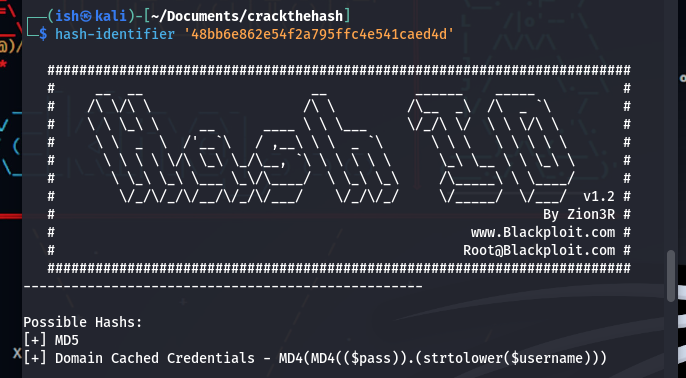
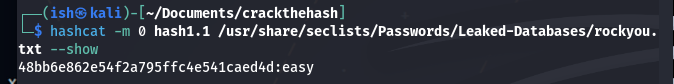
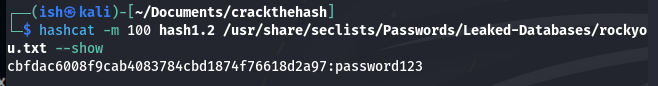
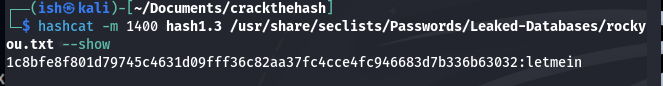
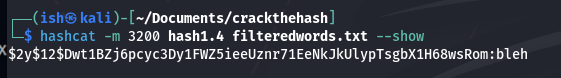
Crack the hash

[Room Link](https://tryhackme.com/room/crackthehash)

Part 1:

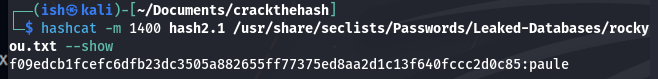
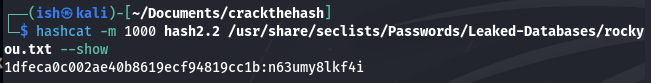
1. 48bb6e862e54f2a795ffc4e541caed4d
   1. The first step, find out what kind of hash this is
   2. Use hashid-m
      1. A computer screen with white text

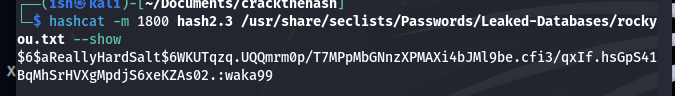
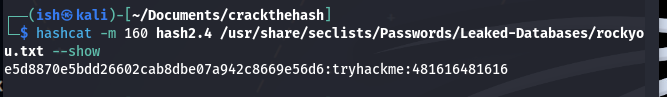
         Description automatically generated
   3. Use hash-identifier just to be sure
      1. 
   4. Both say it could be MD5
      1. Hint: hashid -m tells you the hashcat extension
   5. Command: hashcat -m 0 hash1.1 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt –show
      1. 
      2. Correct Answer = easy
2. CBFDAC6008F9CAB4083784CBD1874F76618D2A97
   1. Same process as before, use both hashid-m and hash-identifier
      1. Hint: hash-identifier doesn’t use files like hashid -m
   2. We find out the hash is SHA-1
   3. Command: hashcat -m 100 hash1.2 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt --show
      1. 
      2. Correct Answer: password123
3. 1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032
   1. Hashid-m and hash-identifier both indicate that this is a SHA-256 hash
   2. Command used: hashcat -m 1400 hash1.3 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt --show
      1. 
      2. Correct Answer: letmein
4. $2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom
   1. Hash-identifier cam up with nothing and hashid -m said it could either be blowfish(openbsd) or bcrypt, both have the same extension
   2. The initial command I ran used the entire rockyou wordlist, it said it was going to take 12 days to run, I was not doing that
   3. If you look at the hint it says that the cracked hash is 4 characters long. In seclists there is a wordlist called 1-4\_all\_letters\_a-z.txt, running this takes significantly less time
   4. However, it takes like 10 hours to do. Enter the grep -E '^[a-zA-Z]{4}$' /usr/shares/seclists/Fuzzing/1-4\_all\_letters\_a-z.txt > filteredwords.txt
   5. This limits it to just 4 letters
   6. Now we run the command hashcat -m 3200 hash1.4 filteredwords.txt
      1. A computer screen shot of a computer program

         Description automatically generated
      2. 
      3. Correct Answer: bleh
      4. See, much less time 😉, didn’t even take that long.
5. 279412f945939ba78ce0758d3fd83daa
   1. This is an MD4 hash
   2. A screenshot of a computer

      Description automatically generated
      1. The hint said it was an MD4 hash, however the rockyou list was exhausted
         1. Command: hashcat -m 900 hash1.5 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
      2. I then ran the hash through a website called [crackstation](https://crackstation.net/), it was able to crack it
      3. Correct answer: Eternity22

Part 2:

1. F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85
   1. Hash is SHA-256
   2. Command used: hashcat -m 1400 hash2.1 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
      1. 
      2. Correct Answer: paule
2. 1DFECA0C002AE40B8619ECF94819CC1B
   1. I was unsure due to the inconsistent results from both hashid -m and hash-identifier
      1. The hint says that it is an ntlm hash
   2. Command used: hashcat -m 1000 hash2.2 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
      1. 
      2. Correct Answer: n63umy8lkf4i
3. $6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.
   1. Hashid -m says it is a SHA-512 Crypt, however I wanted to be sure so I went to the [hashcat wiki for example hashes](https://hashcat.net/wiki/doku.php?id=example_hashes).
   2. Command used: hashcat -m 1800 hash2.3 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
      1. A computer screen shot of a computer

         Description automatically generated
      2. 
      3. Correct Answer: waka99
4. e5d8870e5bdd26602cab8dbe07a942c8669e56d6 Salt: tryhackme
   1. Here the salt isn’t included in the hash already as it was in the previous problem
   2. This is the format to use when placing in txt file: e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme
   3. Here I had to use the wiki again to find out the hash format again
      1. HMAC-SHA1 (key = $salt) This is the one I found to be the closest
   4. Command used: hashcat -m 160 hash2.4 /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
      1. 
      2. Correct Answer: 481616481616