

Write-up paso a paso – Máquina TakeOver

Objetivo: Determinar qué activos pueden ser “tomados” (takeover) mediante enumeración de subdominios y análisis de certificados SSL, obteniendo la *flag* final.

0. Preparación (resolución DNS local)

La máquina requiere resolver el dominio `futurevera.thm` hacia la IP objetivo.

Acción

Editar el archivo `/etc/hosts`:

```
sudo nano /etc/hosts
```

Agregar una línea:

```
10.81.156.209 futurevera.thm
```

```
root@kali: /home/kali
Session Actions Edit View Help
GNU nano 8.7 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.81.156.209 futurevera.thm

Information
```

1. Reconocimiento de puertos y servicios

Se enumeran los puertos abiertos para identificar la superficie de ataque.

Acción

```
nmap -p- -open -sS -sC -sV --min-rate=5000 -n -Pn 10.81.156.209
```

Resultado

Servicios encontrados:

- **22/tcp** SSH
- **80/tcp** HTTP (redirige a HTTPS)
- **443/tcp** HTTPS

```
(root@kali)-[/home/kali]
# nmap -p- -open -sS -sC -sV --min-rate=5000 -n -vvv -Pn 10.81.156.209
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 62  OpenSSH 8.2p1 Ubuntu 4ubuntu0.13
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b1:c4:ba:cb:58:cc:2c:2b:6f:3d:31:05:bf:8c:65:79 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgQBVCiJWjhr5SSJNIPvWADs3YhMeBkObAsoJn3sV8Sv
iE0497M0slame7PeGU3fFjgQolr2qsfx5LH1uj69nTFiYeLLjHLGc0cgVaWsTiH07E7E1fb2
x0aiS1TRIXeHDHyZWKUW07oXEgCvs1XpQc2RQEdJRbrBcXSfp3GZYPmcAGUR9BshMW0weKhd
ouS8HDL5u15iBtyKtPGoqCCE4WS33Eb2HjWcV5oKpkHqjZbWhMiNAwSXhMsGLoeQb/kFMqXk
ftAoCfrqiZ7REOTqS/1WG2aRzqu+6ZqYS/uJCxZVkhPFmbMHusue2EvcCnT+CGWmym1aBHVH
PzHkhn4+ogiFY883Jppn645zoSCokyGaBtS6R/Ye+WBchG78ofr3G5RMV4Xo6ZJ3tG9pGuP9
JPtI10D4y616I8LdIwwV8X1HCb/lzg2p+NbYptrR9k5jrF37Aqi2ndAJDeu015fTpkCxfkVP
tvhM8Ms1RsJ+OVJSky40BNzOIUseKLntrPABGBs=
|   256 4b:2e:11:43:dd:35:ca:ac:dd:c1:07:25:d1:e3:eb:da (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGGOD09xKyUlpyrIICi+
0+GeZpHDDbM6+a+3iroky7VW/NOK4w8vYOn1Bay6CDchFEL36CVX05IMf109JzRG9Ig=
|   256 48:f4:d8:53:0a:6e:77:7b:86:5e:a2:59:59:cc:3c:13 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDhGTItNMudMjJDxteqz9s4Z1v+6RsxHL/UCyUD5U3bG
80/tcp    open  http      syn-ack ttl 62  Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to https://futurevera.thm/
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
443/tcp    open  ssl/http  syn-ack ttl 62  Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
```

```
| ssl-cert: Subject:
commonName=futurevera.thm/organizationName=Futurevera/stateOrProvinceName=Oregon/countryName=US/organizationalUnitName=Thm/localityName=Portland
| Issuer:
commonName=futurevera.thm/organizationName=Futurevera/stateOrProvinceName=Oregon/countryName=US/organizationalUnitName=Thm/localityName=Portland
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-13T10:05:19
| Not valid after: 2023-03-13T10:05:19
| MD5: 2e8d 6097 6b23 188c 06d5 f2cd 8def dd3a
| SHA-1: 8023 fcfc 5e63 a29b 3d5e eAAF 8f70 8b35 d8eb c120
| SHA-256: bdfF 4317 03bb 91a1 2144 4c8f e62a 2842 3b72 7169 858a 1f5f
f618 dd3f efb0 aa33
| -----BEGIN CERTIFICATE-----
| MIIDuzCCAqOgAwIBAgIUMx0OgCh/xob6nWlsHR+iKDXKZRkwDQYJKoZIhvcNAQEL
| BQAwbTELMAkGA1UEBhMCVVMxZDZANBgNVBAGMBk9yZWdvbjERMA8GA1UEBwwIUg9y
| dGxhbmQxEzARBgNVBAoMCKZ1dHVyZXZlcmExDDAKBgNVBAsMA1RobTEXMBUGA1UE
| AwwOZnV0dXJldmVyYS50aG0wHhcNMjIwMzEzMTAwNTE5WhcNMjMwMzEzMTAwNTE5
| WjBtMQswCQYDVQQGEwJVUzEPMA0GA1UECAwGT3JlZ29uMREwDwYDVQQHDAhQb3J0
| bGFuZDEtMBEGA1UECgwKRnV0dXJldmVyYTEMMAoGA1UECwwDVGhtMRcwFQYDVQQD
| DA5mdXR1cmV2ZXJhLnRobTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AKZio9bT9eb0ivcm+9xKKCUAobE2cdU5VFbi1Ve7oxsSGKWWecsqLUn7tFj1jjKq
| hWDMZXxEW6aN3jU5p5zF6ATmwIuvNQqWZ0aK8iKjXs8IWEBIQyz/iKBF6deWrN+8
| II+whTaSberFaND2G0VchB7OrOu/mlP1KNhm2kEKwak7YHxvFkSp7Nmu2yTQAnyp
| WK2CBh3tdeGSq7/lyo8W3la/kPKhb4lmtBMS/tKPFs1Mxl0v0cSbNsvFVgJQ7jti
| OZKPo/DAeaFIFB/32HocscQXM2VdQNXnQ06M1cbBNskYWzvw6di+wYzjjCWtM4o
| Rg+3c/k5hqkEftEiwV7xAXcCAwEAAaNTMFEwHQYDVR0OBBYEFD23WEw1BMTDTPWI
| 0eMU0IMaJyPJMB8GA1UdIwQYMBaAFD23WEw1BMTDTPWI0eMU0IMaJyPJMA8GA1Ud
| EwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBACu3W2VV8zRdD4M7oUWN8S6f
| lM1z8aCkSckgFDEX7jtyJjWMQVwPizKkX17XQs6EgnWqD/PVt2Tf9dRhUH6FQmTK
| qh35hnsS0d03sQB8CnQ3Sn1beUYXY2mY/aUhz/1Akx6mURGuSen8BSbuL4mcm5Dk
| AXxfa+SHc5XAjuYS1XVUSPy8noqFOLxvcGz+zPN2RQYwQkMDgQtUX2n0VcjwgTLN
| bEuEm210+IGPX+ZEQWsnSSmz0SyUryBwc5BsJMaFUdAncxEBKcN1p4oN8gm6NQ32
| FHFbghTgLGMTahuLWpXdeuVF87+pHU1roRHdgb1Qtb2wSwqVaDGHafFiZcUMv/Y=
| -----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_ http/1.1
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: FutureVera
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2. Enumeración de tecnologías web

Se identifica el comportamiento HTTP/HTTPS y tecnologías visibles.

Acción

```
whatweb http://futurevera.thm
```

Resultado

- HTTP realiza **redirect** a `https://futurevera.thm/`
- Servidor Apache en Ubuntu

```
(root@kali)-[/home/kali]
└─# whatweb http://futurevera.thm
http://futurevera.thm [302 Found] Apache[2.4.41], Country[RESERVED][ZZ],
HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.81.156.209],
RedirectLocation[https://futurevera.thm/]
https://futurevera.thm/ [200 OK] Apache[2.4.41], Bootstrap,
Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41
(Ubuntu)], IP[10.81.156.209], Script, Title[FutureVera]
```

3. Enumeración de subdominios (VHOST)

Se busca la existencia de subdominios configurados en el servidor.

Acción

```
gobuster vhost -u futurevera.thm \
-w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt \
-t 50 --append-domain
```

Resultado

Se descubre el subdominio:

- `portal.futurevera.thm`

```
(root@kali)-[/home/kali]
└─# gobuster vhost -u futurevera.thm -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 50
--append-domain
=====
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
```

```
[+] Url: http://futurevera.thm
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent: gobuster/3.8.2
[+] Timeout: 10s
[+] Append Domain: true
[+] Exclude Hostname Length: false

=====
Starting gobuster in VHOST enumeration mode
=====
portal.futurevera.thm Status: 200 [Size: 69]
Progress: 4989 / 4989 (100.00%)
=====
Finished
=====
```

4. Añadir subdominio descubierto al hosts

Para poder acceder al subdominio recién descubierto, se añade a `/etc/hosts`.

Acción

```
10.81.156.209 futurevera.thm portal.futurevera.thm
```

```
Session Actions Edit View Help
GNU nano 8.7 /etc,
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.81.156.209 futurevera.thm portal.futurevera.thm
```

5. Inferencia de subdominios por contexto

Leyendo la descripción del sitio, se menciona que publican un **blog** y que el **support** está en reconstrucción. Esto sugiere la posible existencia de subdominios.

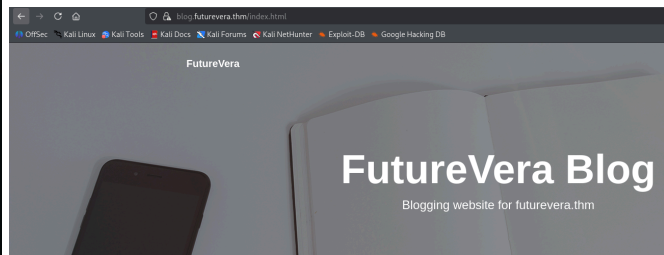
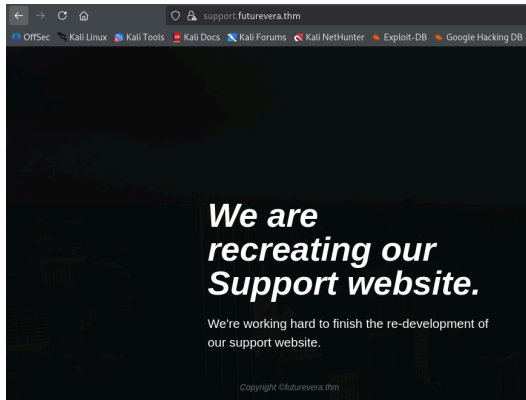
Acción

Se prueban manualmente:

- `blog.futurevera.thm`
- `support.futurevera.thm`

Se añaden al `/etc/hosts`:

```
10.81.156.209 futurevera.thm portal.futurevera.thm blog.futurevera.thm
support.futurevera.thm
```



6. Análisis del certificado SSL (SAN)

El objetivo es identificar subdominios internos filtrados por el certificado SSL, especialmente en `support.futurevera.thm`.

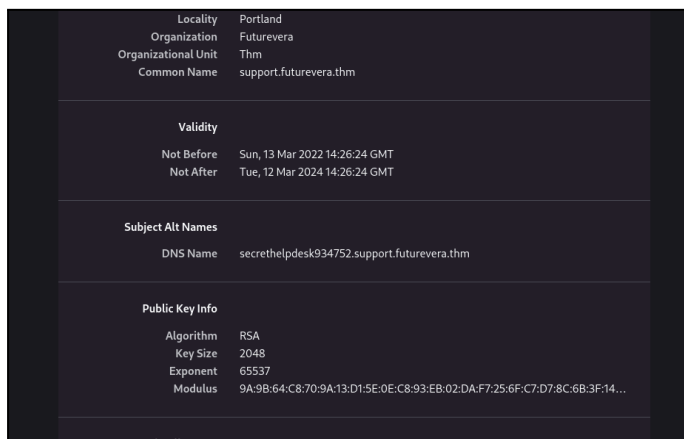
Acción

- Abrir `https://support.futurevera.thm`
- Inspeccionar el certificado SSL.
- Revisar la sección **Subject Alternative Names (SAN)**.

Resultado

Se encuentra un DNS interno adicional expuesto en el certificado:

- `secrethelpdesk934752.support.futurevera.thm`



7. Acceso al subdominio oculto

Se agrega el nuevo DNS descubierto al `/etc/hosts`.

Acción

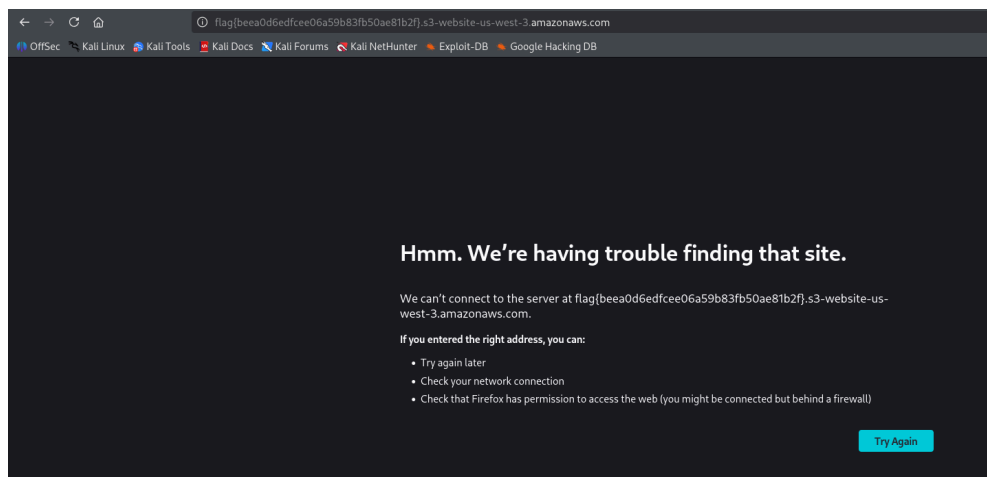
```
10.81.156.209  secrethelpdesk934752.support.futurevera.thm
```

Se accede al subdominio:

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

Resultado

El subdominio redirige a un recurso externo en AWS S3 (website endpoint), indicando un escenario típico de **Subdomain Takeover**.



8. Obtención de la flag

Siguiendo la redirección se obtiene la flag:

- `flag{beea0d6edfcee06a59b83fb50ae81b2f}`

Conclusión

La máquina demuestra un escenario realista de riesgo por:

- Enumeración de subdominios (VHOST)
- Filtración de subdominios internos en certificados SSL (SAN)
- Redirección a un recurso cloud externo (S3) que podría permitir **toma de control del subdominio** si el recurso no está correctamente gestionado.

El impacto potencial incluye secuestro de subdominio, phishing y distribución de contenido malicioso bajo un dominio legítimo.