

TASK 4

- Identify Hash Type

```
(kali㉿kali)-[~]
$ hash-identfier
#####
#                                     #
#                               #       #
#   ^^^^      ,    ^^^        vvvv     #
#   / \ / \ / \ / \ / \ / \ / \ / \ / \ #
#   |_| |_| |_| |_| |_| |_| |_| |_| |_| #
#   |_| |_| |_| |_| |_| |_| |_| |_| |_| #
#                                   v1.2 #
#                                By Zion3R #
#                            www.Blackexploit.com #
#                        Root@Blackexploit.com #
#####

HASH: 482c811da5d5b4bc6d497ffa98491e38

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

The Hash is correctly identified as a MD5 Hash.

- Cracking the Hash

```
(kali㉿kali)-[~]  
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.t  
xt  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password123 (?)  
1g 0:00:00:00 DONE (2026-02-01 02:53) 2.222g/s 3413p/s 3413c/s 3413C/s 75395  
1..mexico1  
Use the "--show --format=Raw-MD5" options to display all of the cracked pass  
words reliably  
Session completed.
```

As we can see the original plain text is recovered