ATTACK DEFENSE

by PentesterAcademy

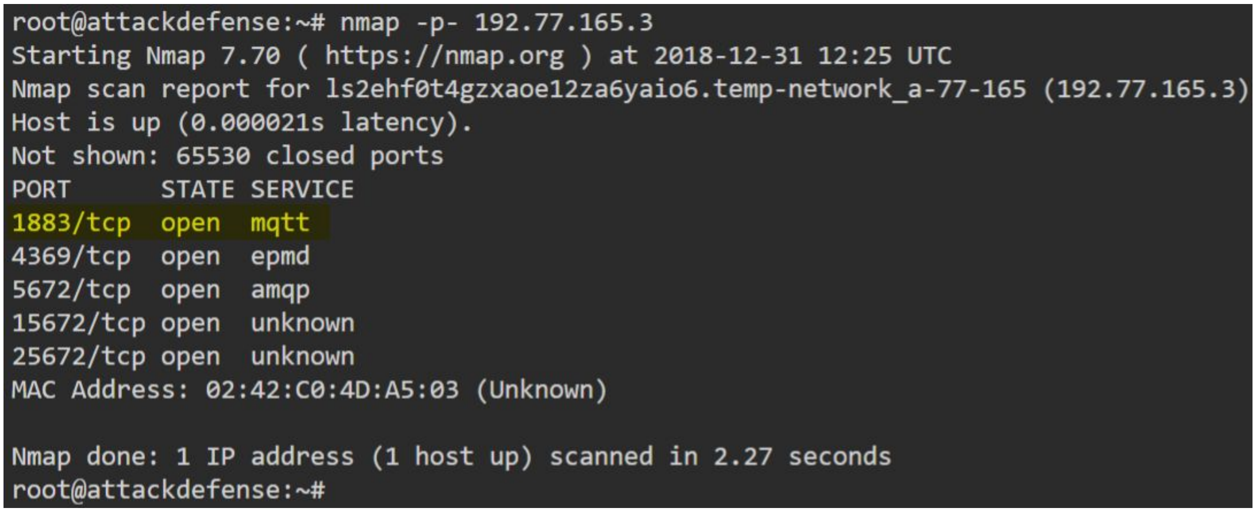
Name	RabbitMQ: MQTT Basics
URL	https://www.attackdefense.com/challengedetails?cid=574
Type	IoT : MQTT

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 MQTT over TLS is available on the target server?

Answer: No

Command: nmap -p- 192.78.197.3



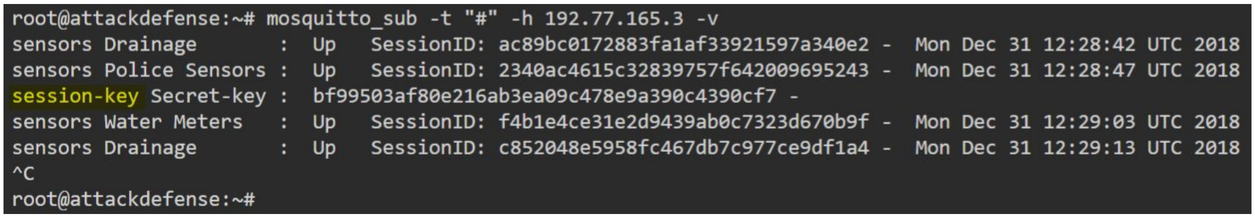
```
root@attackdefense:~# nmap -p- 192.77.165.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-31 12:25 UTC
Nmap scan report for ls2ehf0t4gzxaoe12za6yaio6.temp-network_a-77-165 (192.77.165.3)
Host is up (0.000021s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE
1883/tcp  open  mqtt
4369/tcp  open  epmd
5672/tcp  open  amqp
15672/tcp open  unknown
25672/tcp open  unknown
MAC Address: 02:42:C0:4D:A5:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds
root@attackdefense:~#
```

As Default ports 8883 (MQTT over TLS) is not operating. Hence, MQTT over TLS is not available

Q2. Which topic is being used to publish the session keys?

Answer: session-key

Command: mosquitto_sub -t "#" -h 192.78.197.3

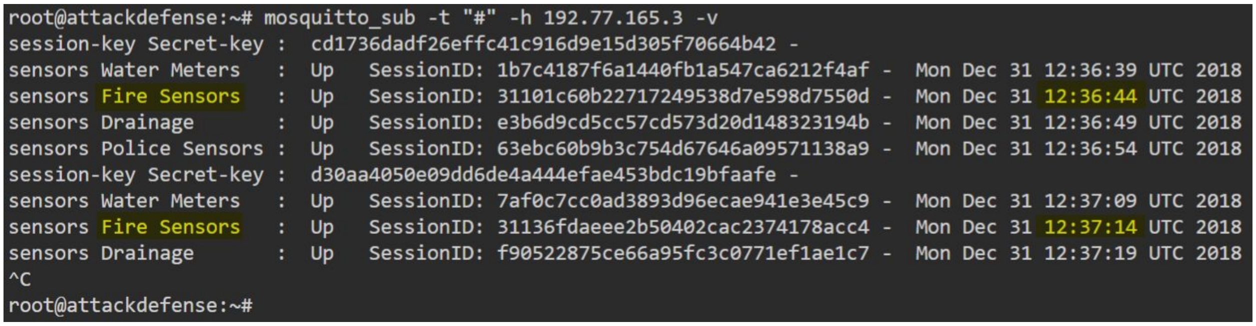


```
root@attackdefense:~# mosquitto_sub -t "#" -h 192.77.165.3 -v
sensors Drainage        :  Up   SessionID: ac89bc0172883fa1af33921597a340e2 -  Mon Dec 31 12:28:42 UTC 2018
sensors Police Sensors :  Up   SessionID: 2340ac4615c32839757f642009695243 -  Mon Dec 31 12:28:47 UTC 2018
session-key Secret-key :  bf99503af80e216ab3ea09c478e9a390c4390cf7 -
sensors Water Meters    :  Up   SessionID: f4b1e4ce31e2d9439ab0c7323d670b9f -  Mon Dec 31 12:29:03 UTC 2018
sensors Drainage        :  Up   SessionID: c852048e5958fc467db7c977ce9df1a4 -  Mon Dec 31 12:29:13 UTC 2018
^C
root@attackdefense:~#
```

Q3. What is the approx time period between two consecutive reports/messages of Fire Sensors?

Answer: 30 seconds

Command: mosquitto_sub -v -t "#" -h 192.78.197.3



```
root@attackdefense:~# mosquitto_sub -t "#" -h 192.77.165.3 -v
session-key Secret-key :  cd1736dadf26effc41c916d9e15d305f70664b42 -
sensors Water Meters    :  Up   SessionID: 1b7c4187f6a1440fb1a547ca6212f4af -  Mon Dec 31 12:36:39 UTC 2018
sensors Fire Sensors    :  Up   SessionID: 31101c60b22717249538d7e598d7550d -  Mon Dec 31 12:36:44 UTC 2018
sensors Drainage        :  Up   SessionID: e3b6d9cd5cc57cd573d20d148323194b -  Mon Dec 31 12:36:49 UTC 2018
sensors Police Sensors :  Up   SessionID: 63ebc60b9b3c754d67646a09571138a9 -  Mon Dec 31 12:36:54 UTC 2018
session-key Secret-key :  d30aa4050e09dd6de4a444efae453bdc19bfaafe -
sensors Water Meters    :  Up   SessionID: 7af0c7cc0ad3893d96ecae941e3e45c9 -  Mon Dec 31 12:37:09 UTC 2018
sensors Fire Sensors    :  Up   SessionID: 31136fdaeee2b50402cac2374178acc4 -  Mon Dec 31 12:37:14 UTC 2018
sensors Drainage        :  Up   SessionID: f90522875ce66a95fc3c0771ef1ae1c7 -  Mon Dec 31 12:37:19 UTC 2018
^C
root@attackdefense:~#
```

All the Fire Sensors updates have a timestamp. From that timestamp, calculate the time difference.