

Day 8 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: John the Ripper

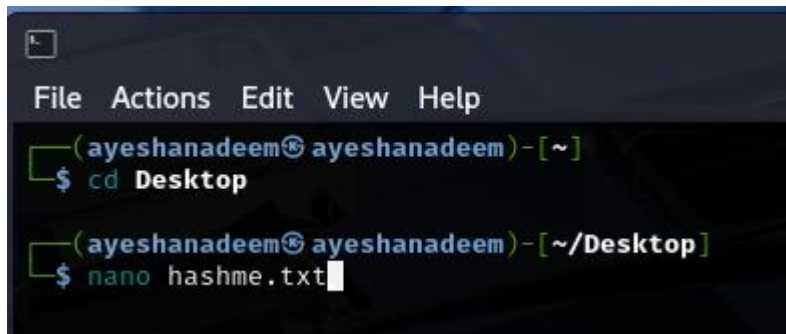


Contact Me: ayeshanm8@gmail.com

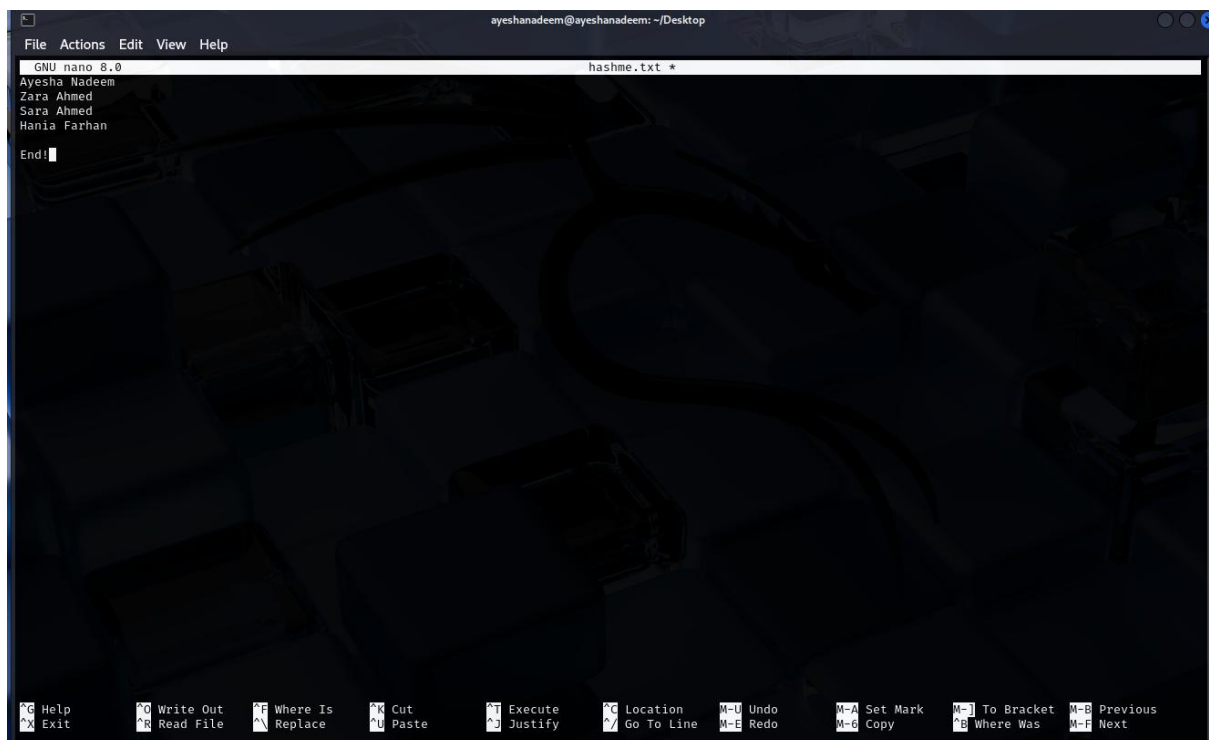
Date: 8th July, 2025

John the Ripper: Password Auditing & Cracking

Create & Edit a file

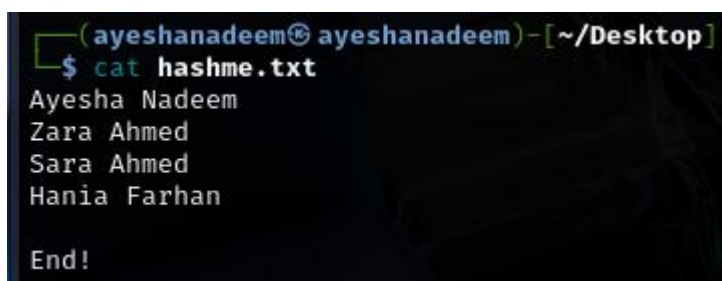


```
(ayeshanadeem@ayeshanadeem)-[~]  
$ cd Desktop  
  
(ayeshanadeem@ayeshanadeem)-[~/Desktop]  
$ nano hashme.txt
```



```
GNU nano 8.0 hashme.txt *  
Ayesha Nadeem  
Zara Ahmed  
Sara Ahmed  
Hania Farhan  
End!  
  
⌘ Help      ⌘ Write Out  ⌘ Where Is  ⌘ Cut       ⌘ Execute   ⌘ Location  ⌘ Undo     ⌘ Set Mark  ⌘ To Bracket ⌘ Previous  
⌘ Exit      ⌘ Read File  ⌘ Replace   ⌘ Paste     ⌘ Justify   ⌘ Go To Line ⌘ Redo     ⌘ Copy      ⌘ Where Was ⌘ Next
```

- Press Ctrl + O, then Enter
- Press Ctrl + X, to save changes



```
(ayeshanadeem@ayeshanadeem)-[~/Desktop]  
$ cat hashme.txt  
Ayesha Nadeem  
Zara Ahmed  
Sara Ahmed  
Hania Farhan  
  
End!
```

Generate a Hash of hashme.txt file

MD5

```
(ayeshanadeem@ayeshanadeem) - [~/Desktop]
$ md5sum hashme.txt
437f9ac0dd8dd958eace2302793851a2 hashme.txt
```

SHA 256

```
(ayeshanadeem@ayeshanadeem) - [~/Desktop]
$ sha256sum hashme.txt
46bd2068e546995cf5d2b6d1d630363fcc7261dba7396cc4c46d9a5de8a22baf hashme.txt
```

I had created the hash of some names using md5 and sha256 hashing algorithm. The **more secure** algorithm is sha256 because the hash generated by sha256 is more **lengthy and tricky to break**. The hash length of sha256 is **256 bits**, means less hash collisions while md5 hash length is 128 bits, means more hash collisions

Password Hashes Crack

Edit these hash one by one in nano editor then, apply john the ripper tool to crack these hashes.

No	Hash of Password generated in MD5	Password
1	50c60ac437e4d4ef19c77bdca5bbcf3b	University
2	b9698b8546220246fe600a949db326bf	Pakistan
3	dc647eb65e6711e155375218212b3964	Password
4	07a094a210794e74a0e5e1a1457a92ee	Word
5	88756ab57e0945c6455553c4c4cc622e	Islamabad

Cracked using John the Ripper

```

ayeshanadeem@kali: ~/Desktop
File Actions Edit View Help

ayeshanadeem@kali:~/Desktop
$ john hash1.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ADICII
ag 0:00:00:07 3/3 ag/s 25470Kc/s 25470Kc/s h1h20k..h1h2an
Session aborted

ayeshanadeem@kali:~/Desktop
$ john hash2.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ADICII
ag 0:00:00:03 3/3 ag/s 16453Kc/s 16453Kc/s av11jk..av136j
Session aborted

ayeshanadeem@kali:~/Desktop
$ john hash3.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

ayeshanadeem@kali:~/Desktop
$ john hash4.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

ayeshanadeem@kali:~/Desktop
$ john hash5.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ADICII
ag 0:00:00:03 3/3 ag/s 15255Kc/s 15255Kc/s syrewo..syrs3l
Session aborted

ayeshanadeem@kali:~/Desktop
$ john hash1.txt --show --format=raw-md5

```

Output:

```

ayeshanadeem@kali: ~/Desktop
File Actions Edit View Help

ayeshanadeem@kali:~/Desktop
$ john hash1.txt --show --format=raw-md5
0 password hashes cracked, 1 left

ayeshanadeem@kali:~/Desktop
$ john hash2.txt --show --format=raw-md5
0 password hashes cracked, 1 left

ayeshanadeem@kali:~/Desktop
$ john hash3.txt --show --format=raw-md5
1Password
1 password hash cracked, 0 left

ayeshanadeem@kali:~/Desktop
$ john hash4.txt --show --format=raw-md5
?word
1 password hash cracked, 0 left

ayeshanadeem@kali:~/Desktop
$ john hash5.txt --show --format=raw-md5
0 password hashes cracked, 1 left

ayeshanadeem@kali:~/Desktop

```

Only hash 3 and 4 is successfully decrypted by John the Ripper.

Reference:

[Decrypt MD5, SHA1, MySQL, NTLM, SHA256, MD5 Email, SHA256 Email, SHA512, Wordpress, Bcrypt hashes for free online](#)