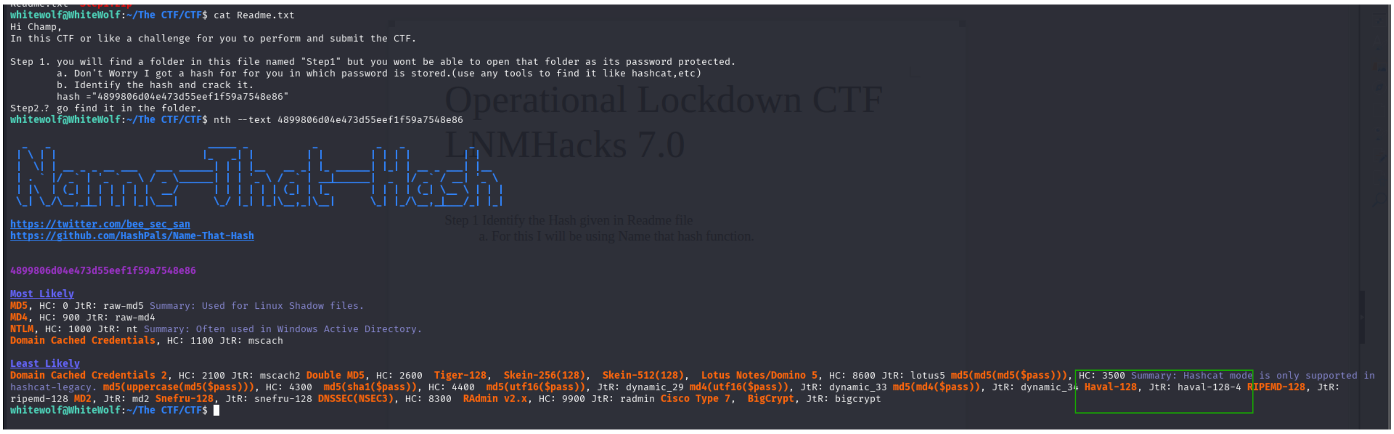
Operational Lockdown CTF LNMHacks 7.0

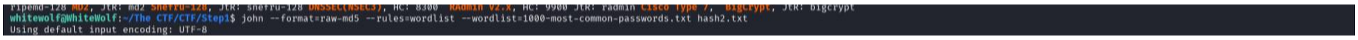
Step 1. Identify the Hash given in Readme file

1) For this I will be using Name that hash function.



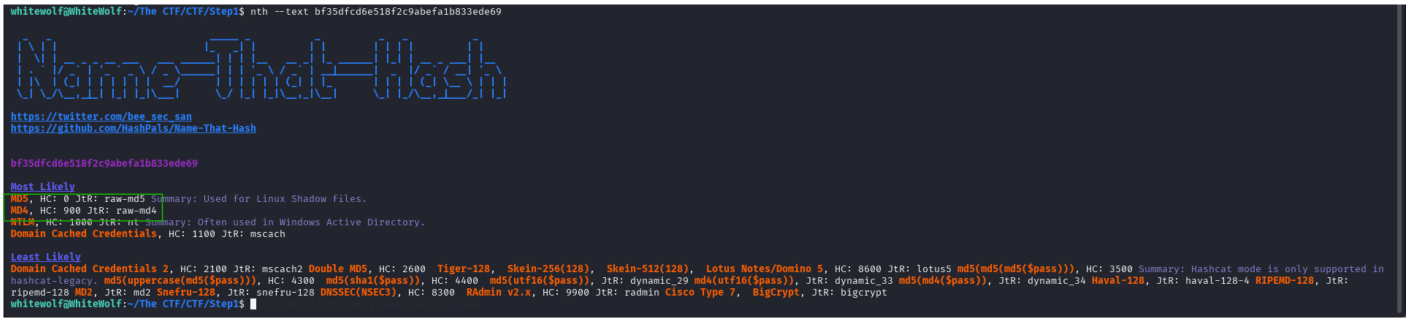
```
Readme.txt  Step1.zip
whitewolf@WhiteWolf:~/The CTF/CTF$ cat Readme.txt
Hi Champ,
In this CTF or like a challenge for you to perform and submit the CTF.

Step 1. you will find a folder in this file named "Step1" but you wont be able to open that folder as its password protected.
        a. Don't Worry I got a hash for for you in which password is stored.(use any tools to find it like hashcat,etc)
        b. Identify the hash and crack it.
        hash ="4899806d04e473d55eef1f59a7548e86"
Step2.? go find it in the folder.
whitewolf@WhiteWolf:~/The CTF/CTF$ nth --text 4899806d04e473d55eef1f59a7548e86

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash


4899806d04e473d55eef1f59a7548e86

Most Likely
MD5, HC: 0 JtR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JtR: raw-md4
NTLM, HC: 1000 JtR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JtR: mscach

Least Likely
Domain Cached Credentials 2, HC: 2100 JtR: mscach2 Double MD5, HC: 2600  Tiger-128,  Skein-256(128),  Skein-512(128),  Lotus Notes/Domino 5, HC: 8600 JtR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300  md5(sha1($pass)), HC: 4400  md5(utf16($pass)), JtR: dynamic_29 md4(utf16($pass)), JtR: dynamic_33 md5(md4($pass)), JtR: dynamic_34 Haval-128, JtR: haval-128-4 RIPEMD-128, JtR:
ripemd-128 MD2, JtR: md2 Snefru-128, JtR: snefru-128 DNSSEC(NSEC3), HC: 8300  RAdmin v2.x, HC: 9900 JtR: radmin Cisco Type 7,  BigCrypt, JtR: bigcrypt
whitewolf@WhiteWolf:~/The CTF/CTF$
```

2) You have to run all these formats and find which one will crack it.
3) store the hash in text file for sure to crack it.



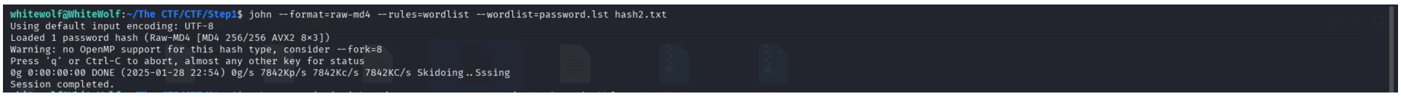
```
ripemd-128 MD2, JtR: md2 Snefru-128, JtR: snefru-128 DNSSEC(NSEC3), HC: 8300  RAdmin v2.x, HC: 9900 JtR: radmin Cisco Type 7,  BigCrypt, JtR: bigcrypt
whitewolf@WhiteWolf:~/The CTF/CTF/Step1$ john --format=raw-md5 --rules=wordlist --wordlist=1000-most-common-passwords.txt hash2.txt
Using default input encoding: UTF-8
```

4) Well I know its “Haval-128-4” encoding and crack the password “Butterfly3”. By running this above command.
5) Now we must get the wordlist in step 2.
6) Same command to Identify the hash and try it. Hash is “raw-md4”



```
whitewolf@WhiteWolf:~/The CTF/CTF/Step1$ nth --text bf35dfcd6e518f2c9abefa1b833ede69

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash


bf35dfcd6e518f2c9abefa1b833ede69

Most Likely
MD5, HC: 0 JtR: raw-md5 Summary: Used for Linux Shadow files.
MD4, HC: 900 JtR: raw-md4
NTLM, HC: 1000 JtR: nt Summary: Often used in Windows Active Directory.
Domain Cached Credentials, HC: 1100 JtR: mscach

Least Likely
Domain Cached Credentials 2, HC: 2100 JtR: mscach2 Double MD5, HC: 2600  Tiger-128,  Skein-256(128),  Skein-512(128),  Lotus Notes/Domino 5, HC: 8600 JtR: lotus5 md5(md5(md5($pass))), HC: 3500 Summary: Hashcat mode is only supported in
hashcat-legacy. md5(uppercase(md5($pass))), HC: 4300  md5(sha1($pass)), HC: 4400  md5(utf16($pass)), JtR: dynamic_29 md4(utf16($pass)), JtR: dynamic_33 md5(md4($pass)), JtR: dynamic_34 Haval-128, JtR: haval-128-4 RIPEMD-128, JtR:
ripemd-128 MD2, JtR: md2 Snefru-128, JtR: snefru-128 DNSSEC(NSEC3), HC: 8300  RAdmin v2.x, HC: 9900 JtR: radmin Cisco Type 7,  BigCrypt, JtR: bigcrypt
whitewolf@WhiteWolf:~/The CTF/CTF/Step1$
```

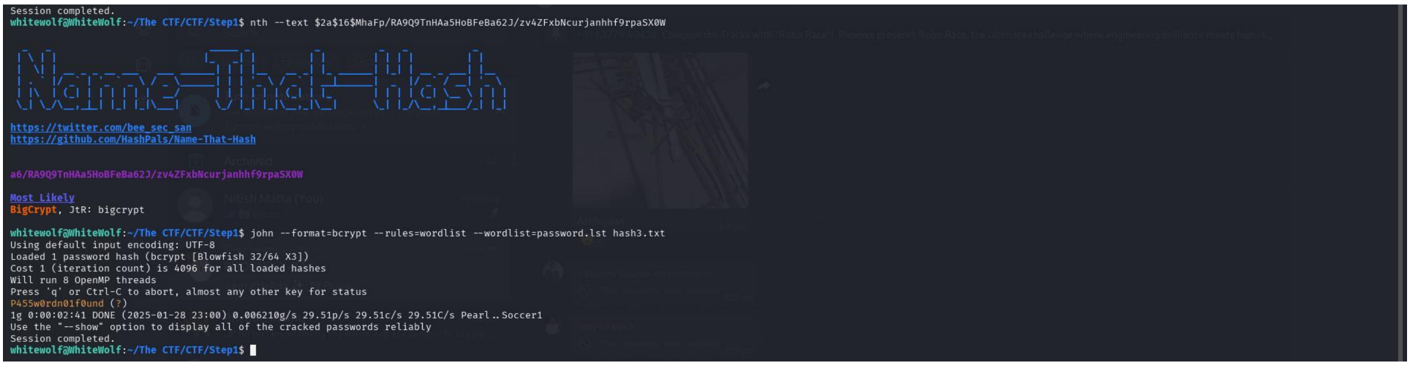
7) Run the command and get the password “Password@123”.



```
whitewolf@WhiteWolf:~/The CTF/CTF/Step1$ john --format=raw-md4 --rules=wordlist --wordlist=password.lst hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2025-01-28 22:54) 0g/s 7842Kp/s 7842Kc/s 7842KC/s Skidoing..Sssing
Session completed.
```

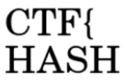
8) Here, It’s not showing password as its already cracked earlier but will show when done first.

9) Similar command and get the password “P455w0rdn01f0und”

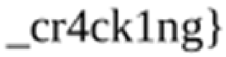


```
Session completed.
whitewolf@WhiteWolf:~/The CTF/CTF/Step1$ nth --text $2a$16$MhaFp/RA9Q9TnHAa5HoBFeBa62J/zv4ZFxbNcurjanhhf9rpaSX0W

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash


a6/RA9Q9TnHAa5HoBFeBa62J/zv4ZFxbNcurjanhhf9rpaSX0W

Most Likely
BigCrypt, JtR: bigcrypt

whitewolf@WhiteWolf:~/The CTF/CTF/Step1$ john --format=bcrypt --rules=wordlist --wordlist=password.lst hash3.txt
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, almost any other key for status
P455w0rdn01f0und (?)
1g 0:00:02:41 DONE (2025-01-28 23:00) 0.006210g/s 29.51p/s 29.51c/s 29.51C/s Pearl..Soccer1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
whitewolf@WhiteWolf:~/The CTF/CTF/Step1$ 
```

10) Now get the polygot file which has to open in two ways PNG and PDF.



CTF{
HASH



_cr4ck1ng}

11) Flag is “hacks{HASH_cr4ck1ng}”.