ATTACK DEFENSE

by PentesterAcademy

Name	Access Control List
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.

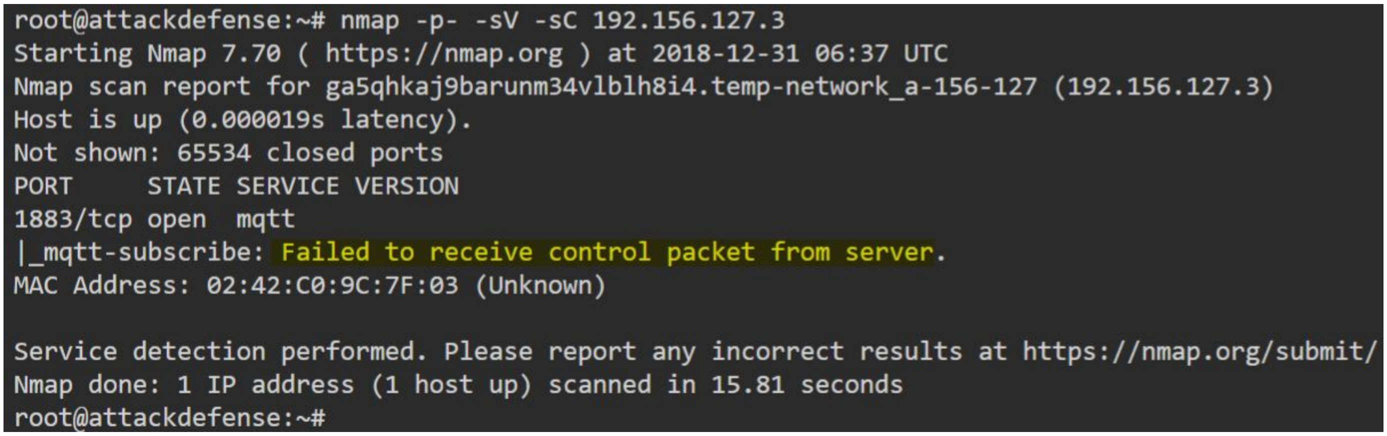
Q1. Has the target server deployed access controls?

Answer: Yes

Solution:

On running nmap enumeration script on the target server, server won't give any response.

Command: nmap -p- -sV -sC 192.156.127.3



```
root@attackdefense:~# nmap -p- -sV -sC 192.156.127.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-31 06:37 UTC
Nmap scan report for ga5qhkaj9barunm34vlblh8i4.temp-network_a-156-127 (192.156.127.3)
Host is up (0.000019s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE VERSION
1883/tcp open  mqtt
|_mqtt-subscribe: Failed to receive control packet from server.
MAC Address: 02:42:C0:9C:7F:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 15.81 seconds
root@attackdefense:~#
```

This means that server only entertains pre-defined users.

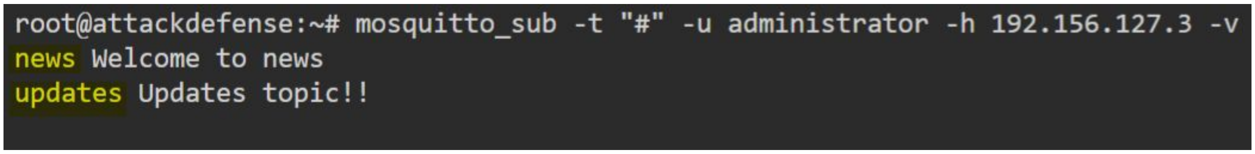
Q2. On how many topics, we can subscribe using user “administrator”?

Answer: 2

Solution:

Try to perform wildcard subscription using “administrator” user

Command: mosquitto_sub -t "#" -u administrator -h 192.156.127.3 -v



```
root@attackdefense:~# mosquitto_sub -t "#" -u administrator -h 192.156.127.3 -v
news Welcome to news
updates Updates topic!!
```

One can observe that the messages are from “news” and “updates” topics.

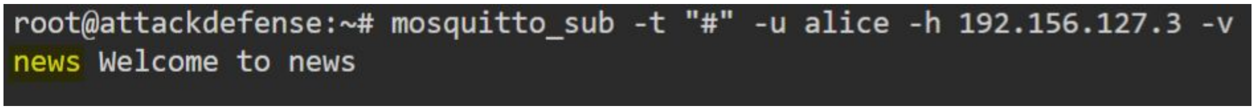
Q3. There is another user named "alice" on the system. For which topic, alice only has read permission?

Answer: news

Solution:

Perform wildcard subscription with alice user and check which topics alice is able to listen.

Command: mosquitto_sub -t "#" -u alice -h 192.156.127.3 -v



```
root@attackdefense:~# mosquitto_sub -t "#" -u alice -h 192.156.127.3 -v
news Welcome to news
```

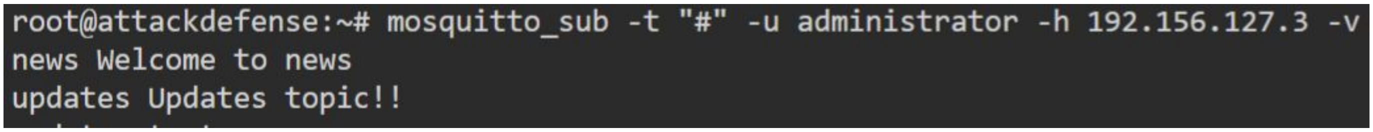
Q4. For which topic, alice only has write permissions?

Answer: updates

Solution:

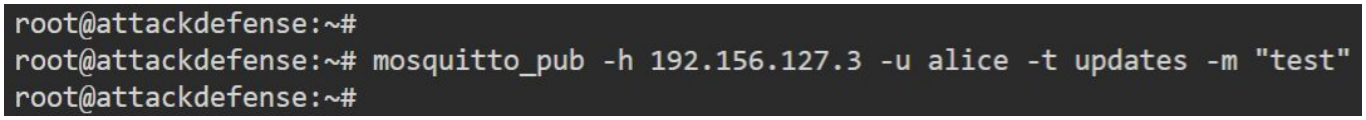
Perform wildcard subscription with administrator user and check if administrator can listen when user alice posts on any of the present two topics.

Command: mosquitto_sub -t "#" -u administrator -h 192.156.127.3 -v



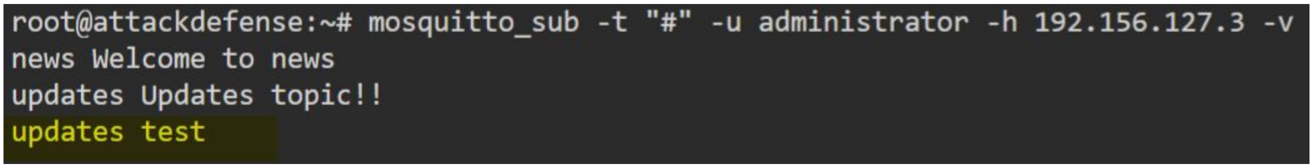
```
root@attackdefense:~# mosquitto_sub -t "#" -u administrator -h 192.156.127.3 -v
news Welcome to news
updates Updates topic!!
```

Command: mosquitto_pub -h 192.156.127.3 -u alice -t updates -m "test"



```
root@attackdefense:~#
root@attackdefense:~# mosquitto_pub -h 192.156.127.3 -u alice -t updates -m "test"
root@attackdefense:~#
```

If administrator can listen what alice is posting, it will be clear that alice has write privileges.



```
root@attackdefense:~# mosquitto_sub -t "#" -u administrator -h 192.156.127.3 -v
news Welcome to news
updates Updates topic!!
updates test
```