TakeOver

- Enumeración
  - Ping
  - Nmap
  - HTTP
    - Fuzzing Web

Resolviendo la máquina TakeOver

> En esta publicación, comparto cómo resolví la máquina **TakeOver** de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.141.85
```

```
PING 10.10.141.85 (10.10.141.85) 56(84) bytes of data.
64 bytes from 10.10.141.85: icmp_seq=1 ttl=63 time=42.8 ms

── 10.10.141.85 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 42.840/42.840/42.840/0.000 ms
```

TTL=63 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.141.85 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 07:51 CEST
Initiating SYN Stealth Scan at 07:51
Scanning 10.10.141.85 [65535 ports]
Discovered open port 22/tcp on 10.10.141.85
Discovered open port 443/tcp on 10.10.141.85
Discovered open port 80/tcp on 10.10.141.85
Completed SYN Stealth Scan at 07:51, 12.02s elapsed (65535 total ports)
Nmap scan report for 10.10.141.85
Host is up, received user-set (0.045s latency).
Scanned at 2025-07-24 07:51:19 CEST for 12s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 63
80/tcp  open  http    syn-ack ttl 63
443/tcp open  https   syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.10 seconds
           Raw packets sent: 67271 (2.960MB) | Rcvd: 66659 (2.666MB)
```

`nmap -p22,80,443 -sCV 10.10.141.85`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 07:51 CEST
Nmap scan report for 10.10.141.85
Host is up (0.048s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3f:c3:e8:02:2b:db:90:23:81:f3:91:d6:ba:28:92:6f (RSA)
|   256 bf:4e:92:78:49:db:54:96:b2:12:0f:1b:36:69:65:cb (ECDSA)
|_  256 26:cc:95:c1:0f:47:f2:c0:64:b7:88:1c:7b:a2:86:44 (ED25519)
80/tcp  open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to https://futurevera.thm/
443/tcp open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=futurevera.thm/organizationName=Futurevera/stateOrProvinceName=Oregon/countryName=US
| Not valid before: 2022-03-13T10:05:19
|_Not valid after:  2023-03-13T10:05:19
|_http-title: FutureVera
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds
```

HTTP

Fuzzing Web

Se añade al `/etc/hosts`.

`echo "10.10.141.85 futurevera.thm" >> /etc/hosts`

`gobuster dir -u futurevera.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://futurevera.thm
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 279]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

`dirsearch -u futurevera.thm -t 50 -i 200`

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 11460

Output File: /home/manumore/Escritorio/manumore/Laboratorios/TryHackMe/TakeOver/reports/_futurevera.thm/_25-07-24_07-57-08.txt

Target: https://futurevera.thm/

[07:57:08] Starting:
[07:57:18] 200 -  491B  - /assets/
[07:57:24] 200 -  495B  - /js/

Task Completed
```

`dirb https://futurevera.thm/`

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 24 08:01:19 2025
URL_BASE: https://futurevera.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://futurevera.thm/ ----
==> DIRECTORY: https://futurevera.thm/assets/
==> DIRECTORY: https://futurevera.thm/css/
+ https://futurevera.thm/index.html (CODE:200|SIZE:4605)
==> DIRECTORY: https://futurevera.thm/js/
+ https://futurevera.thm/server-status (CODE:403|SIZE:280)

---- Entering directory: https://futurevera.thm/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://futurevera.thm/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://futurevera.thm/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Jul 24 08:05:23 2025
DOWNLOADED: 4612 - FOUND: 2
```

`wfuzz -c --hl=0 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -H "Host: FUZZ.futurevera.thm" -u 10.10.141.85`

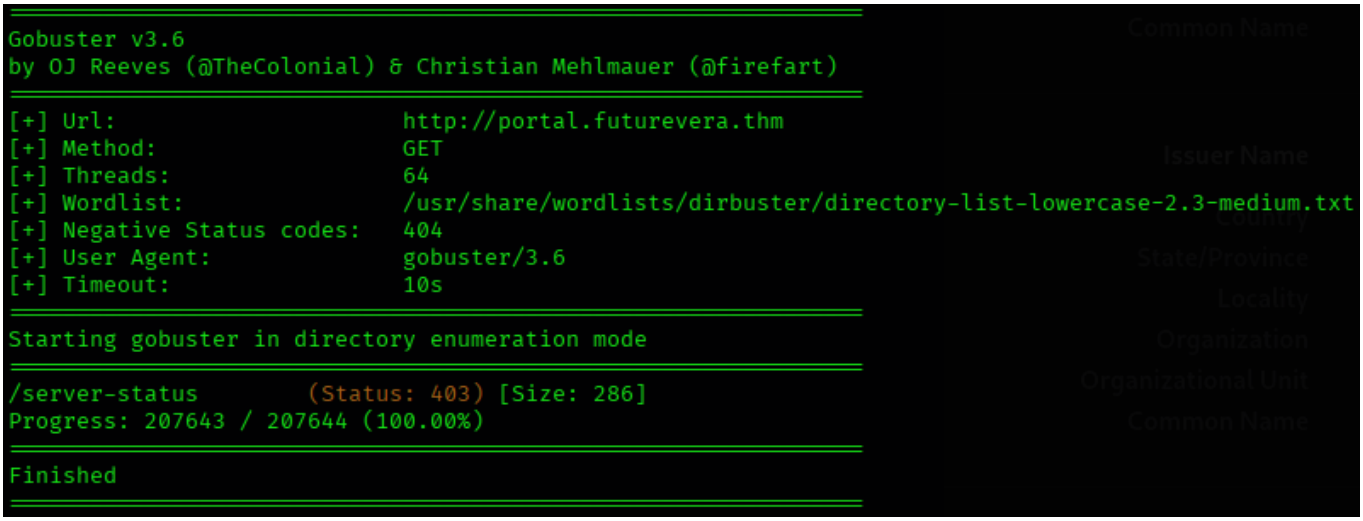
```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.141.85/
Total requests: 19966

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000048:   200        1 L      9 W        69 Ch       "portal"
000005309:   200        1 L      9 W        70 Ch       "payroll"
000009532:   400        10 L     35 W       334 Ch      "#www"
000010581:   400        10 L     35 W       334 Ch      "#mail"

Total time: 105.8577
Processed Requests: 19966
Filtered Requests: 19962
Requests/sec.: 188.6115
```

Se añaden al `/etc/hosts`.

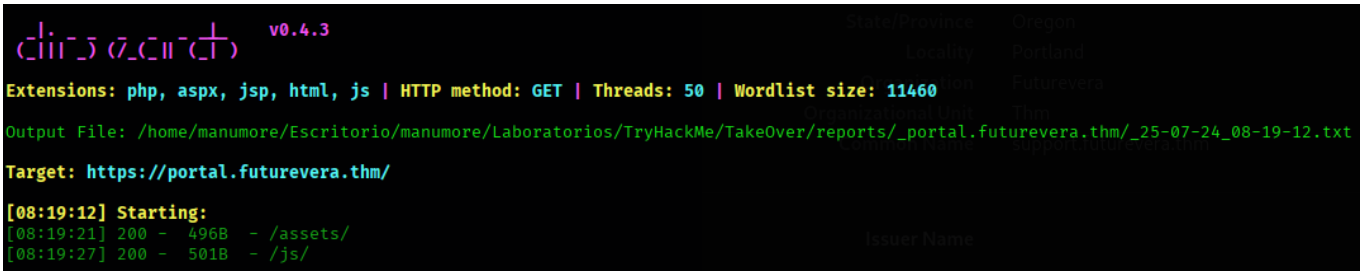
```
echo "10.10.141.85 portal.futurevera.thm" >> /etc/hosts
```

```
echo "10.10.141.85 payroll.futurevera.thm" >> /etc/hosts
```

```
gobuster dir -u portal.futurevera.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```




```
dirsearch -u portal.futurevera.thm -t 50 -i 200
```




```
dirb https://portal.futurevera.thm/
```

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 24 08:14:42 2025
URL_BASE: https://portal.futurevera.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://portal.futurevera.thm/ ----
==> DIRECTORY: https://portal.futurevera.thm/assets/
==> DIRECTORY: https://portal.futurevera.thm/css/
+ https://portal.futurevera.thm/index.html (CODE:200|SIZE:4605)
==> DIRECTORY: https://portal.futurevera.thm/js/
+ https://portal.futurevera.thm/server-status (CODE:403|SIZE:287)

---- Entering directory: https://portal.futurevera.thm/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://portal.futurevera.thm/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://portal.futurevera.thm/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Jul 24 08:18:45 2025
DOWNLOADED: 4612 - FOUND: 2
```

`gobuster dir -u payroll.futurevera.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://payroll.futurevera.thm
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 287]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

`dirsearch -u payroll.futurevera.thm -t 50 -i 200`

```
v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 11460

Output File: /home/manumore/Escritorio/manumore/Laboratorios/TryHackMe/TakeOver/reports/_payroll.futurevera.thm/_25-07-24_08-27-41.txt

Target: https://payroll.futurevera.thm/

[08:27:41] Starting:
[08:27:50] 200 -  497B  - /assets/
[08:27:56] 200 -  502B  - /js/

Task Completed
```

`dirb https://payroll.futurevera.thm/`

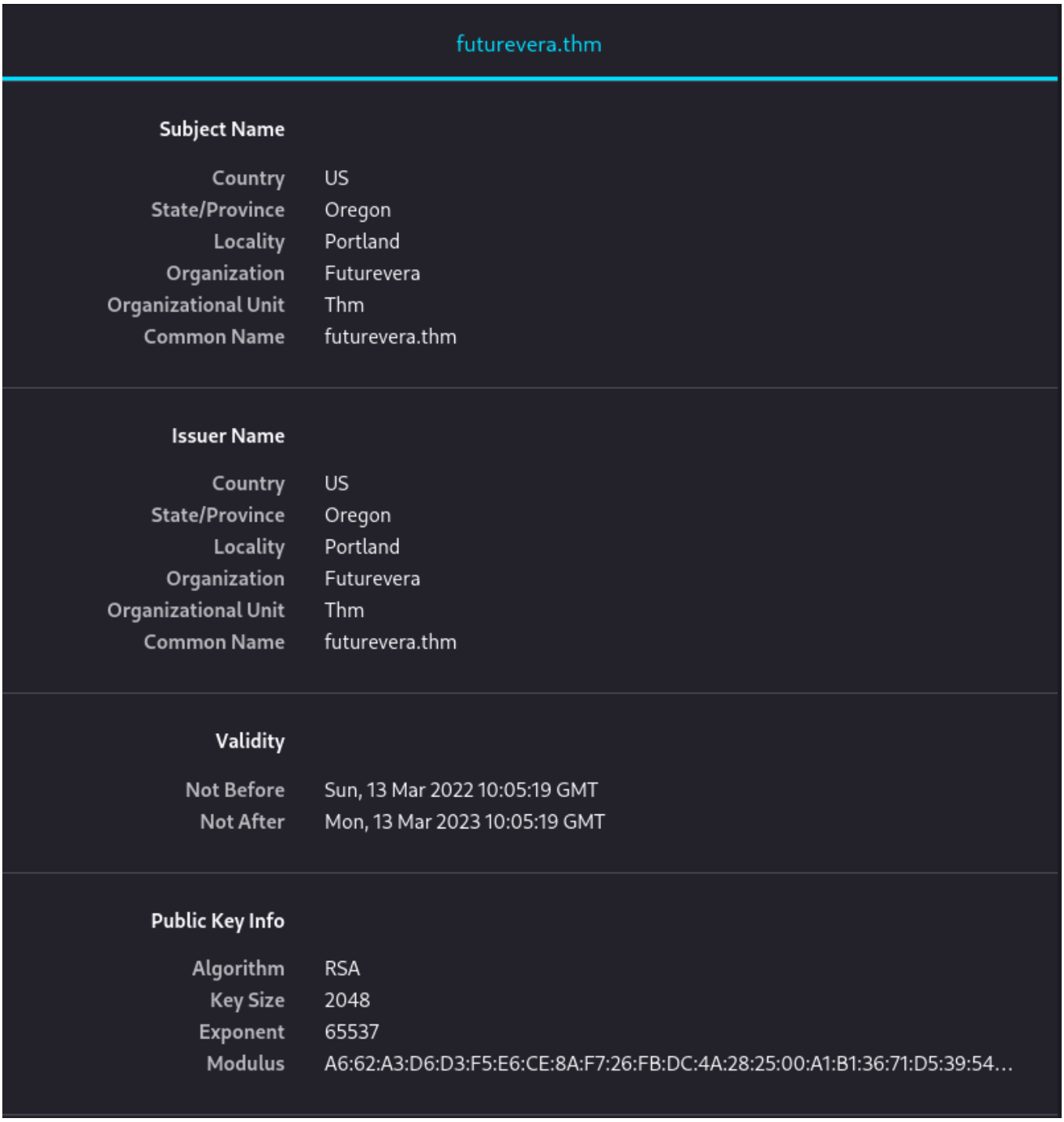
```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 24 08:23:14 2025
URL_BASE: https://payroll.futurevera.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://payroll.futurevera.thm/ ----
==> DIRECTORY: https://payroll.futurevera.thm/assets/
==> DIRECTORY: https://payroll.futurevera.thm/css/
+ https://payroll.futurevera.thm/index.html (CODE:200|SIZE:4605)
==> DIRECTORY: https://payroll.futurevera.thm/js/
+ https://payroll.futurevera.thm/server-status (CODE:403|SIZE:288)

---- Entering directory: https://payroll.futurevera.thm/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://payroll.futurevera.thm/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://payroll.futurevera.thm/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Jul 24 08:27:13 2025
DOWNLOADED: 4612 - FOUND: 2
```

Se procede a revisar todos los directorios encontrados:

- `futurevera.thm`.
  - `/index.html`.
  - `/assets`.
  - `/js`.
  - `/css`.

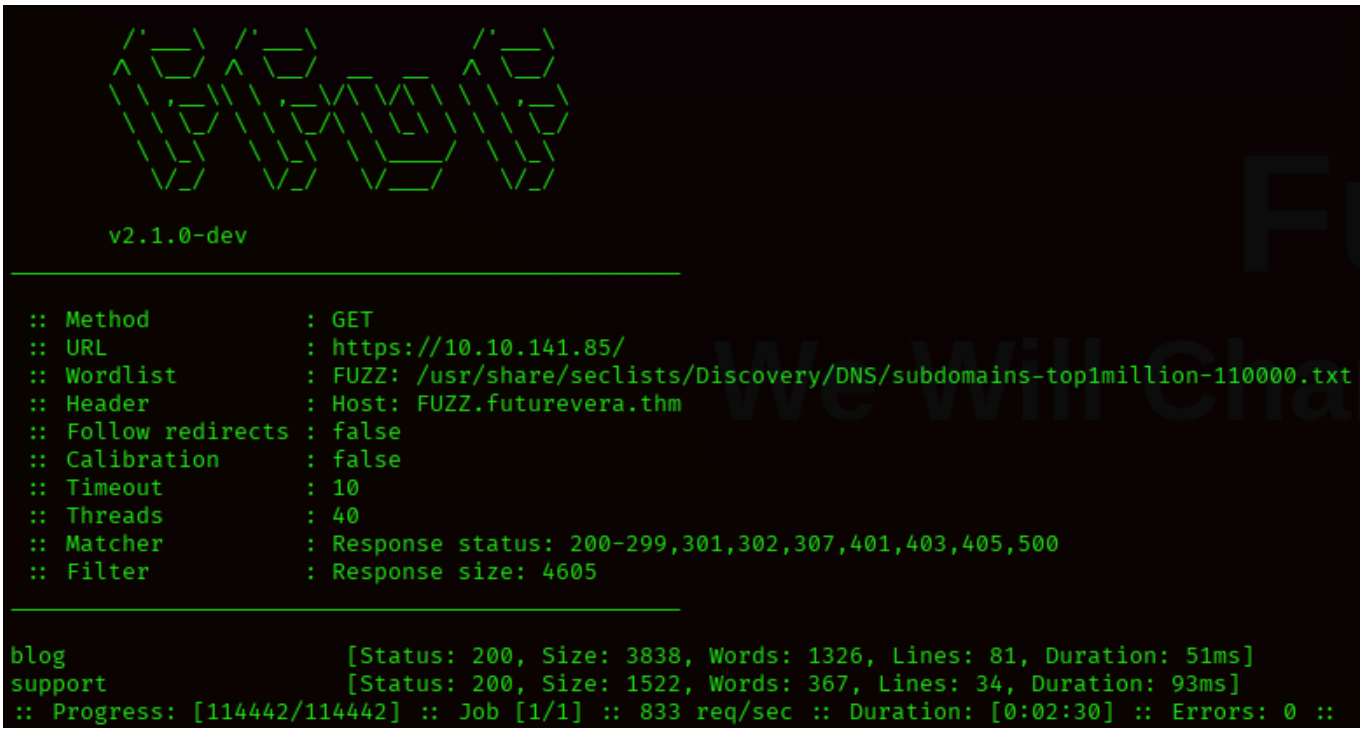
    - `/server-status`.
- `portal.futurevera.thm`.
    - `/index.html`.
    - `/assets`.
    - `/js`.
    - `/css`.
    - `/server-status`.
- `payroll.futurevera.thm/`.
    - `/index.html`.
    - `/assets`.
    - `/js`.
    - `/css`.
    - `/server-status`.

Al no encontrar nada, se procede a mirar información en el certificado.



No se encuentra nada, se procede a volver a realizar *fuzzing web* con la herramienta *ffuf*.

```
ffuf -u https://10.10.141.85/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.futurevera.thm" -fs 4605
```



Se añaden al `/etc/hosts`.

```
echo "10.10.141.85 blog.futurevera.thm" >> /etc/hosts
```

```
echo "10.10.141.85 support.futurevera.thm" >> /etc/hosts
```

Se procede a mirar información en el certificado.

blog.futurevera.thm

Subject Name

Country	US
State/Province	Oregon
Locality	Portland
Organization	Futurevera
Organizational Unit	Thm
Common Name	blog.futurevera.thm

Issuer Name

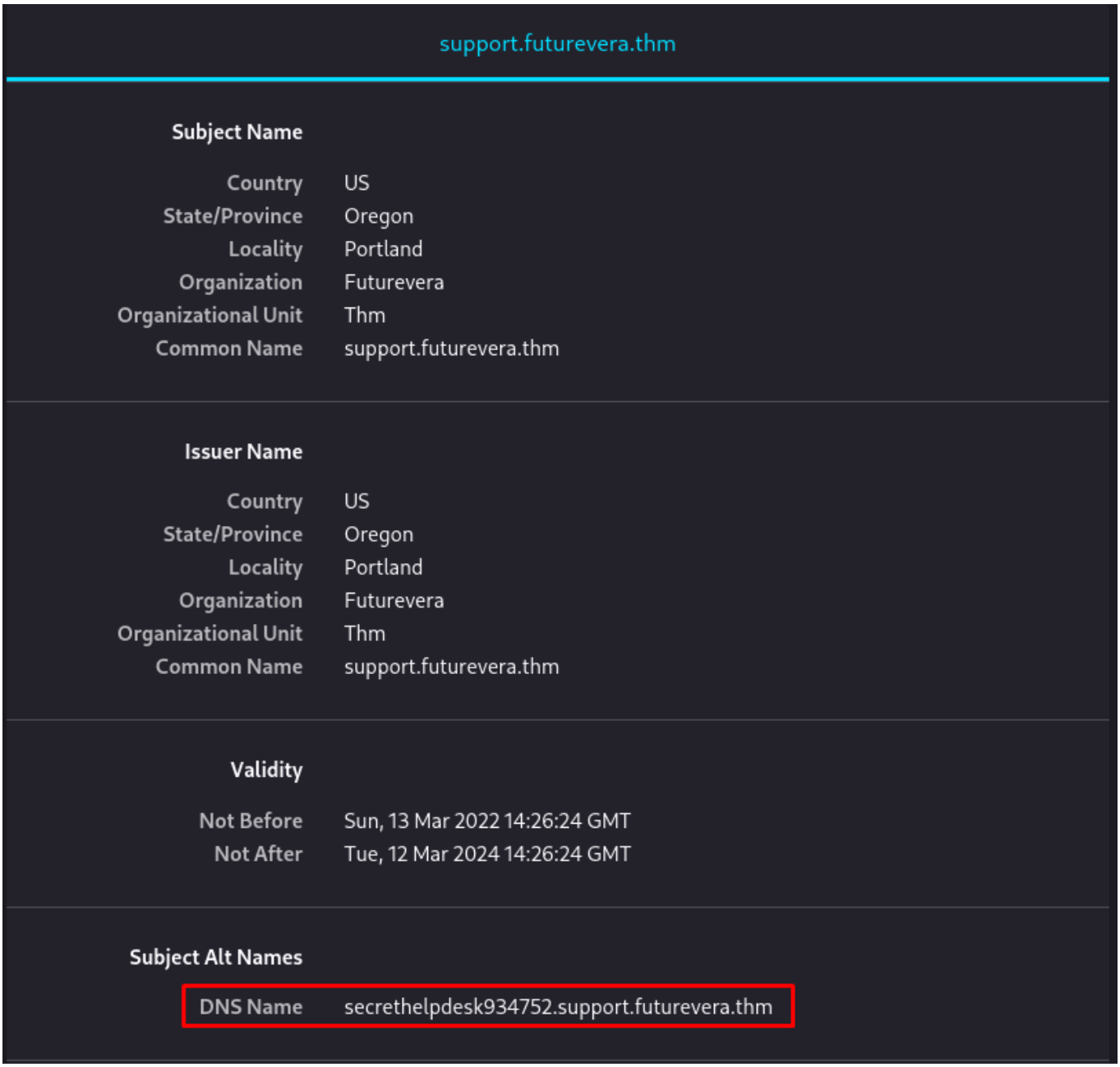
Country	US
State/Province	Oregon
Locality	Portland
Organization	Futurevera
Organizational Unit	Thm
Common Name	blog.futurevera.thm

Validity

Not Before	Sun, 13 Mar 2022 10:22:57 GMT
Not After	Mon, 13 Mar 2023 10:22:57 GMT

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CB:6F:F7:3D:85:ED:EA:86:CF:47:EC:EC:12:FA:94:5E:8E:D9:1C:F7:CE:2B:2B:95…



Se añade al `/etc/hosts`.

```
echo "10.10.141.85 secrethelpdesk934752.support.futurevera.thm" >> /etc/hosts
```

`http://secrethelpdesk934752.support.futurevera.thm`