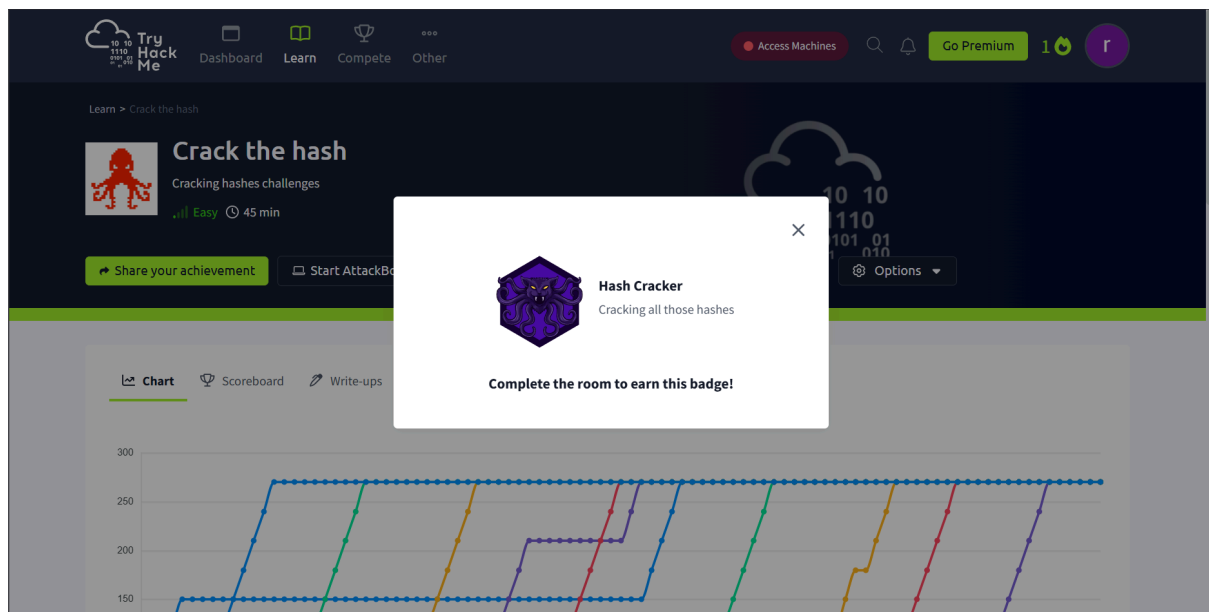


# TASK 1 - TryHackMe.

I've completed the Crack the Hash room in the TryHackMe as part of the CyberSecurity Bootcamp.

During the cracking of hashes I've faced many difficulties. I have beginner level experience in this field. I knew about the tool hashcat, but had to do a quick google search and chat gpt to understand how it works.



This is the Badge I got after completing this room.

Here is what i did :

## 1. Understand what encryption algorithm is used in the hash.

For that i had to use the hashid command and [hashes.com](https://hashes.com) to confirm its hash type.

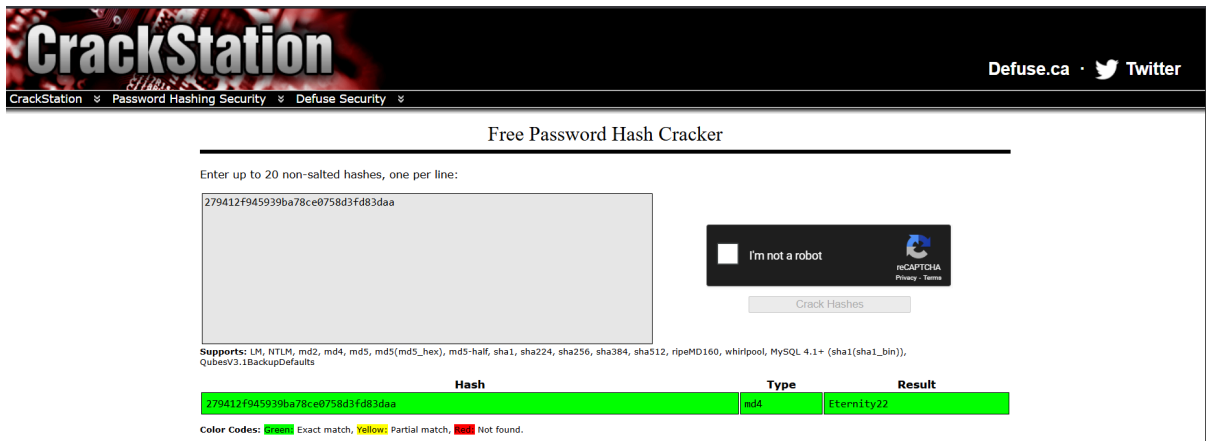
## 2.Start brute forcing.

After I got the hash type, I used the correct command for hashcat.

Eg: hashcat -m 0 hash.txt rockyou.txt

-m is for specifying the hash type , 0 is for MD5

But the twist is some of the passwords are not available in rockyou.txt. So I had to use some online sites such as [crackstation.net](https://crackstation.net) , [hashes.com](https://hashes.com) to crack those. Those were hashes given in the task 1



For task 2 of Crack the Hash , they give me a hint that all passwords are available in rockyou.txt and since some of them are salted hashes use a local machine to crack those. In those one specific hash took me more time. It was the sha512crypt algorithm, I had to rely on some online guide to understand why it took time and confusion. And guess what? They also had the same confusion at first. But anyways I managed to crack it last.

```

$ hashcat -m 1000 1DFECA0C002AE40B8619ECF94819CC1B /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #
* Device #1: cpu-penryn-12th Gen Intel(R) Core(TM) i7-12650H, 1438/2941 MB (512 MB allocatable), 2MCU

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

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

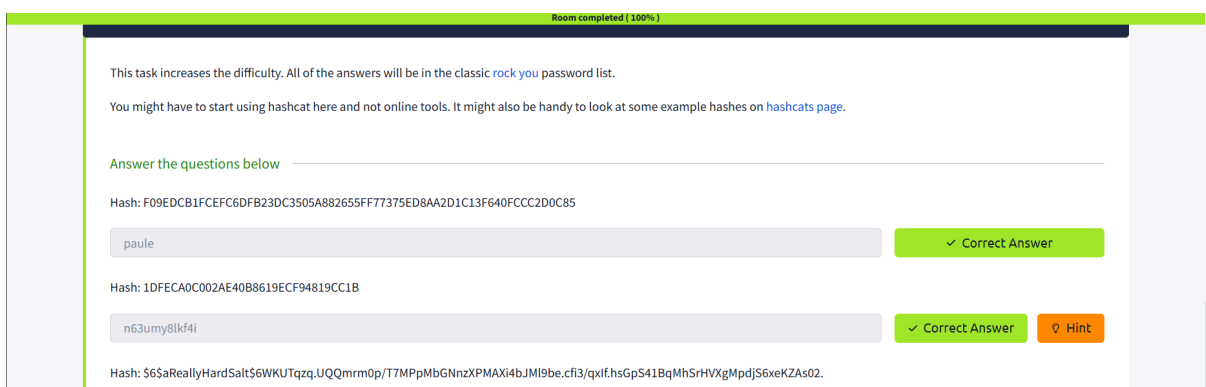
Started: Sun Jul 13 06:58:53 2025
Stopped: Sun Jul 13 06:58:53 2025

(kali@kali)-[~]
$ hashcat -m 1000 1DFECA0C002AE40B8619ECF94819CC1B /usr/share/wordlists/rockyou.txt --show
1dfeca0c002ae40b8619ecf94819cc1b:n63umy8l4i

```

### 3. Enter the password and submit it.

After I submitted all the passwords I got the badge.



And that's how I completed this TryHackMe room . I was so happy to finish this task of this bootcamp, and really excited to see what's more to offer in this bootcamp.

THE END.