TakeOver - Tryhackme

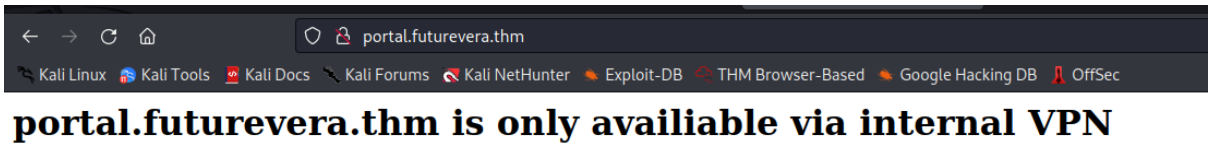
- As the room description says that it revolves around subdomain enumeration.
- We start with subdomain enumeration.
- First we need to add the address (futurevera.thm) to our /etc/hosts file.

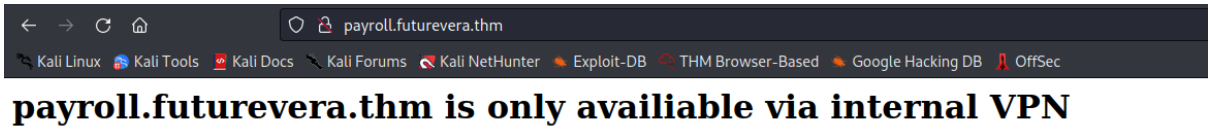
```
┌──(kali㉿kali)-[~/Documents/Tryhackme/TakeOver]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.203.180   futurevera.thm
```

- Then we perform subdomain enumeration using the tool `ffuf` on http protocol.

```
$ ffuf -u http://futurevera.thm/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.futurevera.t
hm" -fs 0


       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://futurevera.thm/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.futurevera.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 0

portal                  [Status: 200, Size: 69, Words: 9, Lines: 2, Duration: 487ms]
payroll                 [Status: 200, Size: 70, Words: 9, Lines: 2, Duration: 667ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

- Used the `-fs` flag to enumerate responses of 0 size.
- Got two subdomains, and added them in the /etc/hosts file
- Visited http://portal.futurevera.thm and http://payroll.futurevera.thm but nothing interesting there.





- Also checked the certificates but got nothing interesting.
- Then performed subdomain enumeration with the **https** protocol.

```
┌──(kali㉿kali)-[~]
└─$ ffuf -u https://futurevera.thm/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.futurevera.thm" -fs 0

      /'___\  /'___\           /'___\
     /\ \__/ /\ \__/  __  __  /\ \__/
     \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
      \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
       \ \_\   \ \_\  \ \____/  \ \_\
        \/_/    \/_/   \/___/    \/_/

      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : https://futurevera.thm/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.futurevera.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
 0 [tmux]  1 openvpn
```

```
________________________________________________

forum                   [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 453ms]
ns4                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 453ms]
mail2                   [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 449ms]
pop                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 450ms]
ns3                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 453ms]
secure                  [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 450ms]
www                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 458ms]
pop3                    [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 459ms]
webmail                 [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 461ms]
www2                    [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 474ms]
dev                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 483ms]
new                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 475ms]
imap                    [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 485ms]
beta                    [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 457ms]
vpn                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 490ms]
old                     [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 491ms]
mx                      [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 491ms]
mobile                  [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 481ms]
admin                   [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 491ms]
mysql                   [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 479ms]
cp                      [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 534ms]
demo                    [Status: 200, Size: 4605, Words: 1511, Lines: 92, Duration: 477ms]
```

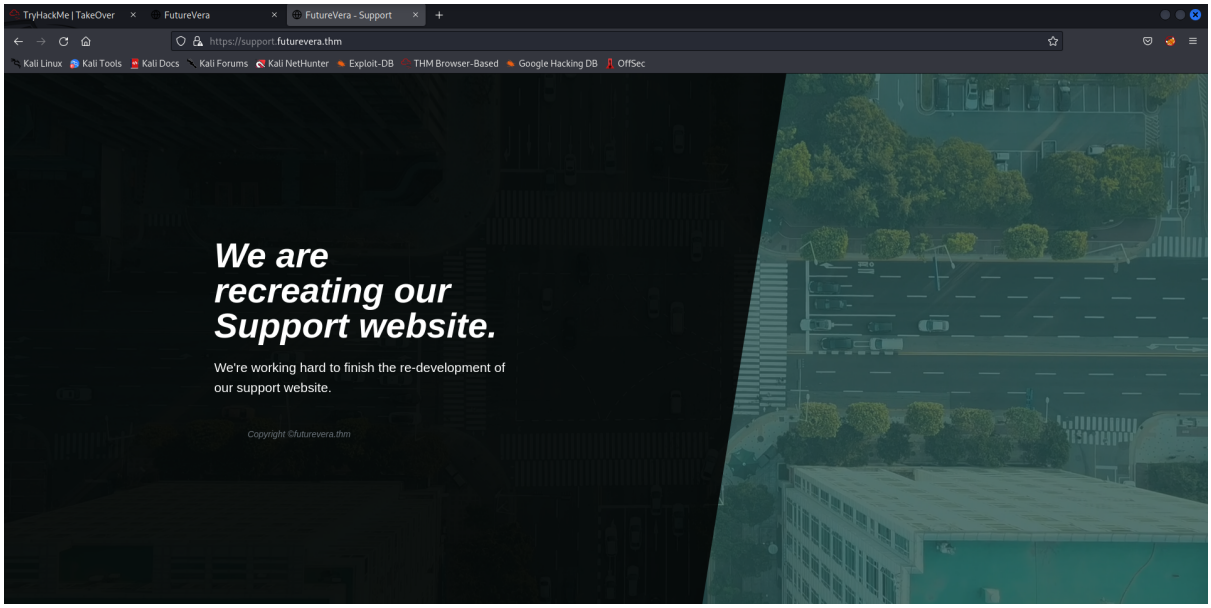
- But it was giving many responses with same response size i.e. 4605.
- Hence, used response filter and again run the command.

```
$ ffuf -u https://10.10.203.180/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.futurevera.t
hm" -fs 4605

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.203.180/
```

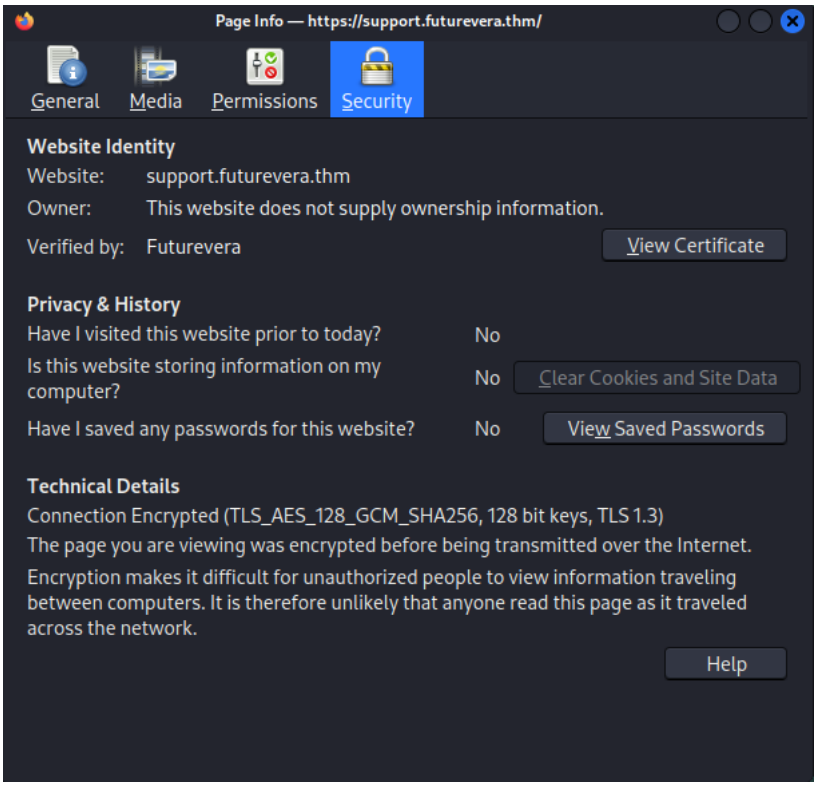
```
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.futurevera.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 4605
________________________________________________

support                 [Status: 200, Size: 1522, Words: 367, Lines: 34, Duration: 1431ms]
blog                    [Status: 200, Size: 3838, Words: 1326, Lines: 81, Duration: 416ms]
```

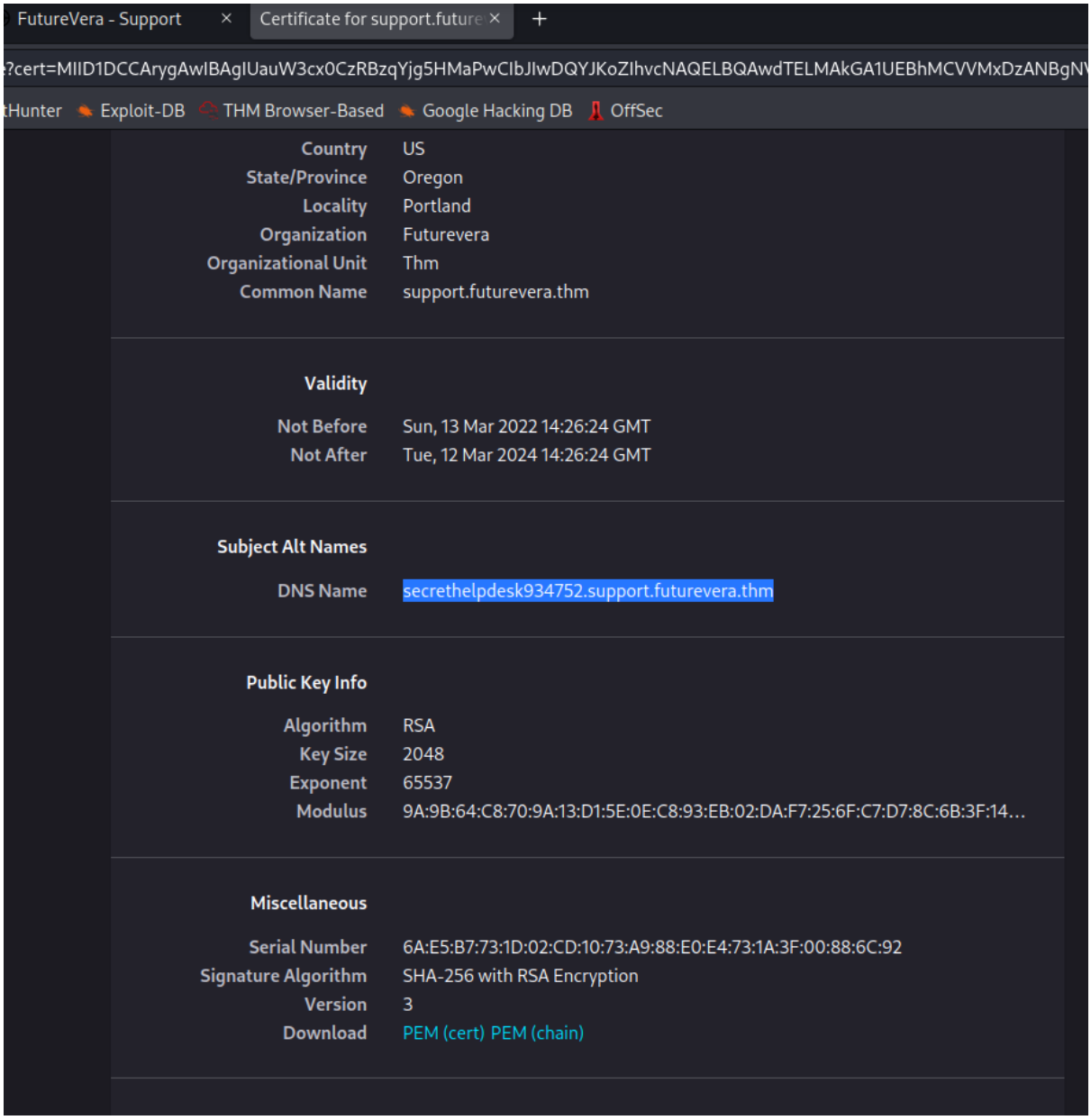
- Got two subdomains and added them in /etc/hosts file.
- Visited https://blog.futurevera.thm , got nothing interesting

- Visited https://support.futurevera.thm



- Checked its certificate and got an interesting subdomain.





- Added the subdomain in /etc/hosts file.
- Executed a curl command to get the headers as-

```
┌──(kali㉿kali)-[~]
└─$ curl --head secrethelpdesk934752.support.futurevera.thm
HTTP/1.1 302 Found
Date: Mon, 29 May 2023 20:01:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: http://flag{beea0d6edfcee06a59b83fb50ae81b2f}.s3-website-us-west-3.amazonaws.com/
Content-Type: text/html; charset=UTF-8
```

- Got the flag in the **Location** section.
- Also, if we visit http://secrethelpdesk934752.support.futurevera.thm , we get the flag in the address bar itself.