Crack The Hash

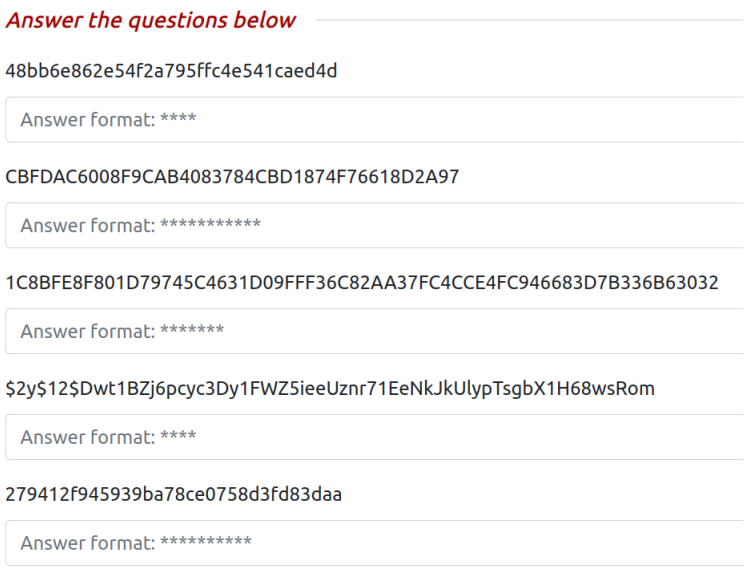
Kumpel7

November 2023

I used ubuntu machine and openVPN. All of the solutions (with questions) are provided at the end of the document.

1 Level 1

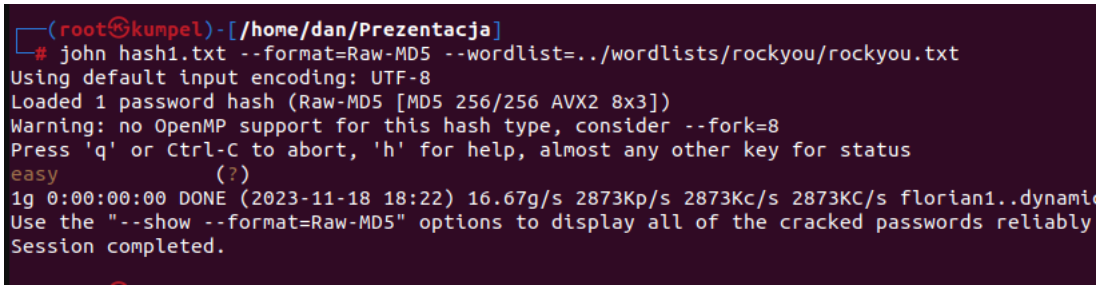
All of the hashes names I guessed because of hints, experience + knowledge of how many characters one hash is built of. For example Sha-256 has 256 bits, so 64 letters. MD5 is 128 bits, so 32 letters.



Rysunek 1: The hashes we need to crack

The first one is an MD5 hash. I insert it into john and immediately get the answer. I am using the rockyou.txt file as a dictionary. So my command is (as a root):

```
john hash1.txt --format=Raw-MD5 --wordlist=../wordlists/rockyou/rockyou.txt
```



The second one I didn't even have to guess, as john found out that this is Sha-1.

```
└─# john hash2.txt  --wordlist=../wordlists/rockyou/rockyou.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedir
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
password123      (?)
1g 0:00:00:00 DONE (2023-11-18 18:29) 25.00g/s 34600p/s 34600c/s 34600C/s jesse..password123
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

The 3rd one is Sha-256.

```
└─# john hash3.txt --format=raw-sha256 --wordlist=../wordlists/rockyou/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=8
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
letmein          (?)
1g 0:00:00:00 DONE (2023-11-18 18:34) 20.00g/s 2621Kp/s 2621Kc/s 2621KC/s 123456..koryna
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliab
Session completed.
```

hashes that start with $2y$ are called bcrypt. Here we knew that password will have 4 letters, so i used the additional lenght option.

```
└─# john hash4.txt --format=bcrypt --wordlist=../wordlists/rockyou/rockyou.txt --length=4
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
bleh             (?)
1g 0:00:00:18 DONE (2023-11-18 18:46) 0g/s 34.69p/s 34.69c/s 34.69C/s spam..5050
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

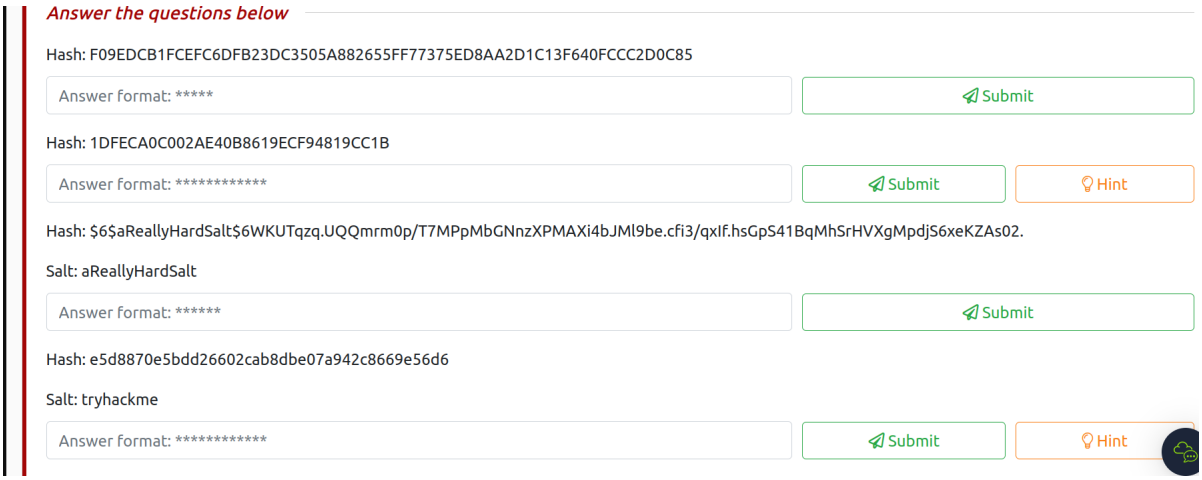
The last one from this level is md4 hash. This comes with a little suprise, as it is not from rockyou.txt. For this one i used the john preinstalled wordlist.

```
└─# john hash5.txt --format=raw-md4
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/home/dan/src/john/run/password.lst
Enabling duplicate candidate password suppressor
Eternity22       (?)
1g 0:00:00:01 DONE 2/3 (2023-11-18 18:52) 0g/s 2069Kp/s 2069Kc/s 2069KC/s Iamanurse..Kaylin01
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

2 Level 2

The first one is easy, because it is sha-256.

```
└─# john hash6.txt --format=raw-sha256 --wordlist=../wordlists/rockyou/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=8
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
paule            (?)
1g 0:00:00:00 DONE (2023-11-18 18:57) 16.67g/s 2184Kp/s 2184Kc/s 2184KC/s 123456..koryna
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```



Rysunek 2: New Exercises

The second one is hard to guess, as I encounter it for the first time in the rooms, it is NTLM from microsoft.

```
┌──(root㉿kumpel)-[/home/dan/Prezentacja]
└─# john hash7.txt --format=nt --wordlist=../wordlists/rockyou/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
n63umy8lkf4i     (?)
1g 0:00:00:00 DONE (2023-11-18 19:01) 2.273g/s 11907Kp/s 11907Kc/s 11907KC/s n65452..n601325
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

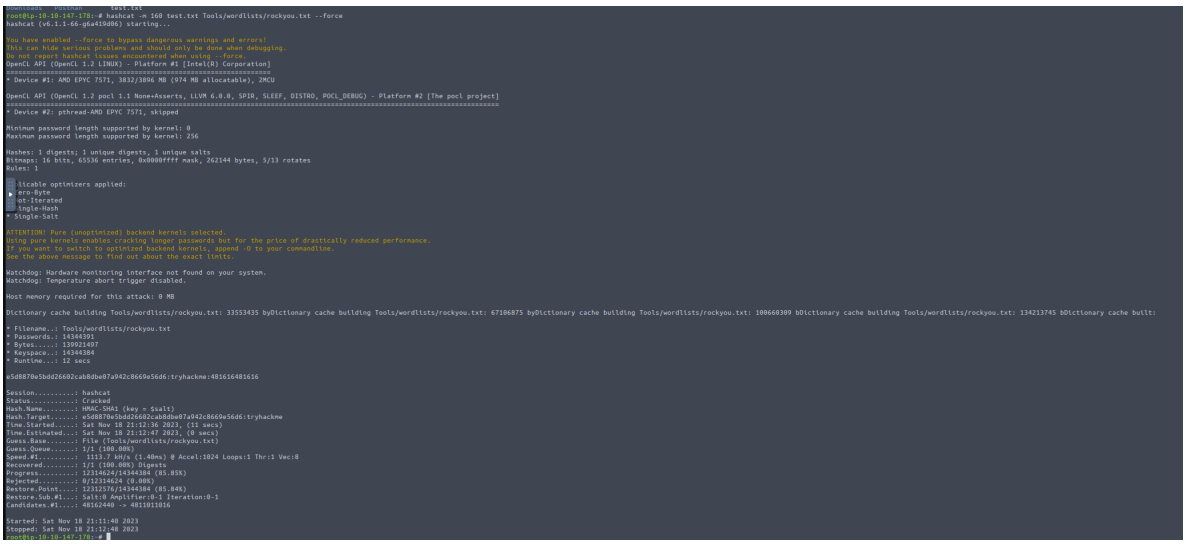
The next 2 hashes are with salt. The 3rd one should be sha-512 as it has 6 before the hash. This password took a while to crack, so i used lenght=6, because i see I will have 6–letter password :).

```
┌──(root㉿kumpel)-[/home/dan/Prezentacja]
└─# john --wordlist=../wordlists/rockyou/rockyou.txt --format=sha512crypt --length=6 hash8.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:14 0.45% (ETA: 20:31:09) 0g/s 2116p/s 2116c/s 2116C/s 021792..030703
0g 0:00:00:19 0.66% (ETA: 20:27:26) 0g/s 2194p/s 2194c/s 2194C/s 042281..cendol
0g 0:00:00:25 0.87% (ETA: 20:27:02) 0g/s 2162p/s 2162c/s 2162C/s xiexie..jack94
waka99           (?)
1g 0:00:05:25 DONE (2023-11-18 19:44) 0g/s 1949p/s 1949c/s 1949C/s wanuel..wajwaj
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

And now the last hash, for which john has the problem... https://github.com/openwall/john/issues/4259 ...
So we need to crack it using something different. I found a program called hashcat, so let's use that, and because I have some driver issues with hashcat, I will use it on the attackbox provided on tryhackme.

```
1    hashcat -m 160 test.txt Tools/wordlists/rockyou.txt --force
```

-m 160 means what hash am i cracking, –force ignores some stupid attackbox errors about drivers. This gives a lot of output, but the interesting part is at the end.



If you don't see it well, the password is after the second ":" sign : 481616481616. That's the end.