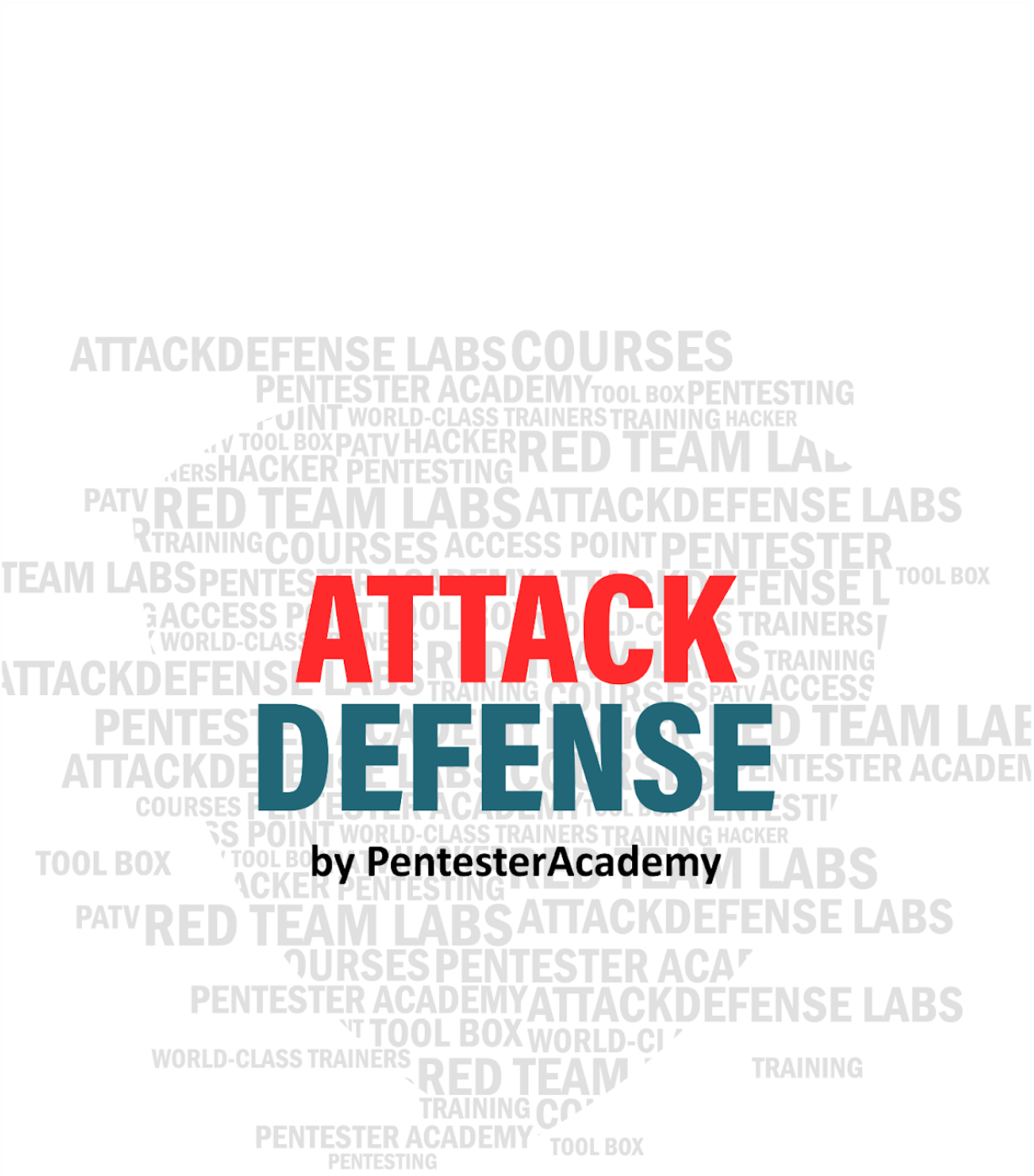
ATTACK
DEFENSE
by PentesterAcademy

Name	Broker Recon and Fingerprinting
URL	https://www.attackdefense.com/challengedetails?cid=566
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 running on the server? If yes, what is the port for MQTT over TLS?

Answer: Yes, 8883

Command: nmap -p- 192.78.197.3

```
root@attackdefense:~# nmap -p- 192.78.197.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-31 06:07 UTC
Nmap scan report for 4pww0laso6dky56i6l9w5s7qo.temp-network_a-78-197 (192.78.197.3)
Host is up (0.000020s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE
1883/tcp open  mqtt
8883/tcp open  secure-mqtt
MAC Address: 02:42:C0:4E:C5:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
root@attackdefense:~#
```

Default ports 1883 (MQTT) and 8883 (MQTT over TLS) are up. So, MQTT server is running.

Q2. What is the name and version of the MQTT server?

Answer: mosquitto version 1.4.15

Commands: nmap -p1883 -sV 192.78.197.3

```
root@attackdefense:~# nmap -p1883 -sV 192.78.197.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-31 06:08 UTC
Nmap scan report for 4pww0laso6dky56i6l9w5s7qo.temp-network_a-78-197 (192.78.197.3)
Host is up (0.000072s latency).

PORT     STATE SERVICE                 VERSION
1883/tcp open  mosquitto version 1.4.15
MAC Address: 02:42:C0:4E:C5:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 18.18 seconds
root@attackdefense:~#
```

Q3. What command can be used to enumerate the MQTT server using NMAP script?

Answer: nmap -p1883 -sV -sC 192.78.197.3

```
root@attackdefense:~# nmap -p1883 -sV -sC 192.78.197.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-31 06:09 UTC
Nmap scan report for 4pww0laso6dky56i6l9w5s7qo.temp-network_a-78-197 (192.78.197.3)
Host is up (0.000060s latency).

PORT     STATE SERVICE                 VERSION
1883/tcp open  mosquitto version 1.4.15
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     $SYS/broker/timestamp: Sat, 07 Apr 2018 11:16:43 +0100
|     $SYS/broker/load/bytes/sent/15min: 610.90
|     $SYS/broker/load/messages/sent/1min: 158.13
|     $SYS/broker/heap/current: 8414544
|     $SYS/broker/load/messages/received/1min: 36.68
|     $SYS/broker/heap/maximum: 8415536
|     $SYS/broker/load/bytes/received/1min: 1540.34
|     $SYS/broker/bytes/sent: 9546
|     $SYS/broker/clients/expired: 0
|     $SYS/broker/load/sockets/5min: 6.79
|     $SYS/broker/load/connections/15min: 2.83
|     $SYS/broker/retained messages/count: 49
|     $SYS/broker/messages/stored: 49
|     $SYS/broker/bytes/received: 6079
|     $SYS/broker/messages/received: 136
```

Q4. What is the welcome message set for topic “industrial”?

Answer: Critical Infrastructure Grid of Gotham City Software Version v9.10\nStatus: Running Security Alerts: 0

Command: mosquitto_sub -t industrial -h 192.78.197.3

```
root@attackdefense:~# mosquitto_sub -t industrial -h 192.78.197.3
Critical Infrastructure Grid of Gotham City Software Version v9.10\nStatus: Running   Security Alerts: 0

^C
root@attackdefense:~#
```

Q5. Which topic is being used by the sensors to publish their updates?

Answer: sensors

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

```
root@attackdefense:~# mosquitto_sub -t  "#" -h 192.78.197.3 -v
industrial Critical Infrastructure Grid of Gotham City Software Version v9.10\nStatus: Running   Security Alerts: 0
sensors Police Sensors :  Up   SessionID: a9d0766b11a8f9af4fbd9765ad93208a -  Mon Dec 31 06:13:47 UTC 2018
sessionkeys Secret-key :  cdc18b69ff870dd331d240a623e73b0fbc4e5583 -
sensors Water Meters   :  Up   SessionID: 82b7d9b6045b5126784b9f5dfadb1aaa -  Mon Dec 31 06:14:02 UTC 2018
sensors Fire Sensors   :  Up   SessionID: 982943c0cfa4e21ffd87d7deac40f229 -  Mon Dec 31 06:14:07 UTC 2018
sensors Drainage       :  Up   SessionID: 1302aa00e17731812a80bac99e0bd07e -  Mon Dec 31 06:14:12 UTC 2018
sensors Police Sensors :  Up   SessionID: e74d7eb8aa4005647484633b561dc455 -  Mon Dec 31 06:14:17 UTC 2018
sessionkeys Secret-key :  93db16d9a029113aa1803504ddb39371a49fb2a4 -
sensors Water Meters   :  Up   SessionID: 9e18b84403f931ec4241fc4780c13266 -  Mon Dec 31 06:14:32 UTC 2018
sensors Fire Sensors   :  Up   SessionID: f4afc52501b794688353f968ff71e1dc -  Mon Dec 31 06:14:37 UTC 2018

^C
root@attackdefense:~#
```

Q6. Session keys are being published on a topic periodically. What is the approx time period between the appearance of two consecutive session-keys?

Answer: 30 seconds

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

Option 1: Measure the time manually (use a stopwatch maybe)

Option 2: Observe that Water Meters is reporting almost at the same time as the Secret-key. The Water Meter updates have a timestamp. From that timestamp, difference can be calculated.

```
sessionkeys Secret-key :  a99978075dfcb83223f2a7a80d7a8055a5a4f800 -
sensors Water Meters   :  Up   SessionID: f8e0ef253c586fa83a7e772c5175392b -  Mon Dec 31 06:22:03 UTC 2018
sensors Fire Sensors   :  Up   SessionID: 5faf506ce20c185d9ea5bcf6729cb8b9 -  Mon Dec 31 06:22:09 UTC 2018
sensors Drainage       :  Up   SessionID: adfe708aa99edb3a933d7688d698182d -  Mon Dec 31 06:22:14 UTC 2018
sensors Police Sensors :  Up   SessionID: 143559f46c22fd96ba436daf324fd443 -  Mon Dec 31 06:22:19 UTC 2018
sessionkeys Secret-key :  20e5ed7cbf165339b886a1766a14891850cde76c -
sensors Water Meters   :  Up   SessionID: 7c81744a6a827bc017fe21657636c989 -  Mon Dec 31 06:22:34 UTC 2018
```

Q7. What is the command to post the content of file /etc/passwd to topic ”confidential”?

Answer: mosquitto_pub -t confidential -h 192.78.197.3 -f /etc/passwd

```
root@attackdefense:~#  mosquitto_sub -t  "#" -h 192.78.197.3 -v
industrial Critical Infrastructure Grid of Gotham City Software Version v9.10\nStatus: Running   Security Alerts: 0
sessionkeys Secret-key :  bc68e64a91b140e2aadb59726ef9c5ae1d6255ba -
sensors Water Meters   :  Up   SessionID: e20ec7bd4d873b0089b6dfc990b40ce4 -  Mon Dec 31 06:20:03 UTC 2018
confidential root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

This can be verified by subscribing for wildcard as shown above.