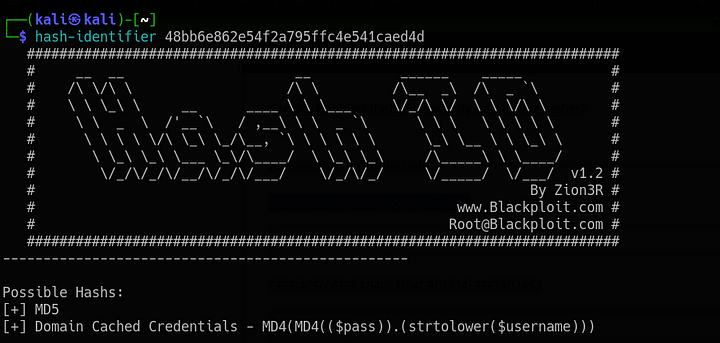
### **TryHackMe: Crack the hash**

Cracking hashes challenges. This walkthrough is basically cracking the different hashes provided in the challenge.

#### **1.48bb6e862e54f2a795ffc4e541caed4d’**

By looking at the hash it can be identified as a MD5 hash but to be 100% sure we can use a tool called “hash-identifier”.

Hash-identifier tool output

The above output confirms that the give hash is MD5. Now we can use hashcat to crack the hash. Hashcat is an opensource password recovery tool.

To crack the above hash we use the following command

hashcat -m 0 pass.txt /usr/share/wordlists/rockyou.txt

here,

**hashcat:** It is the tool used to crack the hash

**-m 0:** -m is used to specify the hash type and 0 is the code foe MD5 algorithm. The codes for the hash algorithm can be found [here](https://hashcat.net/wiki/doku.php?id=example_hashes)

pass.txt: the file where the hash value is stored

**/usr/share/wordlists/rockyou.txt:** this is the path to the common wordlists that hash cat reequires to crack the password. This time I am using rockyou.txt file. There are a lot more password files available in kali linux.

extracted password value

**Answer:** easy

#### **2.CBFDAC6008F9CAB4083784CBD1874F76618D2A97 — SHA1**

hashcat -m 100 pass.txt /usr/share/wordlists/rockyou.txt

**Answer:** password123

#### **3.1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032 — sha256**

hashcat -m 1400 pass.txt /usr/share/wordlists/rockyou.txt

**Answer:** letmein

#### **4.$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom — bcrypt**

For this hash the hash-identifier failed to identify the hash type. But by looking at the prefix ‘$2y$’ it can be identified that this is a bcrypt hash. The bcrypt hashes have a prefix which will be ‘$2\*$’. This can be veerified by any online hash identifier.

When i tried cracking this using the rockyou.txt it was taking a very long time due to my limited computing resources, so I checked the hint which stated to use only 4 letter words from the rockyou.txt. Hence I created a file filtering only 4 letter words from the rockyou.txt file.

cat /usr/share/wordlists/rockyou./txt | grep -E "^[a-z]{4}$" > refined\_pass.txt

the above command filters out only 4 letter words from the rockyou.txt file and stores them in refined\_pass.txt.

now we can decrypt the hash using this refined wordlist.

hashcat -m 3200 pass.txt refined\_pass.txt

**Answer:** bleh

### **5.279412f945939ba78ce0758d3fd83daa — MD5**

This is again an MD5 hash. This time we will use another tool called John the Ripper. John the Ripper is another opensource tool for password recovery.

john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt pass

**john:** call to the tool John the Ripper

**— format:** this specifies the format of the hash

**— wordlist:** this specifies the path to the password wordlist

**pass:** this is the file that contains the hash

**Answer:** Eternity22

### **Task-2**

#### **1.F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85 — SHA-256**

hashcat -m 1400 pass.txt /usr/share/wordlists/rockyou.txt

**Answer:** paule

#### **2.1DFECA0C002AE40B8619ECF94819CC1B — NTLM**

hashcat -m 1000 pass.txt /usr/share/wordlists/rockyou.txt

**Answer:** n63umy8lkf4i

#### **3.$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02 — SHA512**

#### **Salt: aReallyHardSalt**

hashcat -m 1800 pass.txt /usr/share/wordlists/rockyou.txt

**Answer:** waka99

#### **4.Hash: e5d8870e5bdd26602cab8dbe07a942c8669e56d6 — SHA1**

#### **Salt: tryhackme**

hashcat -m 110 pass.txt /usr/share/wordlists/rockyou.txt

**Answer:** 481616481616

Note: Make sure the pass.txt file is updated with the relevant hash each time.