TryHackMe Room Write-up

Title: TakeOver

Description: This challenge resolves around subdomain enumeration.

Author: Igor Buszta

Help Us

Description: *Hello there,*

I am the CEO and one of the co-founders of futurevera.thm. In Futurevera, we believe that the future is in space. We do a lot of space research and write blogs about it. We used to help students with space questions, but we are rebuilding our support.

Recently blackhat hackers approached us saying they could takeover and are asking us for a big ransom. Please help us to find what they can takeover.

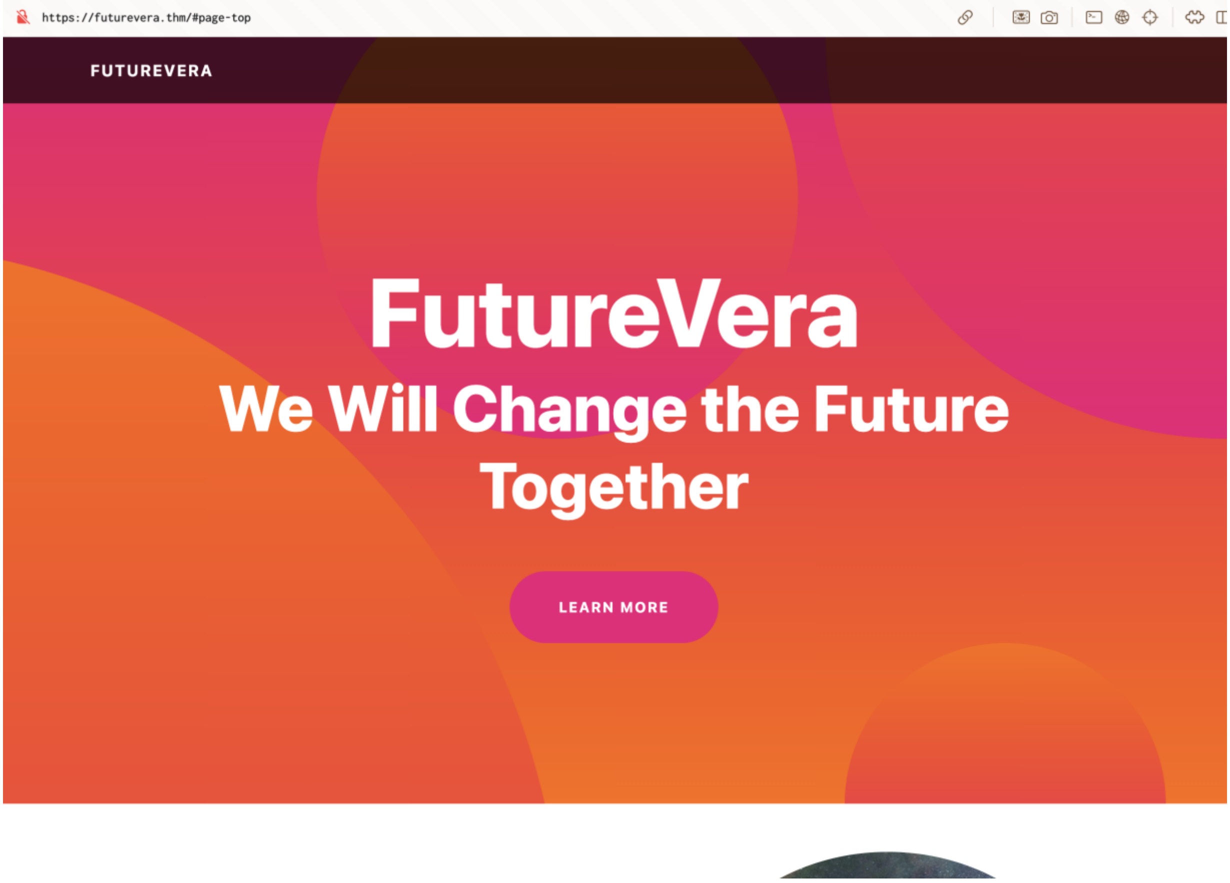
Our website is located at https://futurevera.thm

Hint: Don't forget to add the MACHINE_IP in /etc/hosts for futurevera.thm ;)

Objective*: What's the value of the flag?*

Tools*: macOS, web search engine.*

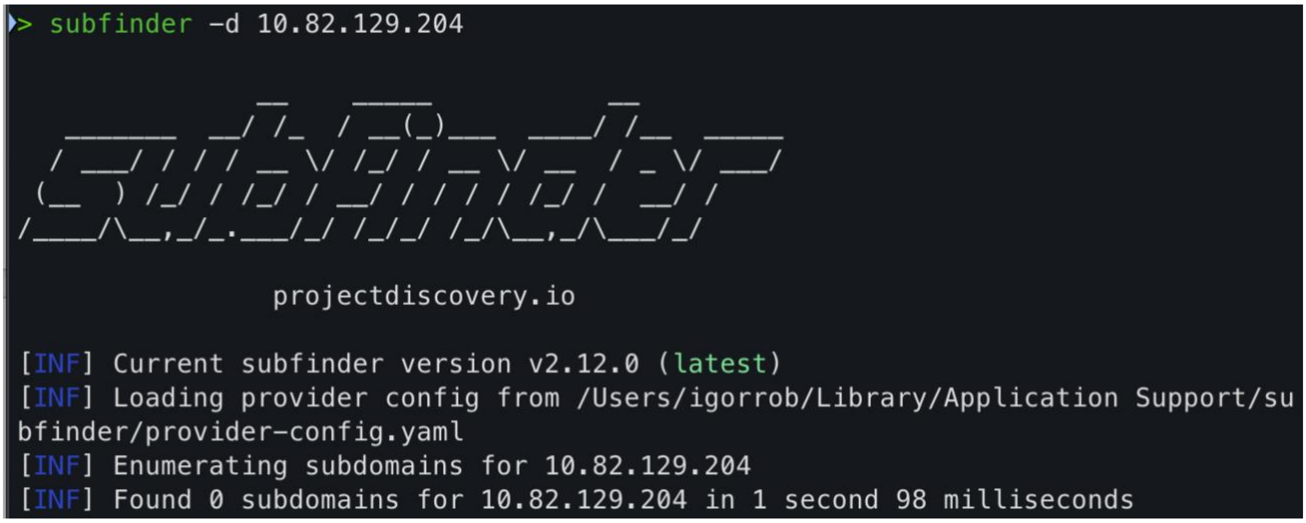
Let's visit the webpage!



https://futurevera.thm/#page-top
FUTUREVERA
FutureVera
We Will Change the Future Together
LEARN MORE

Picture 1: futurevera.thm main page.

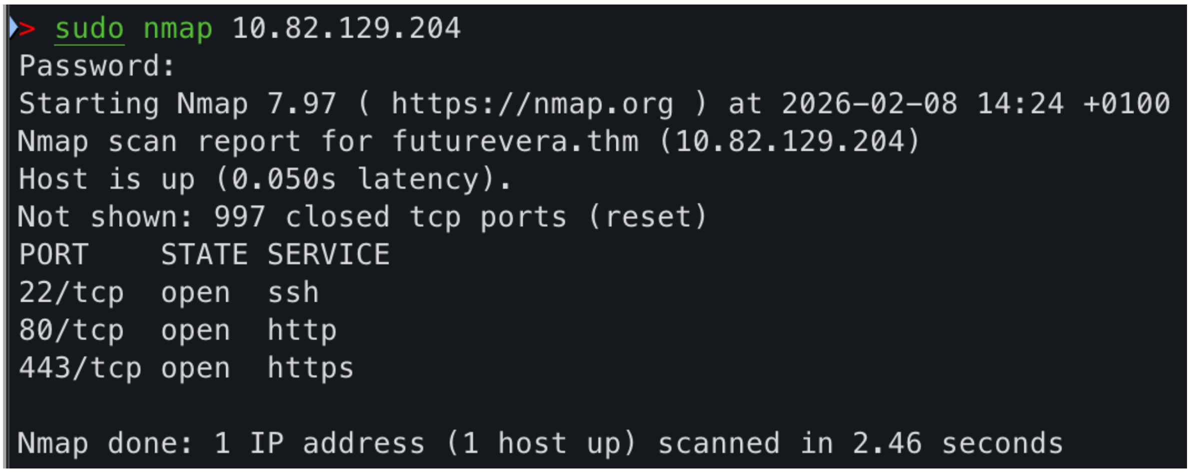
After inspecting the elements and running subfinder to see if there are any subdomains, the results weren't interesting at all.



```
> subfinder -d 10.82.129.204

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.12.0 (latest)
[INF] Loading provider config from /Users/igorrob/Library/Application Support/su
bfinder/provider-config.yaml
[INF] Enumerating subdomains for 10.82.129.204
[INF] Found 0 subdomains for 10.82.129.204 in 1 second 98 milliseconds
```

Picture 2: subfinder results for the webpage.

One classic move is to run nmap and see if there will be something helpful for us.



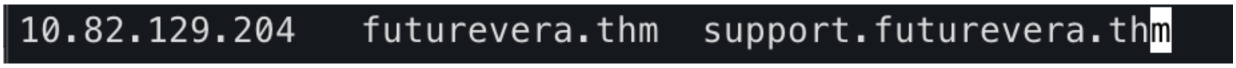
```
> sudo nmap 10.82.129.204
Password:
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-08 14:24 +0100
Nmap scan report for futurevera.thm (10.82.129.204)
Host is up (0.050s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
```

Picture 3: nmap results.

Okay, ports 443 and 80 are open, let's keep that in mind while messing with URLs.

There isn't much info in the webpage but there's something in descriptions. Let's come back and read into it. The narrator states that they're rebuilding their support site. The main theme of this room are subdomains, so let's see if something was hidden in support.futurevera.thm

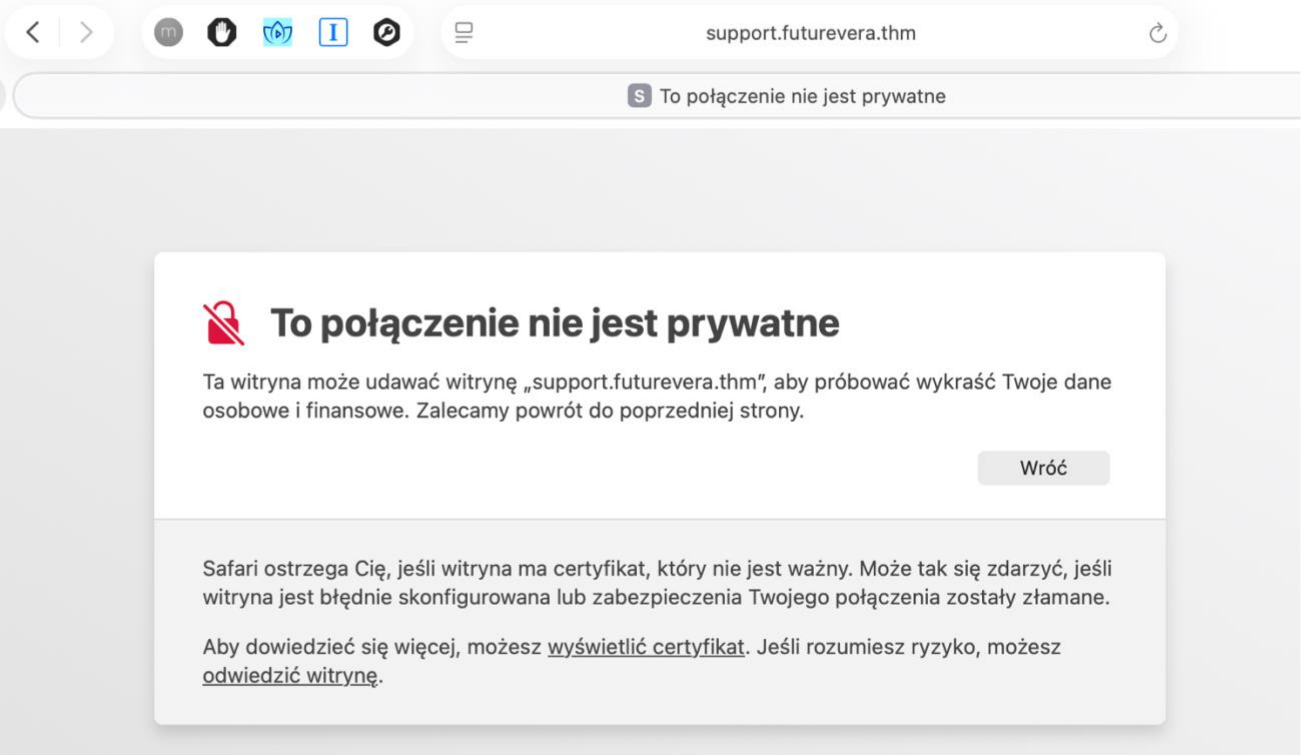
Let’s add those mnemonic names into /etc/hosts



```
10.82.129.204   futurevera.thm   support.futurevera.thm
```

Picture 4: /etc/hosts added line.

Let’s visit that page now.



To połączenie nie jest prywatne

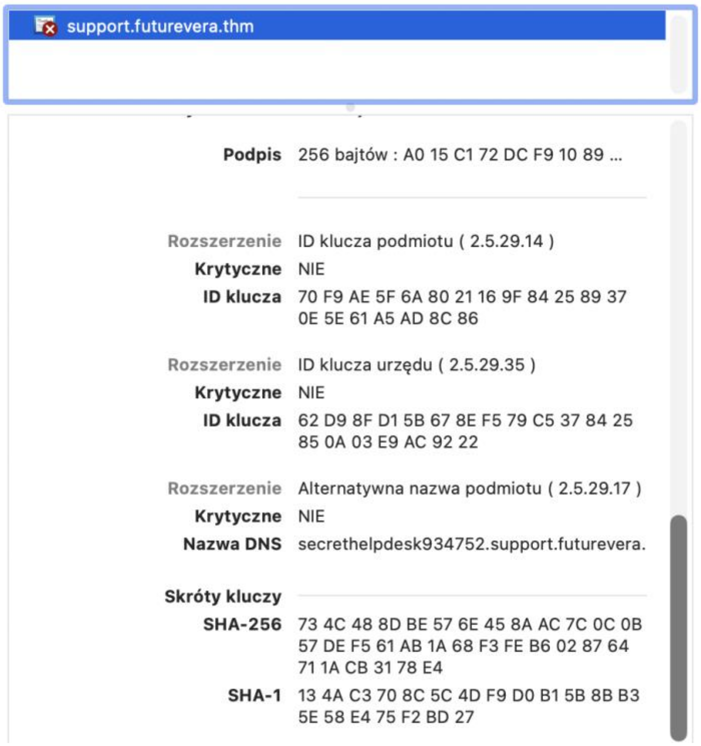
Ta witryna może udawać witrynę „support.futurevera.thm”, aby próbować wykraść Twoje dane osobowe i finansowe. Zalecamy powrót do poprzedniej strony.

Safari ostrzega Cię, jeśli witryna ma certyfikat, który nie jest ważny. Może tak się zdarzyć, jeśli witryna jest błędnie skonfigurowana lub zabezpieczenia Twojego połączenia zostały złamane.

Aby dowiedzieć się więcej, możesz wyświetlić certyfikat. Jeśli rozumiesz ryzyko, możesz odwiedzić witrynę.

Picture 6: „This connection is not private” message (Polish).

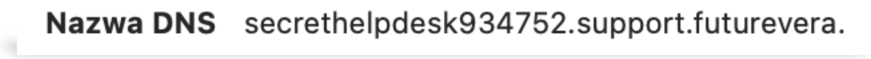
You can skip this warning and head straight into the webpage as I did and find out that it’s just the same. Soi f you need to come back to this warning clear your cookies or cache, or try another browser. Let’s see the certyficate to fin dany info about the page.



support.futurevera.thm

Podpis	256 bajtów : A0 15 C1 72 DC F9 10 89 ...
Rozszerzenie	ID klucza podmiotu (2.5.29.14)
Krytyczne	NIE
ID klucza	70 F9 AE 5F 6A 80 21 16 9F 84 25 89 37 0E 5E 61 A5 AD 8C 86
Rozszerzenie	ID klucza urzędu (2.5.29.35)
Krytyczne	NIE
ID klucza	62 D9 8F D1 5B 67 8E F5 79 C5 37 84 25 85 0A 03 E9 AC 92 22
Rozszerzenie	Alternatywna nazwa podmiotu (2.5.29.17)
Krytyczne	NIE
Nazwa DNS	secrethelpdesk934752.support.futurevera.
Skróty kluczy	
SHA-256	73 4C 48 8D BE 57 6E 45 8A AC 7C 0C 0B 57 DE F5 61 AB 1A 68 F3 FE B6 02 87 64 71 1A CB 31 78 E4
SHA-1	13 4A C3 70 8C 5C 4D F9 D0 B1 5B 8B B3 5E 58 E4 75 F2 BD 27

Picture 7: More information about certyficate (Polish).

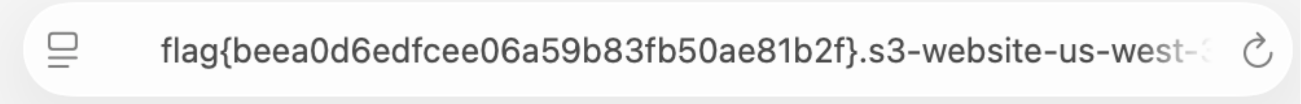


Nazwa DNS secrethelpdesk934752.support.futurevera.

Picture 8: Highlighter information about DNS name.

There’s another subdomain here. Let’s add it again into /etc/hosts file and enter it through browser. (picture from /etc/hosts omitted this time)

After entering the name into the search bar you will get the same warning message (if entered through HTTPS) – if you skip it you will once again find yourself on the front page of futurevera.thm. But remember that the http port is also open. If we enter the helperdesk subdomain through port 80, we will find our flag in the search bar.



flag{beea0d6edfcee06a59b83fb50ae81b2f}.s3-website-us-west-

Picture 9: Found flag.

This room was something very new to me but i surely did learn a lot from it. Hope you had fun!