


# Write-Up: Máquina "TakeOver"

 **Plataforma:** Try Hack Me

 **Dificultad:** Fácil

 **Autor:** Joaquín Picazo

---

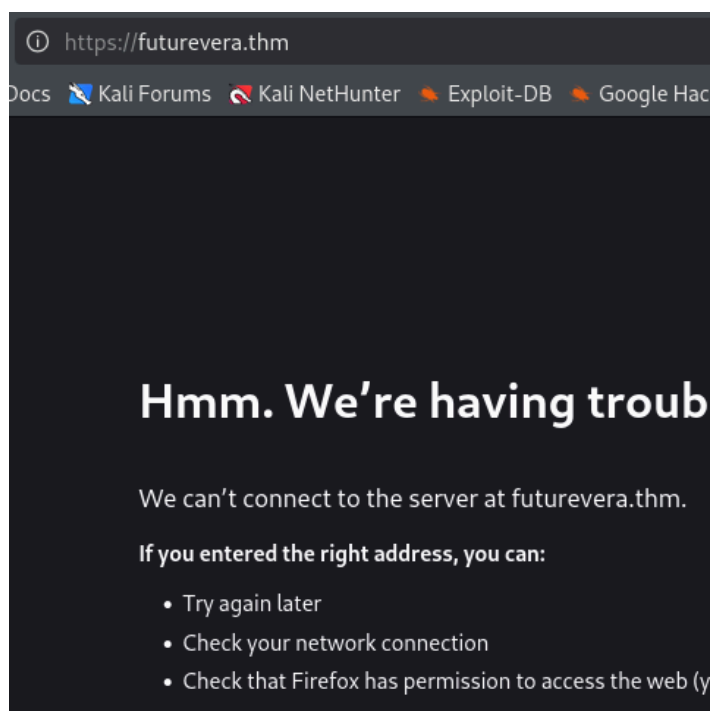
## Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
  - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
  - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
- 

## 1. Reconocimiento y Recolección de Información

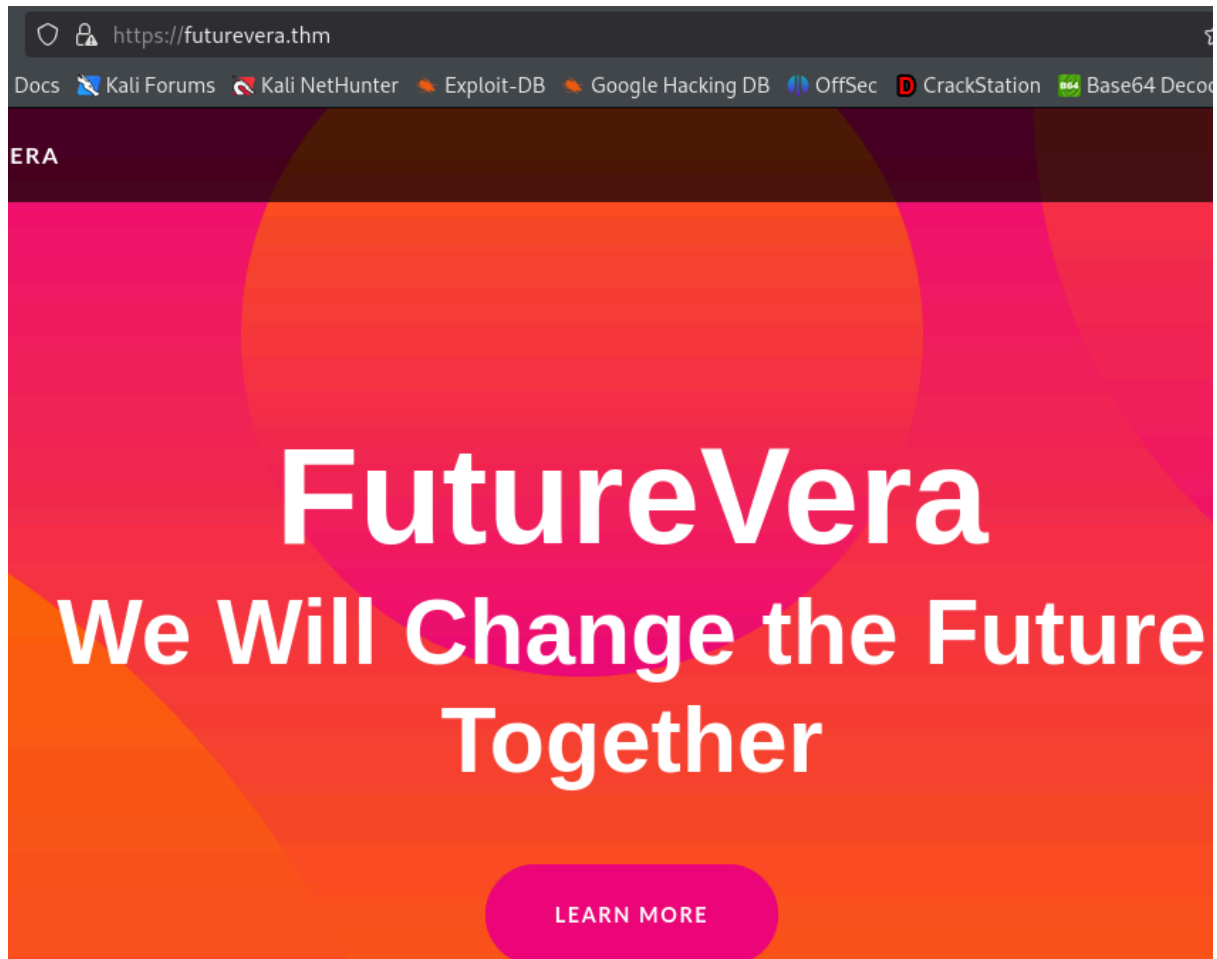
Ingreso a la web mediante la IP otorgada y me dice que no se puede acceder, además me da un dominio al cual está relacionado.



Añadir la IP otorgada a **/etc/hosts** y la relaciono al dominio para que utilice a este.

```
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
10.10.14.138 futurevera.thm
```

Reinicio la página para volver a intentar hacer conexión y ahora carga correctamente.



## 2. Escaneo y Enumeración

Hago fuzzing para subdominios con ffuf.

```
(root@kali)~# ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host: FUZZ.futurevera.thm" -u https://10.10.14.138 -fs 4605

v2.1.0-dev

:: Method      : GET
:: URL         : https://10.10.14.138
:: Wordlist    : FUZZ: /usr/share/wordlists/SecLists/Discovery/DNS/namelist.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: 4605

blog      [Status: 200, Size: 3838, Words: 1326, Lines: 81, Duration: 237ms]
support   [Status: 200, Size: 1522, Words: 367, Lines: 34, Duration: 235ms]
```

Encuentra “blog” y “support”. Hay que añadirlos a **/etc/hosts** para que se relacionen y funcionen al intentar ingresar.

```
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.10.14.138 futurevera.thm support.futurevera.thm
```

Ingreso al certificado de la web de **support.futurevera.thm** y me aparece el siguiente subdominio

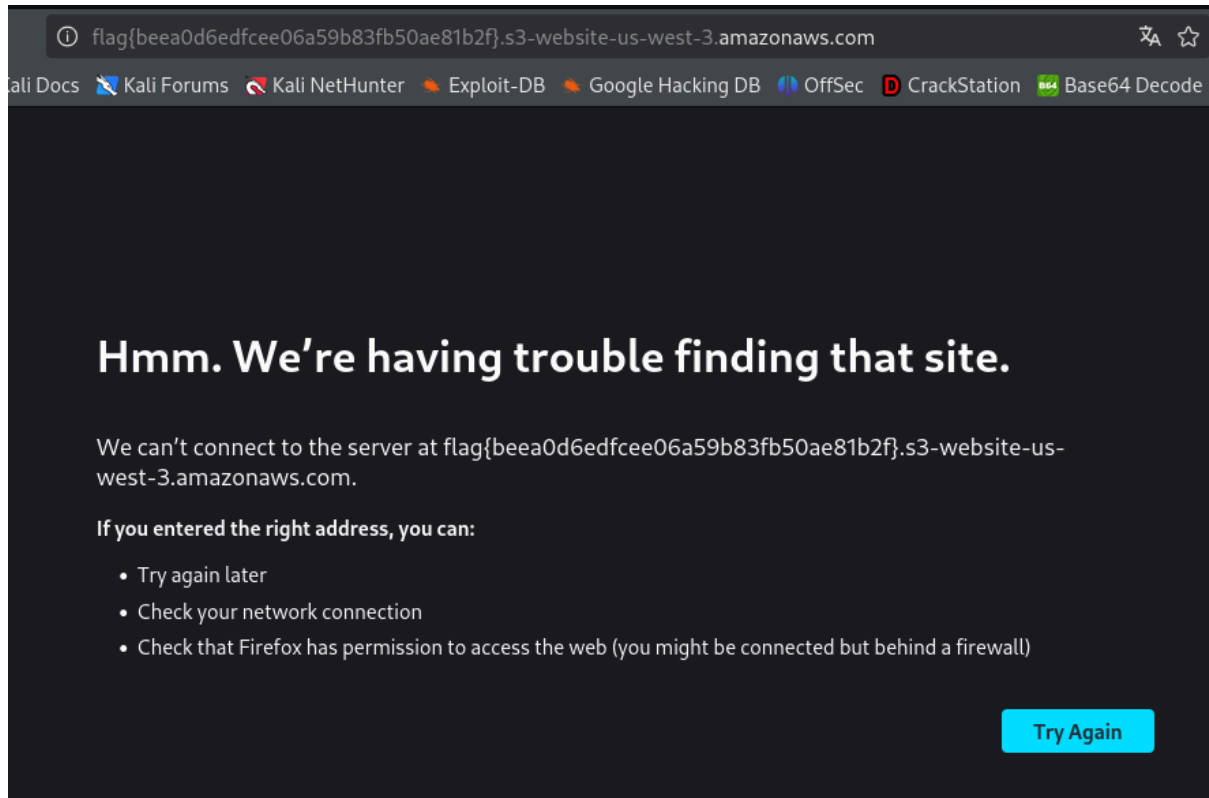
Organization	Futurevera
Organizational Unit	Thm
Common Name	support.futurevera.thm
Issuer Name	
Country	US
State/Province	Oregon
Locality	Portland
Organization	Futurevera
Organizational Unit	Thm
Common Name	support.futurevera.thm
Validity	
Not Before	Sun, 13 Mar 2022 14:26:24 GMT
Not After	Tue, 12 Mar 2024 14:26:24 GMT
Subject Alt Names	
DNS Name	secrethelpdesk934752.support.futurevera.thm

### 🌟 3. Explotación de Vulnerabilidades

Añado el subdominio encontrado anteriormente a **/etc/hosts** para poder acceder a este.

```
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.10.14.138 futurevera.thm support.futurevera.thm secrethelpdesk934752.support.futurevera.thm
```

Luego, ingresé a <http://secrethelpdesk934752.support.futurevera.thm> y me cambió la dirección url, la cual muestra la flag.



### 🏆 Banderas y Resultados

- ✓ **Subdominios:** Se obtuvo la dirección de los subdominios exitosamente.
- ✓ **Bandera:** Se obtuvo la bandera exitosamente.

**Nota:** Más que un hackeo, esta máquina trató de enumerar subdominios con herramientas como ffuf. Por lo tanto no hubo una gran “explotación” o “escalada de privilegios”.