

# TakeOver – TryHackMe

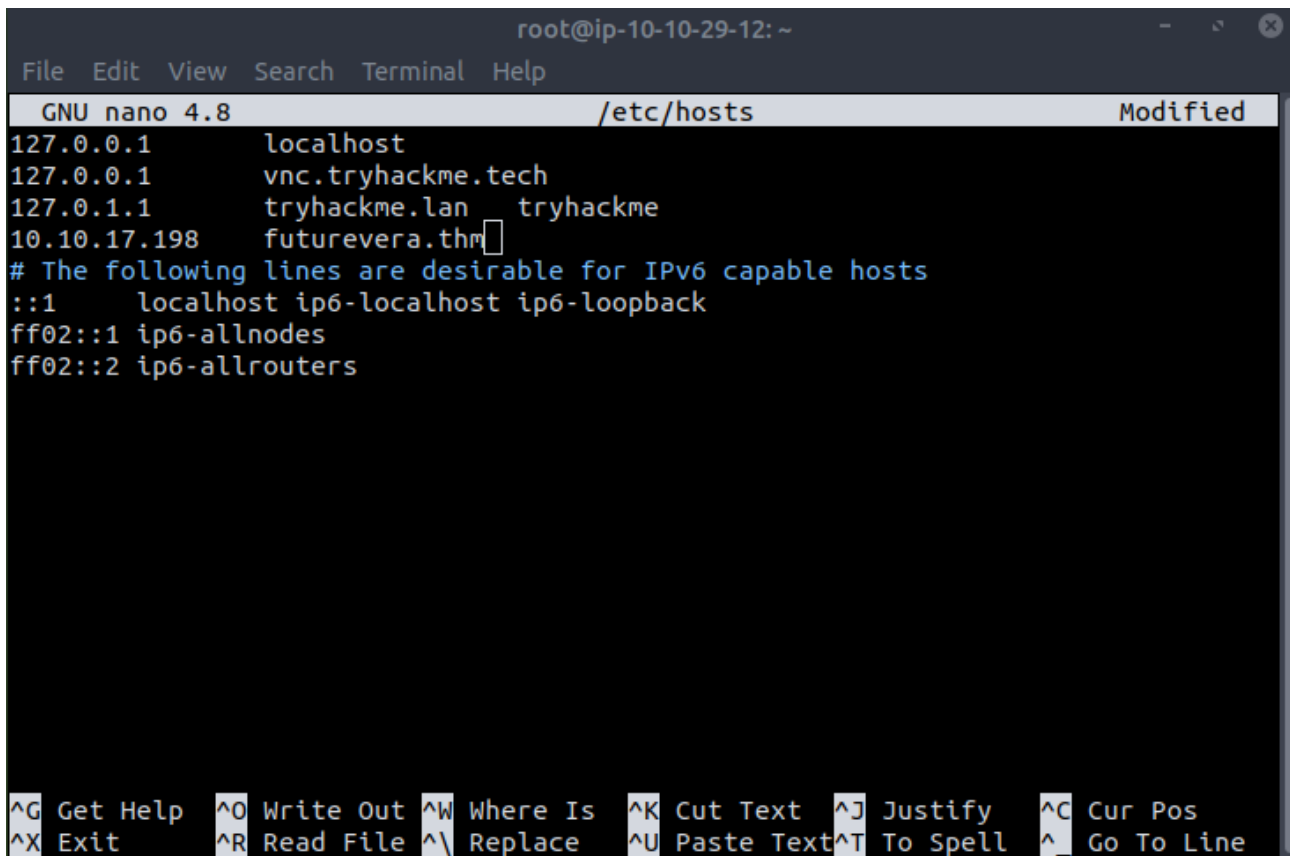
This is a CTF to practice subdomain enumeration; our task is to obtain the flag.

## Contents

1.Task.....	1
2.Summary.....	7

## 1.Task

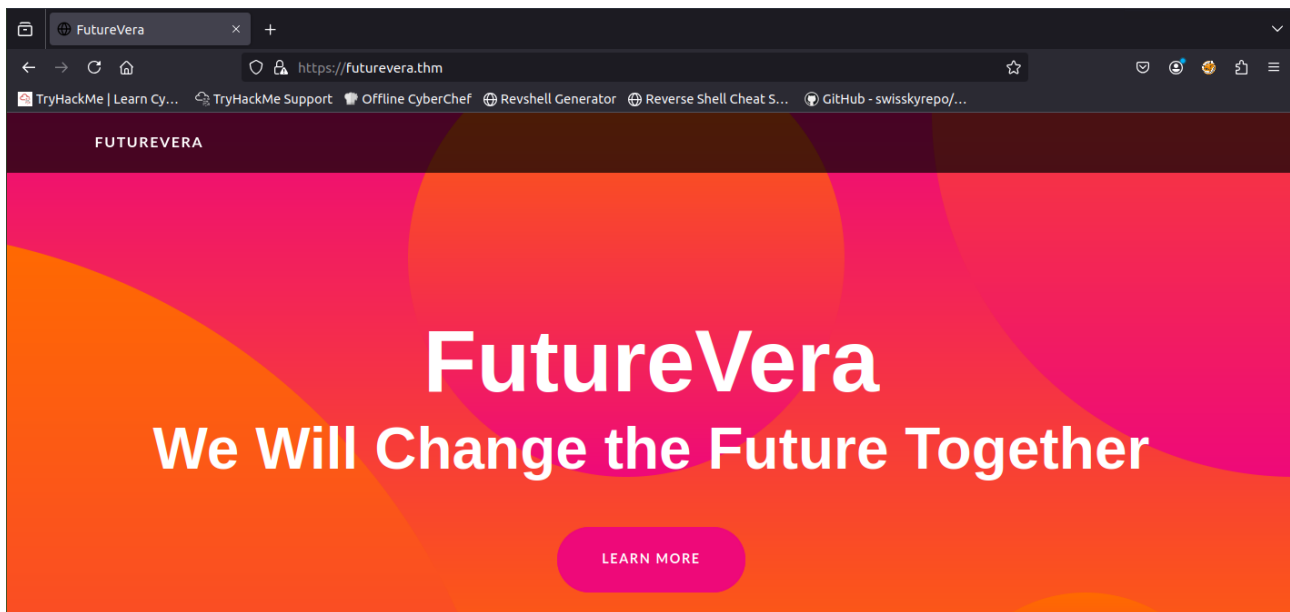
We start by adding futurevera.thm to /etc/hosts.

A screenshot of a terminal window titled 'root@ip-10-10-29-12: ~'. The terminal shows the GNU nano 4.8 editor editing the /etc/hosts file. The file content is as follows:

```
127.0.0.1    localhost
127.0.0.1    vnc.tryhackme.tech
127.0.1.1    tryhackme.lan  tryhackme
10.10.17.198  futurevera.thm
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

The cursor is positioned at the end of the line '10.10.17.198 futurevera.thm'. The bottom of the terminal shows the nano editor's help menu with various shortcuts like ^G for Get Help, ^O for Write Out, etc.

After opening the site, we see:



We start scanning with GoBuster, but with no results.

```
root@ip-10-10-29-12:~# gobuster dir -u https://futurevera.thm/ -w '/root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt' -k
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: https://futurevera.thm/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/assets (Status: 301) [Size: 319] [--> https://futurevera.thm/assets/]
/css (Status: 301) [Size: 316] [--> https://futurevera.thm/css/]
/js (Status: 301) [Size: 315] [--> https://futurevera.thm/js/]
/server-status (Status: 403) [Size: 280]
Progress: 218275 / 218276 (100.00%)
=====
Finished
=====
```

Now I scanned for subdomains and GoBuster returned portal.futurevera.thm.

```

root@ip-10-10-29-12:~# gobuster vhost -w '/root/Desktop/Tools/wordlists/SecLists/D
iscovery/DNS/subdomains-top1million-5000.txt' -u futurevera.thm --append-domain
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://futurevera.thm
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /root/Desktop/Tools/wordlists/SecLists/Discovery/DNS/subdomai
ns-top1million-5000.txt
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: portal.futurevera.thm Status: 200 [Size: 69]
Progress: 4997 / 4998 (99.98%)
=====
Finished
=====

```

We must add that to /etc/hosts.

GNU nano 4.8	/etc/hosts	Modified
127.0.0.1	localhost	
127.0.0.1	vnc.tryhackme.tech	
127.0.1.1	tryhackme.lan tryhackme	
10.10.17.198	futurevera.thm	
10.10.17.198	portal.futurevera.thm	
# The following lines are desirable for IPv6 capable hosts		
:::1	localhost ip6-localhost ip6-loopback	
ff02::1	ip6-allnodes	
ff02::2	ip6-allrouters	

<b>^G</b> Get Help	<b>^O</b> Write Out	<b>^W</b> Where Is	<b>^K</b> Cut Text	<b>^J</b> Justify	<b>^C</b> Cur Pos
<b>^X</b> Exit	<b>^R</b> Read File	<b>^_</b> Replace	<b>^U</b> Paste Text	<b>^T</b> To Spell	<b>^_</b> Go To Line

Now we scan that portal with GoBuster; there is nothing interesting.

```

root@ip-10-10-29-12:~# gobuster dir -u https://portal.futurevera.thm/ -w '/root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt' -k
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                https://portal.futurevera.thm/
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /root/Desktop/Tools/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Timeout:            10s
=====
Starting gobuster in directory enumeration mode
=====
/assets      (Status: 301) [Size: 333] [--> https://portal.futurevera.thm/assets/]
/css         (Status: 301) [Size: 330] [--> https://portal.futurevera.thm/css/]
/js          (Status: 301) [Size: 329] [--> https://portal.futurevera.thm/js/]
/server-status (Status: 403) [Size: 287]
Progress: 218275 / 218276 (100.00%)
=====
Finished
=====

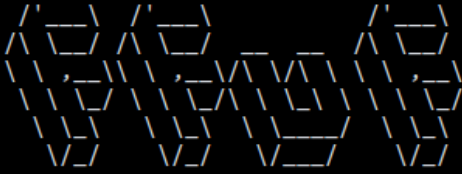
```

Here I paused a bit and ran ffuf to scan subpages and it found 2 more subdomains — blog and support.

```

root@ip-10-10-29-12:~# ffuf -w '/root/Desktop/Tools/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt' -H "Host: FUZZ.futurevera.thm" -u https://10.10.17.198 -fs 4605

```



```

v1.3.1
-----
:: Method      : GET
:: URL         : https://10.10.17.198
:: Wordlist    : FUZZ: /root/Desktop/Tools/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: 200,204,301,302,307,401,403,405
:: Filter     : Response size: 4605
-----
blog           [Status: 200, Size: 3838, Words: 1326, Lines: 81]
support        [Status: 200, Size: 1522, Words: 367, Lines: 34]
:: Progress: [1575/4997] :: Job [1/1] :: 2120 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [1881/4997] :: Job [1/1] :: 2445 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [2127/4997] :: Job [1/1] :: 1777 req/sec :: Duration: [0:00:01] :: Errors: 0 :

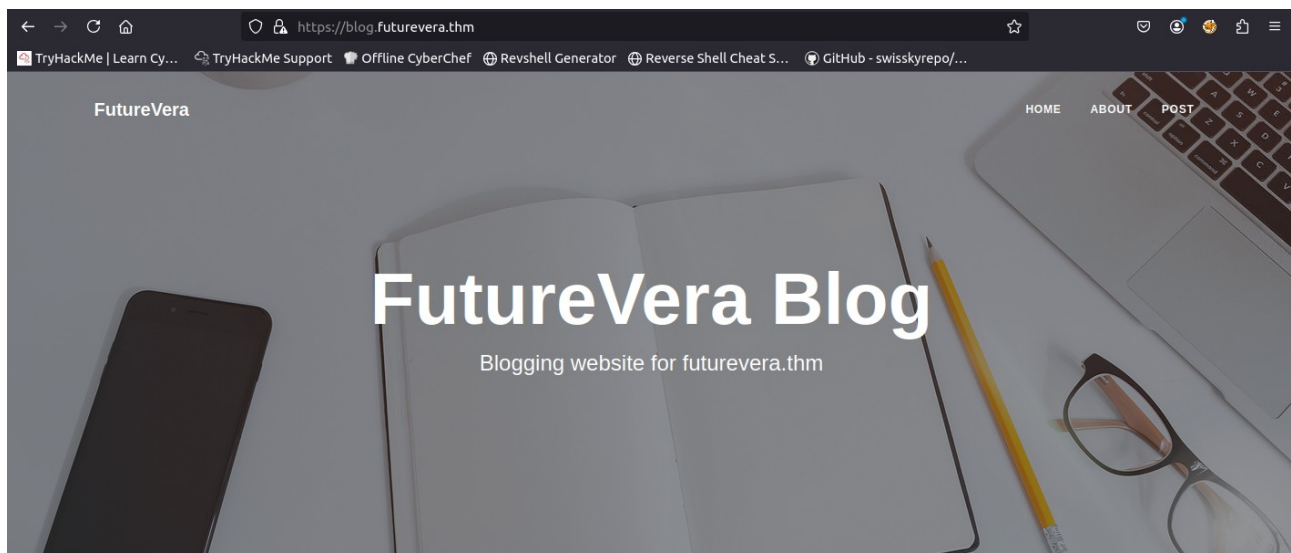
```

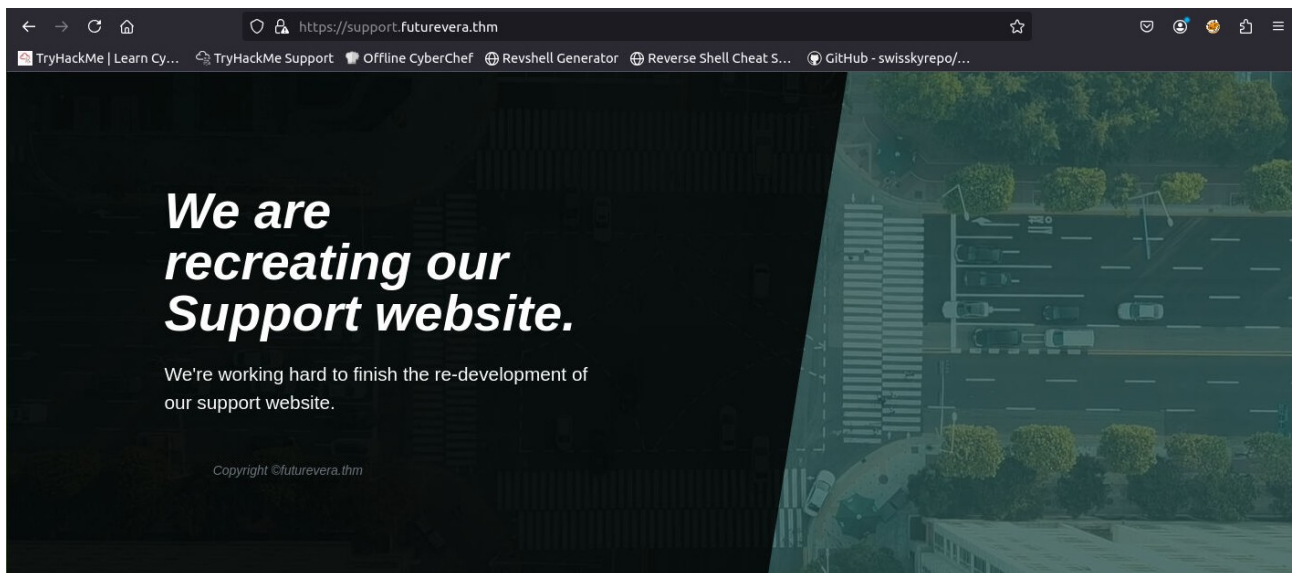
We add them to /etc/hosts.

```
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.0.1 vnc.tryhackme.tech
127.0.1.1 tryhackme.lan tryhackme
10.10.17.198 futurevera.thm
10.10.17.198 portal.futurevera.thm
10.10.17.198 blog.futurevera.thm
10.10.17.198 support.futurevera.thm
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

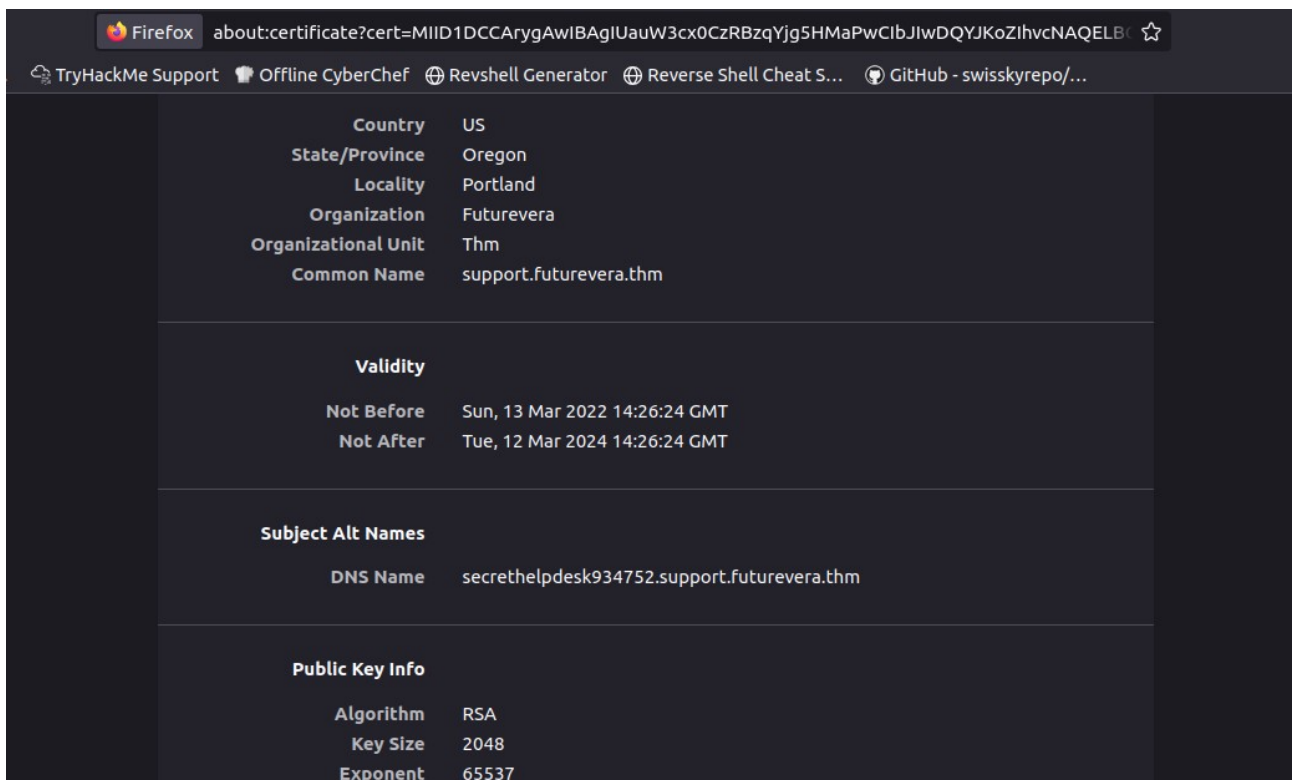
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

On those pages there is nothing interesting.





After entering support we get a certificate error; checking its details we see the name of some DNS that looks like a website.

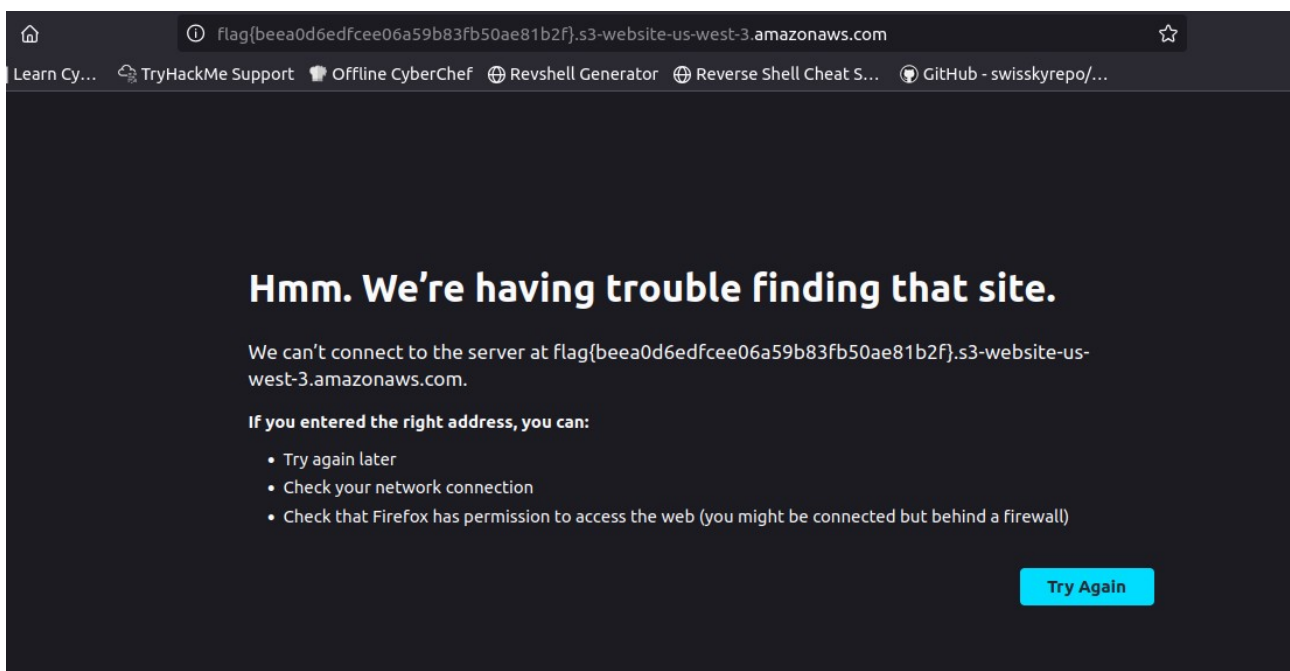


We add that to /etc/hosts.



```
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.0.1 vnc.tryhackme.tech
127.0.1.1 tryhackme.lan tryhackme
10.10.17.198 futurevera.thm
10.10.17.198 portal.futurevera.thm
10.10.17.198 blog.futurevera.thm
10.10.17.198 support.futurevera.thm
10.10.17.198 secrethelpdesk934752.support.futurevera.thm
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

After visiting that site, we have the flag.



## 2.Summary

This CTF focused on subdomain enumeration. After adding futurevera.thm to /etc/hosts, the solver used Gobuster and ffuf to discover portal, blog, and support subdomains, mapped them in /etc/hosts, and ultimately accessed a hidden page that contained the flag.

Concise takeaway: combine active fuzzing with careful host mapping to reveal hidden web hosts and win the flag.