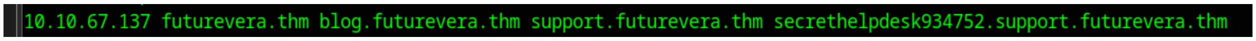
TakeOver
Subdomain Enumeration
TryHackMe

Got the IP address

Add the ip and domain in /etc/hosts file of the attacking machine



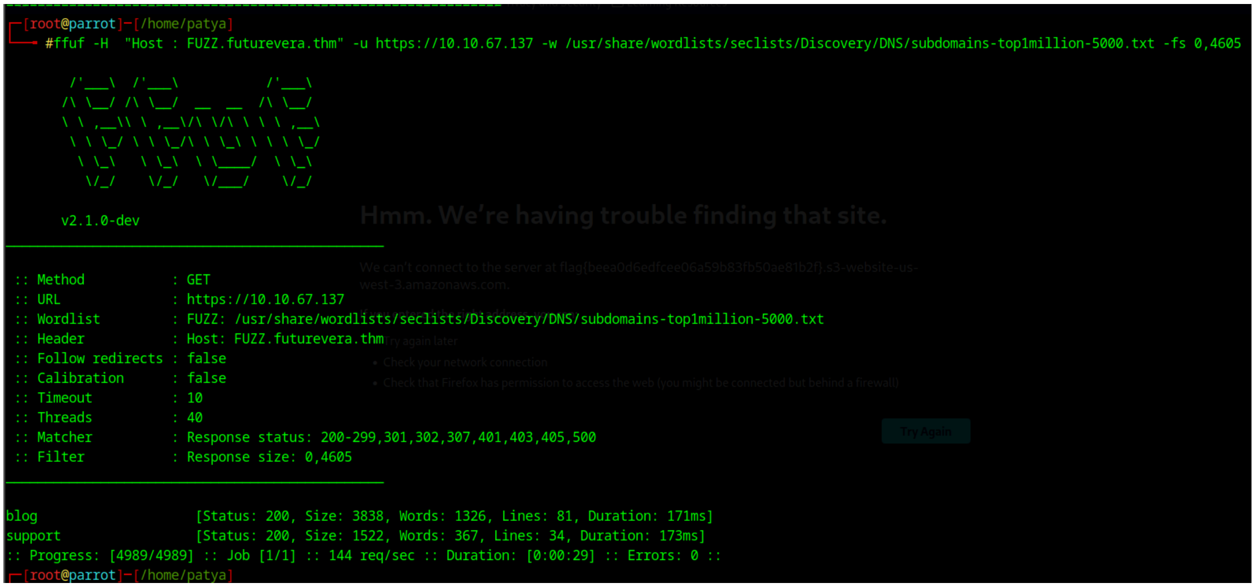
```
10.10.67.137 futurevera.thm blog.futurevera.thm support.futurevera.thm secrethelpdesk934752.support.futurevera.thm
```

Do nmap basic scan and find the ports

Checked the source code of main domain found nothing

Do subdomain enumeration using ffuf

ffuf -H "Host : FUZZ.futurevera.thm" -u https://10.10.67.137 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fs 0,4605

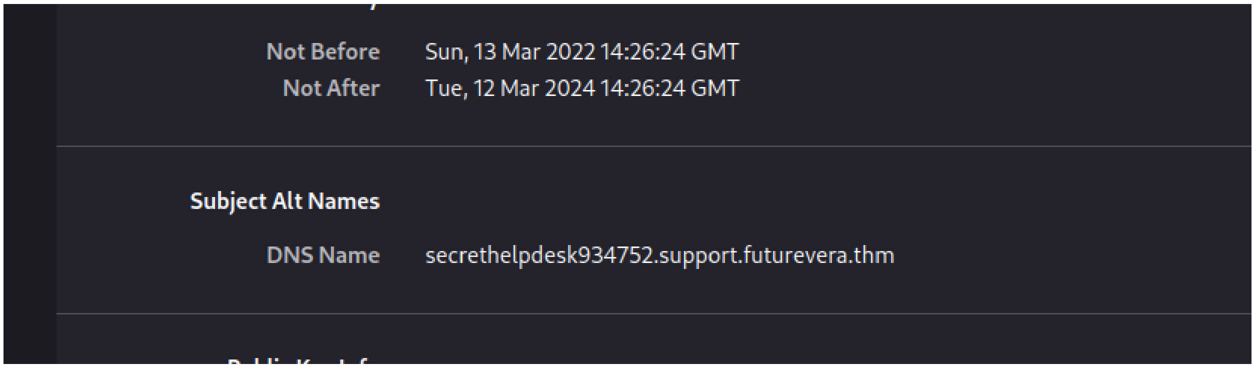


```
┌─[root@parrot]─[/home/patya]
└──╼ #ffuf -H  "Host : FUZZ.futurevera.thm" -u https://10.10.67.137 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -fs 0,4605

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.67.137
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.futurevera.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0,4605
________________________________________________

blog                    [Status: 200, Size: 3838, Words: 1326, Lines: 81, Duration: 171ms]
support                 [Status: 200, Size: 1522, Words: 367, Lines: 34, Duration: 173ms]
:: Progress: [4989/4989] :: Job [1/1] :: 144 req/sec :: Duration: [0:00:29] :: Errors: 0 ::
┌─[root@parrot]─[/home/patya]
```

Found two subdomain → blog and support

Checked both domain and source code nothing was found

But then I checked certificate of support page, found one more subdomain

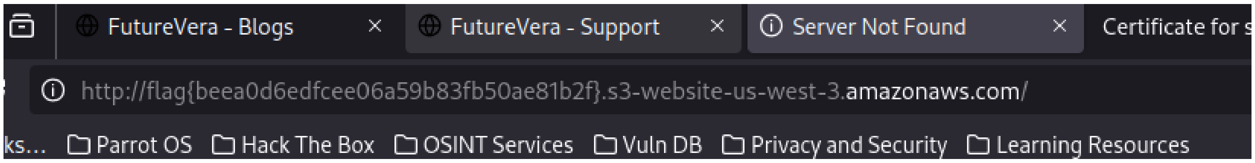


Not Before Sun, 13 Mar 2022 14:26:24 GMT
Not After Tue, 12 Mar 2024 14:26:24 GMT

Subject Alt Names

DNS Name secrethelpdesk934752.support.futurevera.thm

Url that subdomain in http://….
Found the flag in url



http://flag{beea0d6edfcee06a59b83fb50ae81b2f}.s3-website-us-west-3.amazonaws.com/