Cracking The Hash

Here we will crack the hash using the "**john the ripper**" tool.

Step 1 :- Identify the hash format (like md5, SHA1, SHA256, etc).
Here we will use hash-identifier tool in kali linux
Command :- $ hash-identifier
Hash :- 48bb6e862e54f2a795ffc4e541caed4d
It identified hash is "**md5"**

Step 2 :- Save the hash in file (hash1.txt)
Command :- $ echo "48bb6e862e54f2a795ffc4e541caed4d" >> hash1.txt

Step 3 :- Now we use john the ripper tool to crack this hash
First we set the format of the john the ripper and specifying the wordlist
Command :- $ sudo john --format=raw-md5 --wordlist=rockyou.txt hash1.txt

---

Using Hashcat

Hash like :-
"$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom"

This is unknown hash
Need to convert it by giving ' \ ' before ' $ '

"\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom"

Step 1 :- Get the hash ID
Command :- $ hashid -m
"\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom"

```
┌──(root㉿Pratik)-[~/hashCrack]
└─# hashid -m "\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom"
Analyzing '$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom'
[+] Blowfish(OpenBSD) [Hashcat Mode: 3200]
[+] Woltlab Burning Board 4.x
[+] bcrypt [Hashcat Mode: 3200]
```

Step 2 :- We got the hash Id — 3200

Step 3 :- Save the hash in file (hash2.txt)
Command :- $ echo "\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom" >> hash2.txt

Step 4 :- By using “hashcat” tool we will crack the hash (it takes more time than normal hash)
Command :- $ hashcat -m 3200 hash2.txt rockyou.txt

```
┌──(root㉿Pratik)-[~/hashCrack]
└─# hashcat -m 3200 hash4.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: cpu-haswell-AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx, 1425/2914 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
```