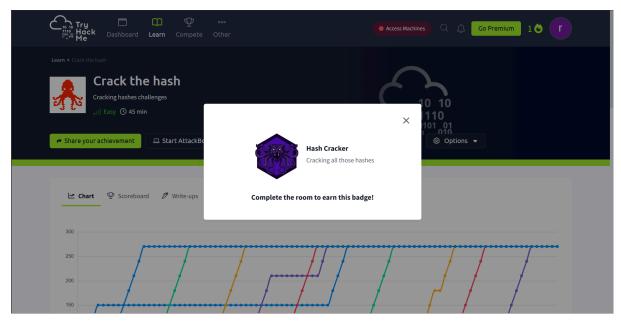
TASK 1 - TryHackMe.

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 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 <u>crackstation.net</u>, <u>hashes.com</u> to crack those. Those were hashes given in the task 1

CrackStation CrackStation * Password Hashing Security * Defuse Security *		Defuse	e.ca · 🏏 Twitter
Free Password Hash	Cracker		
Enter up to 20 non-salted hashes, one per line:			
279412f945939ba78ce8758d3fd83daa	I'm not a robot Crack Hashes	POZATOJA Prisey- Tems	
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha QubesV3.1BackupDefaults			
Hash 279412f945939ba78ce8758d3fd83daa	Type md4 Eternit	Result ty22	
Color Codes: Green: Exact match, Yellow: Partial match, Mot found.			

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:n63umy8lkf4i
```

3. Enter the password and submit it.

After I submitted all the passwords I got the badge.

Room completed (100%)		
This task increases the difficulty. All of the answers will be in the classic rock you password list.		
You might have to start using hashcat here and not online tools. It might also be handy to look at some example hashes on hashcats page.		
Answer the questions below		
Hash: F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85		
paule	✓ Correct Answer	
Hash: 1DFECA0C002AE40B8619ECF94819CC1B		
n63umy8lkf4i	✓ Correct Answer	♥ Hint
Hash: \$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxlf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.		

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.