Lab 11

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

Submitted to: Sir Ubaid Ullah

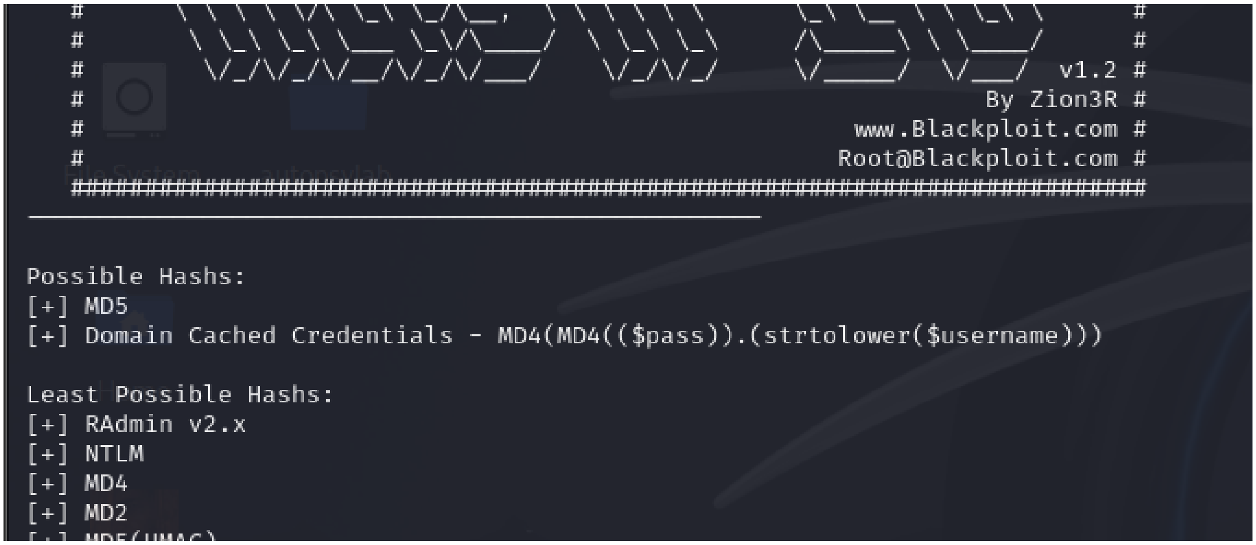
Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

Use the techniques and tools discussed earlier to crack the provided hashes:

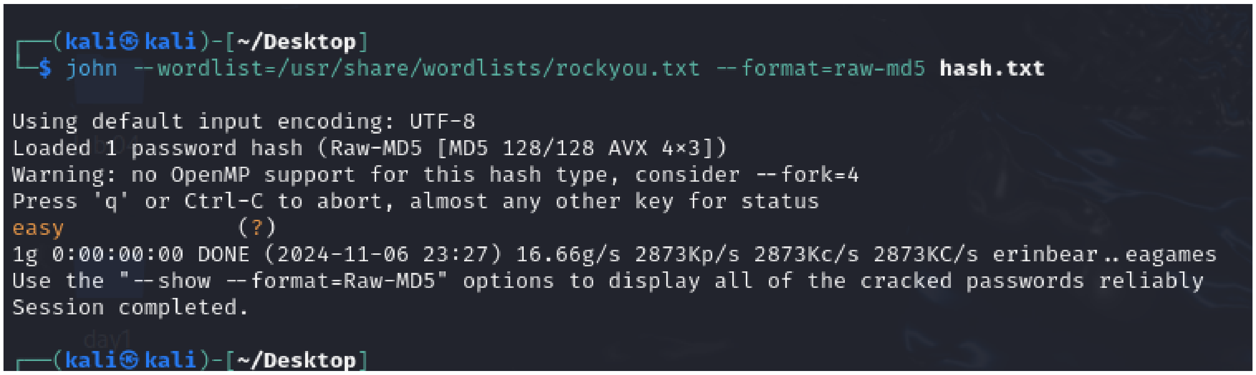
1. 48bb6e862e54f2a795ffc4e541caed4d

For this I first identified the hash by using hash-identifier which was MD5



```
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

 Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
```

Then i used john to crack it using rockyou.txt

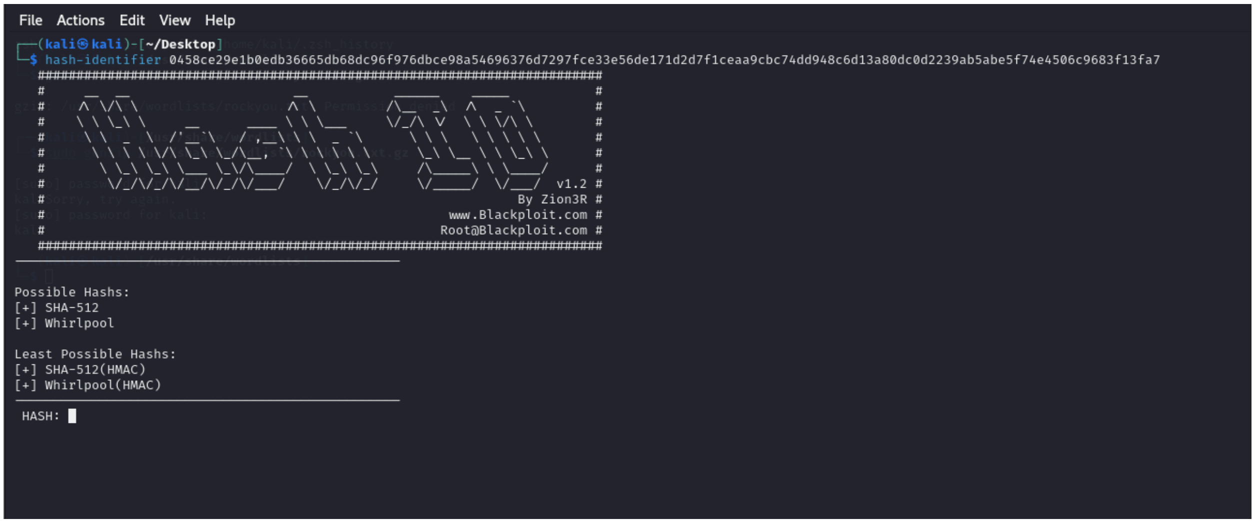


```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
easy             (?)
1g 0:00:00:00 DONE (2024-11-06 23:27) 16.66g/s 2873Kp/s 2873Kc/s 2873KC/s erinbear..eagames
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
```

The password was easy.

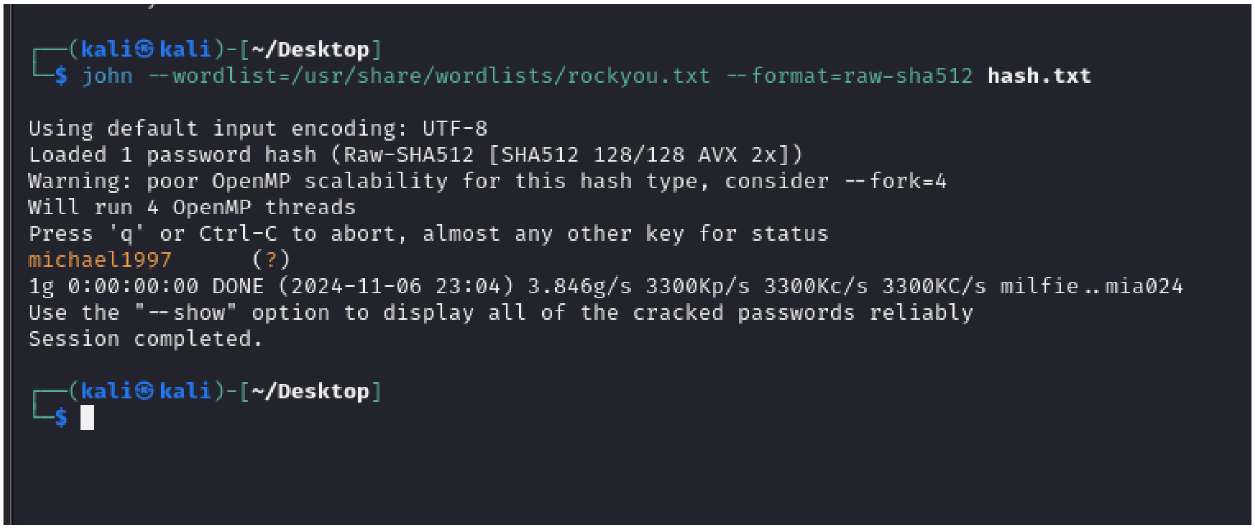
2.0458ce29e1b0edb36665db68dc96f976dbce98a54696376d7297fce33e56de171d2d7f1ceaa9cbc74dd948c6d13a80dc0d2239ab5abe5f74e4506c9683f13fa7

For this i identified the hash which was sha512



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hash-identifier 0458ce29e1b0edb36665db68dc96f976dbce98a54696376d7297fce33e56de171d2d7f1ceaa9cbc74dd948c6d13a80dc0d2239ab5abe5f74e4506c9683f13fa7
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] SHA-512
[+] Whirlpool

Least Possible Hashs:
[+] SHA-512(HMAC)
[+] Whirlpool(HMAC)
--------------------------------------------------

 HASH: 
```

Again i used john to crack the hash.

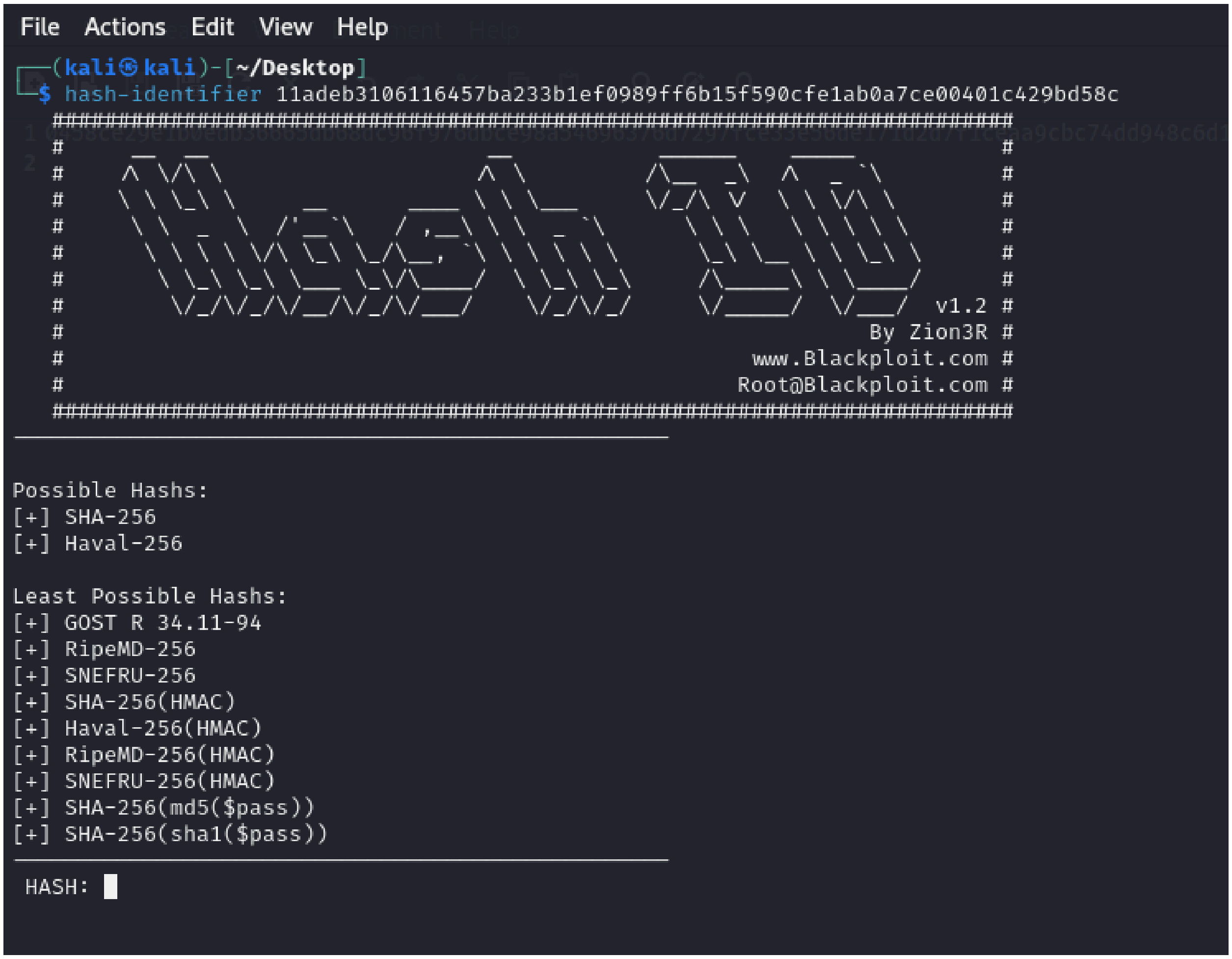


```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha512 hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA512 [SHA512 128/128 AVX 2x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
michael1997      (?)
1g 0:00:00:00 DONE (2024-11-06 23:04) 3.846g/s 3300Kp/s 3300Kc/s 3300KC/s milfie..mia024
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Password was : michael1997

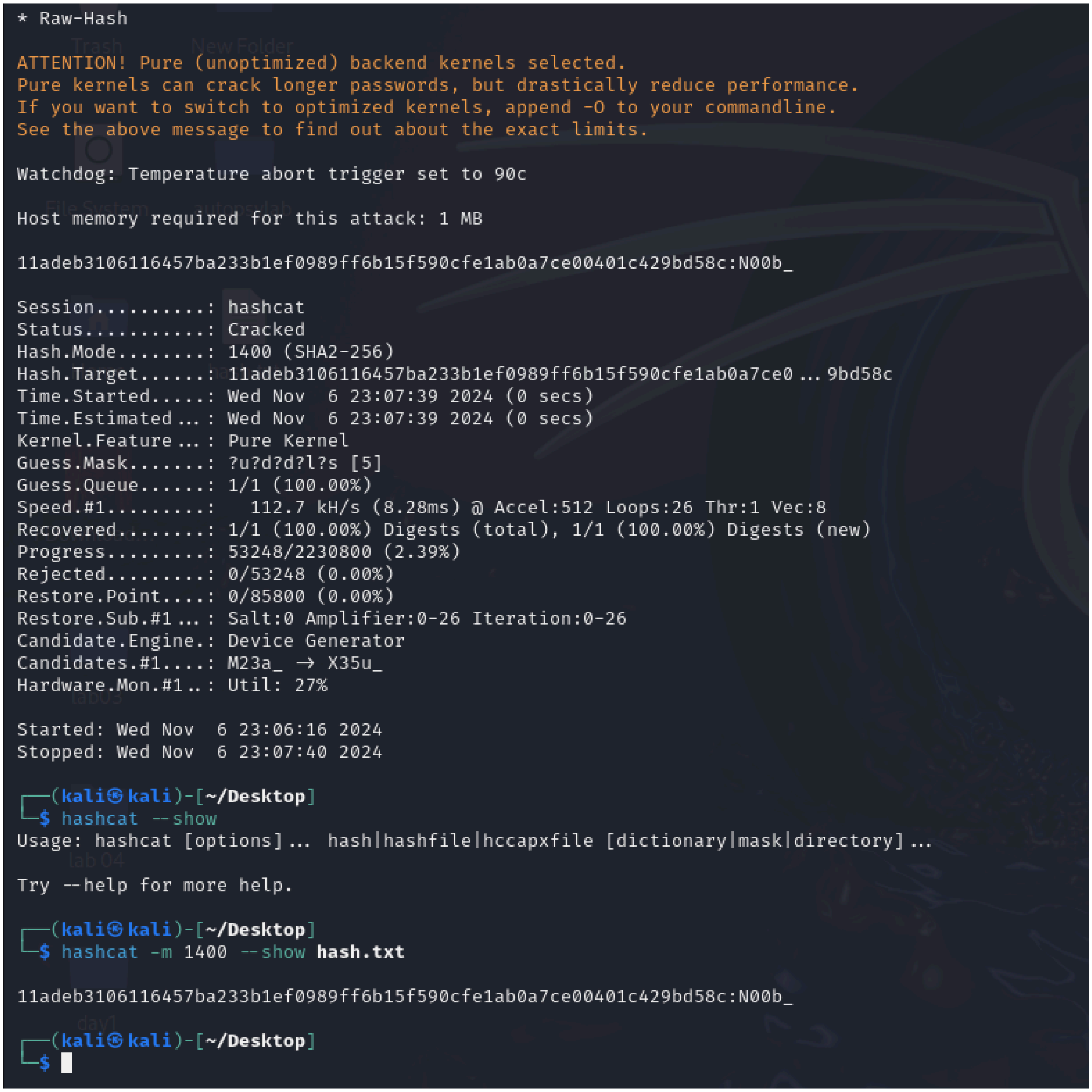
3.11adeb3106116457ba233b1ef0989ff6b15f590cfe1ab0a7ce00401c429 bd58c Hint: The password
is made up of 5 characters with the first character being an uppercase alphabet, followed by two
digits, then a lowercase alphabet, and finally a symbol.

So this one had a pattern so i used hashcat, but first we need to identify the hash.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hash-identifier 11adeb3106116457ba233b1ef0989ff6b15f590cfe1ab0a7ce00401c429bd58c
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] SHA-256
[+] Haval-256

Least Possible Hashs:
[+] GOST R 34.11-94
[+] RipeMD-256
[+] SNEFRU-256
[+] SHA-256(HMAC)
[+] Haval-256(HMAC)
[+] RipeMD-256(HMAC)
[+] SNEFRU-256(HMAC)
[+] SHA-256(md5($pass))
[+] SHA-256(sha1($pass))
--------------------------------------------------
 HASH: 
```

So which was sha256, then i used hash cat to crack the hash which was

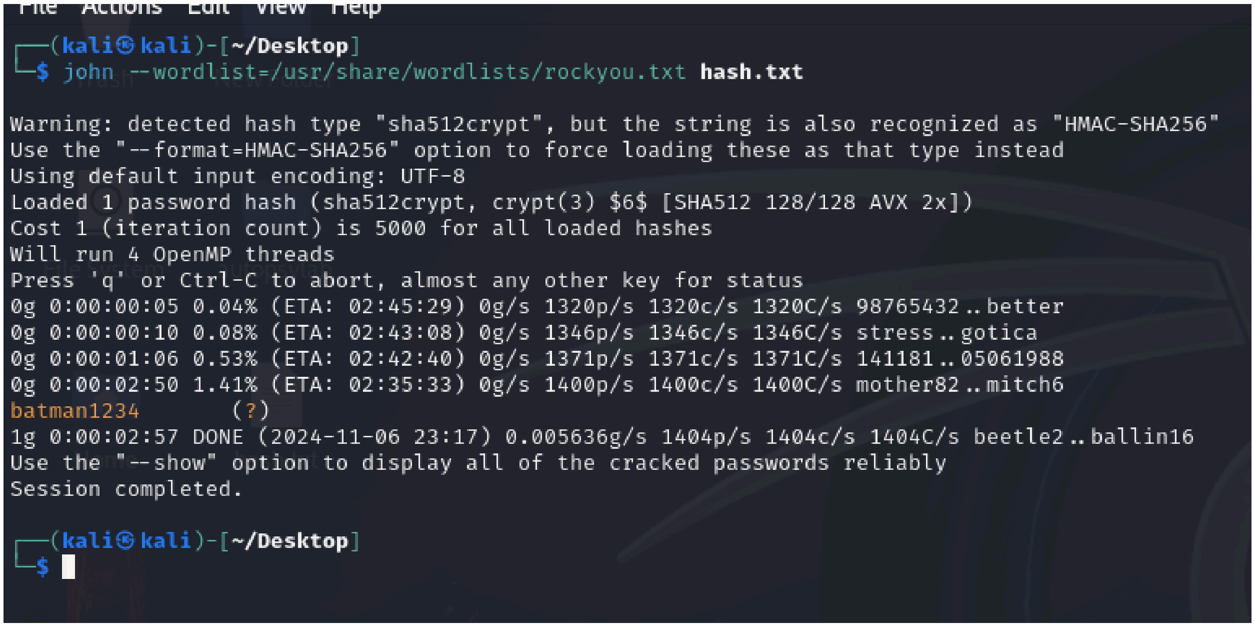


```
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

11adeb3106116457ba233b1ef0989ff6b15f590cfe1ab0a7ce00401c429bd58c:N00b_

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: 11adeb3106116457ba233b1ef0989ff6b15f590cfe1ab0a7ce0...9bd58c
Time.Started.....: Wed Nov  6 23:07:39 2024 (0 secs)
Time.Estimated...: Wed Nov  6 23:07:39 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?u?d?d?l?s [5]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   112.7 kH/s (8.28ms) @ Accel:512 Loops:26 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 53248/2230800 (2.39%)
Rejected.........: 0/53248 (0.00%)
Restore.Point....: 0/85800 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-26 Iteration:0-26
Candidate.Engine.: Device Generator
Candidates.#1....: M23a_ -> X35u_
Hardware.Mon.#1..: Util: 27%

Started: Wed Nov  6 23:06:16 2024
Stopped: Wed Nov  6 23:07:40 2024

┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat --show
Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

Try --help for more help.

┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 1400 --show hash.txt

11adeb3106116457ba233b1ef0989ff6b15f590cfe1ab0a7ce00401c429bd58c:N00b_

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

N00b_

4.$6$sup3rstr0ngs4lt$fZt5XYt.hdLFCs7YOlSIXT.0cDaNIhtP5QdD RdYP6OD349oD8hR9mEYue BRxaSAEHtAJ85wYYNyEELJkb0QSW1 Hint: Google &quot;salt&quot; in the context of hashing.

For this i first identified the hash but it didn’t work, i asked chat gpt what it was , so it told that it was salted hash, salt being “sup3rstr0ngs4lt” ,
So i used john the ripper to decrypt it using rockyou



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 0.04% (ETA: 02:45:29) 0g/s 1320p/s 1320c/s 1320C/s 98765432..better
0g 0:00:00:10 0.08% (ETA: 02:43:08) 0g/s 1346p/s 1346c/s 1346C/s stress..gotica
0g 0:00:01:06 0.53% (ETA: 02:42:40) 0g/s 1371p/s 1371c/s 1371C/s 141181..05061988
0g 0:00:02:50 1.41% (ETA: 02:35:33) 0g/s 1400p/s 1400c/s 1400C/s mother82..mitch6
batman1234       (?)
1g 0:00:02:57 DONE (2024-11-06 23:17) 0.005636g/s 1404p/s 1404c/s 1404C/s beetle2..ballin16
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

And it was batman1234