fooding Apache Active-MQ exploitation

```
└─# nmap -sCV -p80,443,1883,5672,8161,43685,61613,61614,61616 -vvv 172.17.0.2 -oG nmap
```

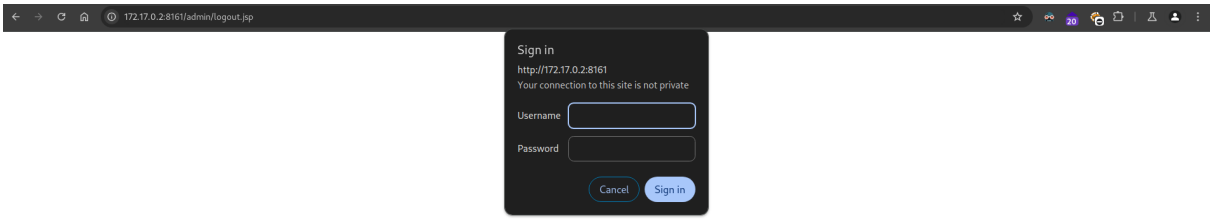
```
PORT      STATE SERVICE    REASON         VERSION
80/tcp    open  http       syn-ack ttl 64 Apache httpd 2.4.59
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.59 (Debian)
443/tcp   open  ssl/http   syn-ack ttl 64 Apache httpd 2.4.59
| tls-alpn:
|_  http/1.1
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=example.com/organizationName=
| Issuer: commonName=example.com/organizationName=Your Organi
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-04-17T08:32:44
| Not valid after:  2025-04-17T08:32:44
| MD5:   6db1:ccf0:3432:12a4:6df3:3a53:00fd:3c83
| SHA-1: 5873:f2c7:0b48:7593:1961:569c:2a4b:e4d5:fc46:956d
| http-server-header: Apache/2.4.59 (Debian)
|_http-title: DockerLabs | Plantilla gratuita Bootstrap 4.3.x
1883/tcp  open  mqtt       syn-ack ttl 64
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     ActiveMQ/Advisory/MasterBroker:
|_    ActiveMQ/Advisory/Consumer/Topic/#:
5672/tcp  open  amqp?      syn-ack ttl 64
| fingerprint-strings:
```

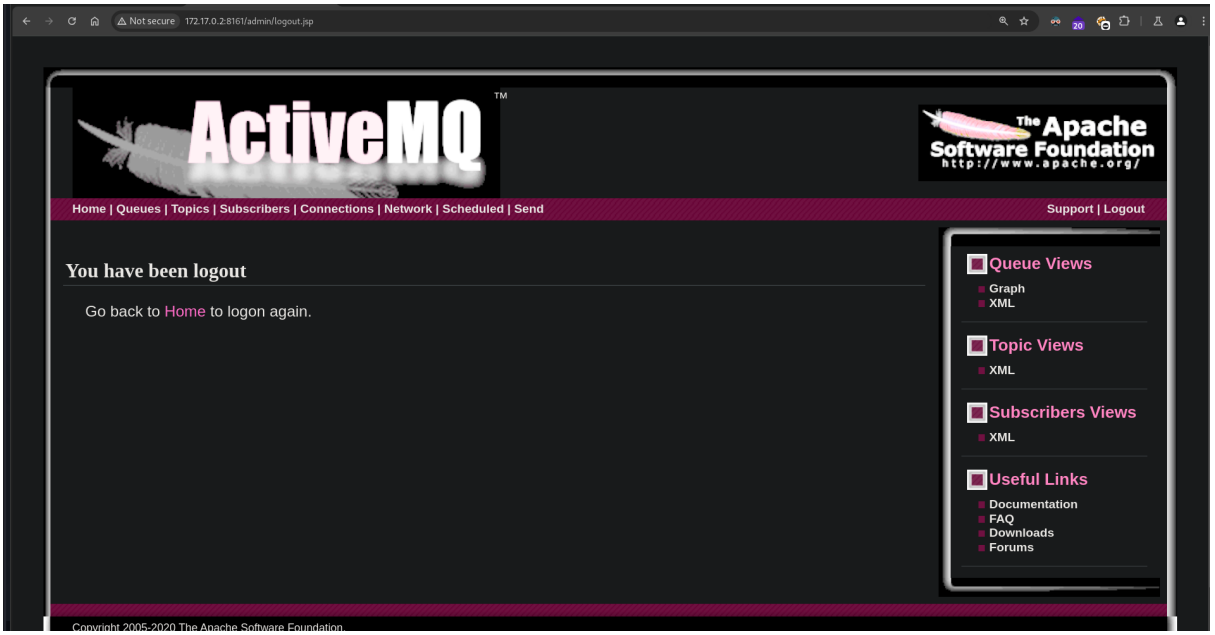
```
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GetRequest, HT
|     AMQP
|     AMQP
|     amqp:decode-error
|_    7Connection from client using unsupported AMQP attempte
|_amqp-info: ERROR: AQMP:handshake expected header (1) frame,
8161/tcp  open  http       syn-ack ttl 64 Jetty 9.4.39.v20210
|_http-server-header: Jetty(9.4.39.v20210325)
|_http-title: Error 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
43685/tcp open  tcpwrapped syn-ack ttl 64
61613/tcp open  stomp      syn-ack ttl 64 Apache ActiveMQ
| fingerprint-strings:
|   HELP4STOMP:
|     ERROR
|     content-type:text/plain
|     message:Unknown STOMP action: HELP
|     org.apache.activemq.transport.stomp.ProtocolException:
|     org.apache.activemq.transport.stomp.ProtocolConverter.o
|     org.apache.activemq.transport.stomp.StompTransportFilte
|     org.apache.activemq.transport.TransportSupport.doConsum
|     org.apache.activemq.transport.tcp.TcpTransport.doRun(Tc
|     org.apache.activemq.transport.tcp.TcpTransport.run(TcpT
|_    java.base/java.lang.Thread.run(Thread.java:840)
61614/tcp open  http       syn-ack ttl 64 Jetty 9.4.39.v20210
|_http-title: Site doesn't have a title.
|_http-server-header: Jetty(9.4.39.v20210325)
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998
| http-methods:
|   Supported Methods: GET HEAD TRACE OPTIONS
|_  Potentially risky methods: TRACE
61616/tcp open  apachemq   syn-ack ttl 64 ActiveMQ OpenWire t
```

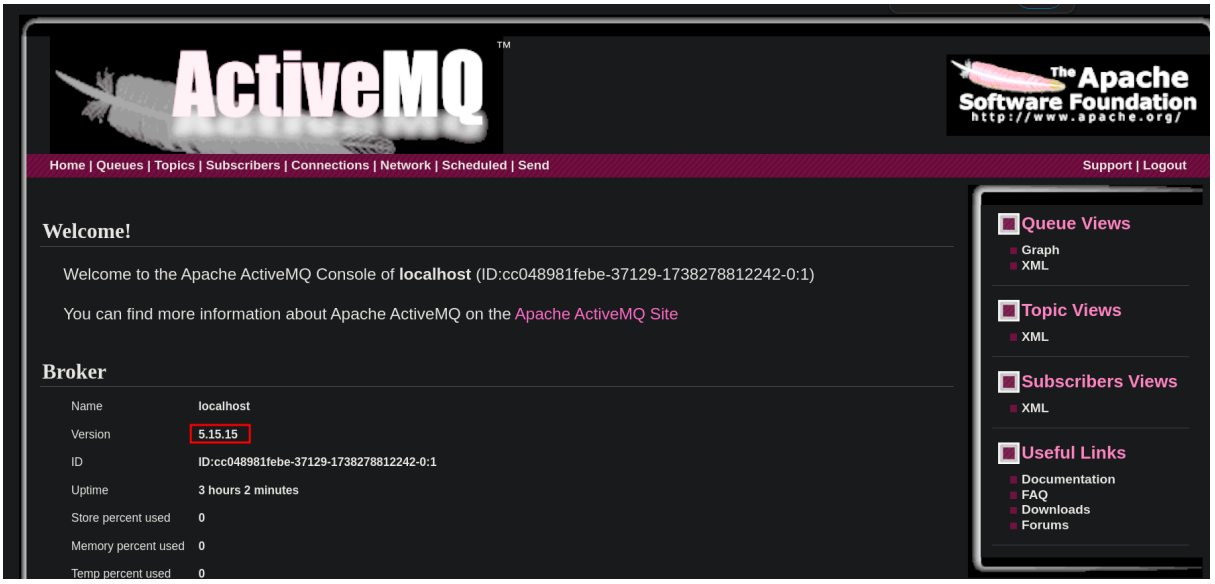
```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Title[Apache2
Debian Default Page: It works]

┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2:8161
http://172.17.0.2:8161 [401 Unauthorized] Country[RESERVED][ZZ], HTTPServer[Jetty(9.4.39.v20210325)], IP[172.17.0.2], Jetty[9.4.39.v20210325], Pow
eredBy[Jetty://], Title[Error 401 Unauthorized], WWW-Authenticate[ActiveMQRealm][basic]

┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2:61614
http://172.17.0.2:61614 [200 OK] Country[RESERVED][ZZ], HTTPServer[Jetty(9.4.39.v20210325)], IP[172.17.0.2], Jetty[9.4.39.v20210325]
```

port 443

Port 8161 con credenciales admin:admin







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

Ojo! avrir el poc-linux.xml y en la linea 11 pones la ip de atacante, el puerto que figura ahi es por el cual te vas a conectar por nc