

John_loves_cat

For this task they have given us a set of hash this task can be done in two ways

- i) using hashcat
- ii) online md5 sha256 sha512 online decryptors

For this task we need to take the hashcat in the terminal window that will already be installed in kali linux since i am using ordinary linux distribution i downloaded it by referring youtube Then we need to enter the command in the following command

hashcat -m 0 "hash" "file location of Rockyou.txt"

The attack mode is 0 here it will vary for each hash type

Here -m refers the mode of attack

#0 refers to the hashcat mode for the MD5

#Rockyou.txt is the text that contains more than 10000 commonly used passwords

So what we do here is each time we are comparing the hash that is given in the question to the newly created hash that is generated from each words in the rockyou.txt

At the end of this comparison they will show the hash along the cracked password

This the common procedure that i used for solving each hash

For identifying the type of hash ,i uploaded the given task into an online hash identifier

- 1.)5cb7c2c3efd274c522679b994d0db5b1: **MD5**
- 2.)816a4092660e4e87b5b584c4a51e7b33db2fb1b8f972578ef90c5ed7608e0f19 :**SHA 256**
- 3.)77dbc87f6b67c777890cef34fbebffc594559e1fda920755e277dee6c058ec7fc104ceff94dc92a5496629ad2075c8ad65d9cfd42cba9c9bff6113e5ac8bebe: **SHA 512**
- 4.)162C809CEF35EAF5FD03139A3B0AC8AA : **NTLM**
- 5.)\$2b\$05\$HnDsP/sv2pk.88xx0pVkMuYolwFu3SUSslxpYxWaWlzi5z4ry5jE.:**bcrypt**

Also The hashcat modes that used for the cracking each hash is different

MD5: 0.

SHA-256: 1400.

SHA-512: 1700.

NTLM: 1000.

bcrypt: 3200.

After entering the common command that is given above we specify the hashcat mode and running it will give the password

```
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: WPDF-2.0 -> WNEOF
Hardware.Mon.#1...: Temp: 70c Util: 50%

Dictionary cache built:
* Filename...: /home/antappan/Downloads/rockyou.txt
* Passwords...: 14344391
* Bytes.....: 139921497
* Keyspace...: 14344384
* Runtime....: 2 secs

5cb7c2c3efd274c522679b994d0db5b1 : 1michelle

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 0 (MD5)
Hash.Target...: 5cb7c2c3efd274c522679b994d0db5b1
Time.Started...: Sun Oct 20 09:54:41 2024 (0 secs)
Time.Estimated...: Sun Oct 20 09:54:41 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/antappan/Downloads/rockyou.txt)
Guess.Queue....: 4/4 (100.00%)
Speed.#1.....: 4876.5 kH/s (0.06ms) @ Accel:256 Loops:1 Thr:1 Vec:16
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 26624/14344384 (0.19%)
Rejected.....: 0/26624 (0.00%)
Restore.Point...: 25600/14344384 (0.18%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: Jesus15 -> 200398
Hardware.Mon.#1...: Temp: 69c Util: 26%

Started: Sun Oct 20 09:54:12 2024
Finished: Sun Oct 20 09:54:42 2024
```

After repeating the procedure for all the hashes

We will get the flags

p3nt35t{1michelle.0_sunshine123.1400_gingerbread.1700_agente007.1000_school123.3200}

If we upload the 1st hash into MD5 decrypter we get the same flag i tried this for hash 1 2 and 3
But couldn't get it for hash 4 and hash 5

5cb7c2c3efd274c522679b994d0db5b1	5cb7c2c3efd274c522679b994d0db5b1 : 1michelle
<button>Encrypt</button>	<button>Decrypt</button>