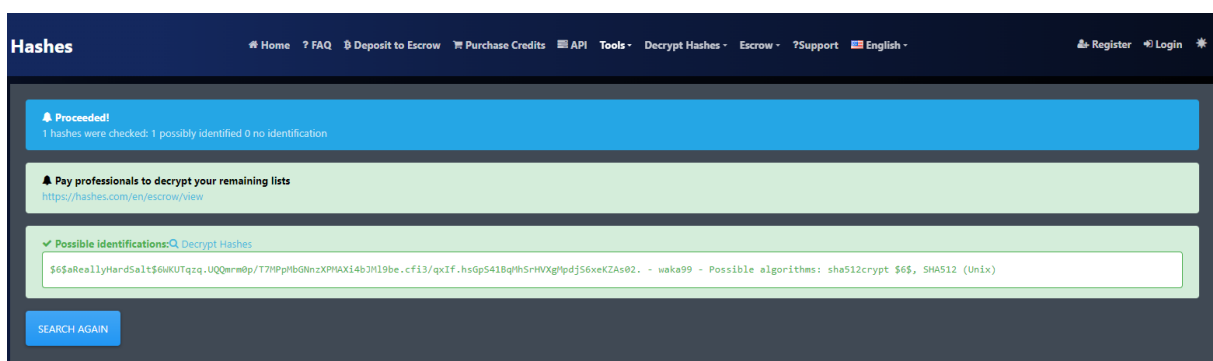


Figure 8: Identifying the hash using Hashes.com tool

2. Finding the “Hash-Mode” value

From the following website “https://hashcat.net/wiki/doku.php?id=example_hashes”, the value is 1800

3. Saving the hash value in a text file using the following command:

```
1 $ echo -n '$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/
    T7MPpMbGNnzXPMAXi4bJML9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.
    ' > hash.txt
```

4. Running **Hashcat** using the following command:

```
1 $ hashcat -m 1800 -d 1 hash.txt /usr/share/wordlists/rockyou.txt
```

```
$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJML9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.:waka99

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target.....: $6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPM...ZAs02.
Time.Started.....: Sun Mar  3 12:27:06 2024 (1 min, 4 secs)
Time.Estimated...: Sun Mar  3 12:28:10 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 44876 H/s (8.75ms) @ Accel:512 Loops:64 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 2850816/14344384 (19.87%)
Rejected.....: 0/2850816 (0.00%)
Restore.Point....: 2818048/14344384 (19.65%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1...: wardreen4 -> vs0924
Hardware.Mon.#1..: Temp: 71c Util: 99% Core:1957MHz Mem:6100MHz Bus:8

Started: Sun Mar  3 12:26:51 2024
Stopped: Sun Mar  3 12:28:11 2024
```

Figure 9: Cracked Password

Level 2 - Hash 4

1. Identifying the hash using the **Hash-Identifier** tool

```
HASH: e5d8870e5bdd26602cab8dbe07a942c8669e56d6 hash.txt
Possible Hashs: 00 -d 1 hash.txt rockyou.txt
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

Figure 10: Identifying the hash using Hash-Identifier tool

2. Finding the “Hash-Mode” value

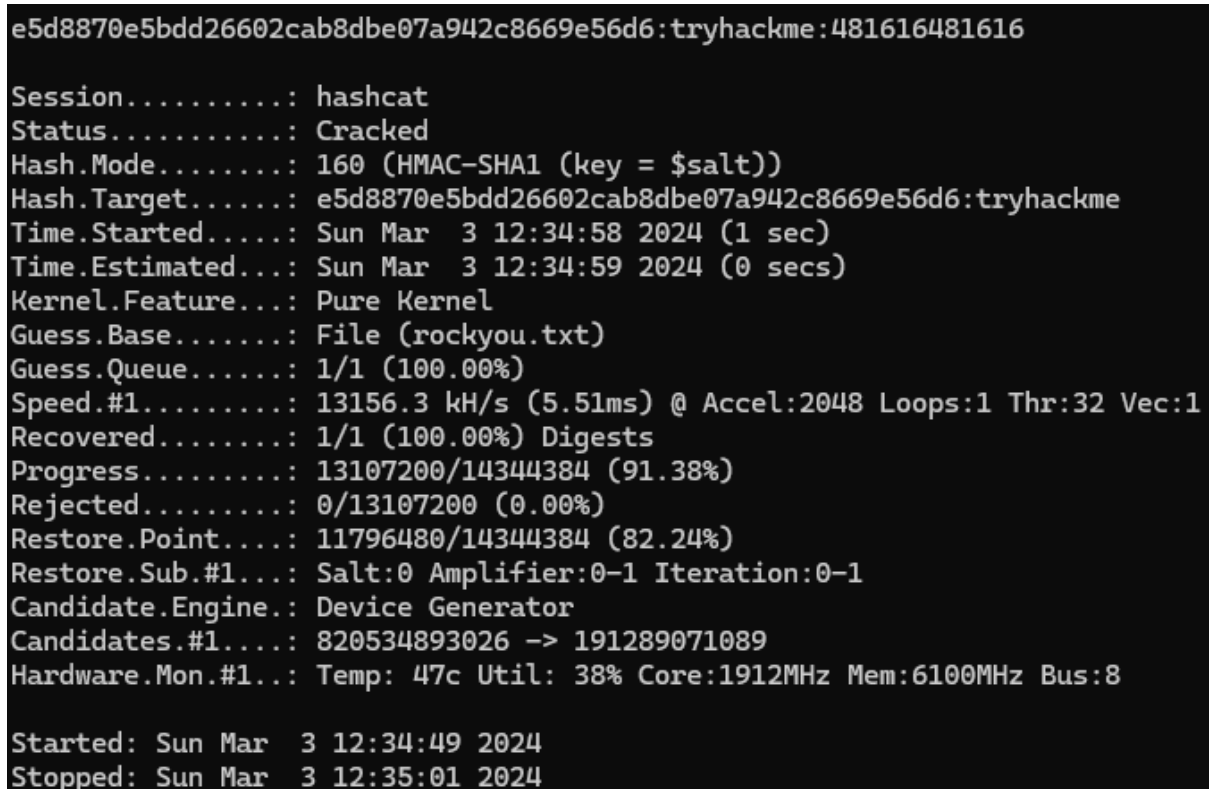
After trying different “Hash-Mode” values but in fail, we used the provided hint and after finding that the right hash type is “HMAC-SHA1” then from the following website “https://hashcat.net/wiki/doku.php?id=example_hashes”, the value is 160

3. Saving the hash value with its salt “tryhackme” in a text file using the following command:

```
1 $ echo -n 'e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme' > hash.txt
```

4. Running **Hashcat** using the following command:

```
1 $ hashcat -m 160 -d 1 hash.txt /usr/share/wordlists/rockyou.txt
```



```
e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme:481616481616
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 160 (HMAC-SHA1 (key = $salt))
Hash.Target.....: e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme
Time.Started.....: Sun Mar 3 12:34:58 2024 (1 sec)
Time.Estimated...: Sun Mar 3 12:34:59 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 13156.3 kH/s (5.51ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 13107200/14344384 (91.38%)
Rejected.....: 0/13107200 (0.00%)
Restore.Point....: 11796480/14344384 (82.24%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 820534893026 -> 191289071089
Hardware.Mon.#1..: Temp: 47c Util: 38% Core:1912MHz Mem:6100MHz Bus:8

Started: Sun Mar 3 12:34:49 2024
Stopped: Sun Mar 3 12:35:01 2024
```

Figure 11: Cracked Password

Note: the `-d 1` option in the hashcat command is to run **Hashcat** using our GPU as it's always faster than using the CPU, so if you have a powerful dedicated GPU use it instead of your CPU.

Additional note: If you face any problem using your GPU with **Hashcat**, check out the following video from Nvidia as it will help you a lot in solving this problem. https://www.youtube.com/watch?v=JaHVsZa2jTc&ab_char

Conclusion

In conclusion, I hope this walkthrough has been informative and shed light on our thought processes, strategies, and the techniques used to tackle each task. CTFs are not just about competition; they're about learning, challenging yourself and your knowledge, and getting hands-on experience through applying your theoretical knowledge.