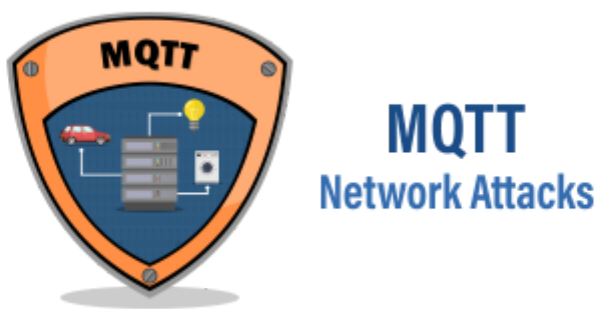

MQ Telemetry Transport (MQTT) is a lightweight protocol that is widely used by IoT devices to communicate with their brokers/servers situated on remote locations and clouds. The protocol is simple and consumes much less bandwidth and power than its peers, making it best for devices where network bandwidth and power are constrained. It is a two-way communication protocol. MQTT works in a subscribe-publish model. Brokers or servers play middleman for the publishers (producers e.g. sensors) and subscribers (consumers e.g. central monitoring system).

In this section, we will learn the basics of MQTT protocol, how to interact with MQTT brokers, perform enumeration and launch dictionary attacks, exploit known DoS vulnerabilities, and interact with a dummy ICS setup.

What will you learn?

- How to fingerprint and interact with an MQTT server
- Launch enumeration and dictionary attacks on MQTT servers
- Interact and manipulate MQTT messages to disrupt systems

References:

1. MQTT (https://mqtt.org/)
2. Mosquitto server (https://mosquitto.org/)
3. RabbitMQ (https://www.rabbitmq.com/)
4. Node-RED (https://nodered.org/)

Labs:

- Broker Recon and Fingerprinting
  Scan, fingerprint and interact with an open MQTT server/broker service provided by Mosquitto.

- Access Control List (ACL)
  Interact with an MQTT broker with a username-based ACL implemented on it. Also, figure out a user's permissions on various topics present on the servers.

- ACL and Authentication
  Interact with an MQTT broker protected with user credentials. Also, launch a dictionary attack on it to figure out the correct password for a valid username.

- Broker-Bridge Configuration
  Interact and launch dictionary attacks on two MQTT brokers that are configured in a broker-bridge configuration.

- Controller-Broker-Sensor Setup
  Analyze and interact with a dummy ICS (Industrial Control System) with multiple components (e.g. MQTT broker, sensor, monitoring dashboard). Then, launch a manipulation attack on the system to trigger false alarm/alert.

- Exploring Node-RED with MQTT
  Interact and configure a Node-RED system. A sample flow is provided along with a MQTT sensor (to act as input).

- CVE-2017-7651
  Exploit the RAM overflow vulnerability to crash an MQTT broker.

- CVE-2018-12543
  Exploit an assert overflow vulnerability to crash an MQTT broker.

Scan, fingerprint and interact with an open MQTT server/broker service running on RabbitMQ server.

- RabbitMQ: Controller-Broker-Sensor Setup
  Analyze and interact with a dummy ICS (Industrial Control System) with multiple components (e.g. RabbitMQ MQTT broker, sensor, monitoring dashboard). Then, launch a manipulation attack on the system to trigger false alarm/alert.

- RabbitMQ: MQTT Dictionary Attack
  Perform a dictionary attack on an MQTT server/broker service running on a RabbitMQ server.

Broker Recon and Fingerprinting

Start

Access Control List (ACL)

Start

ACL and Authentication

Start

Broker-Bridge Configuration

Start

Controller-Broker-Sensor Setup

Start

Exploring Node Red with MQTT

Start

CVE-2017-7651

Start

CVE-2018-12543

Start

RabbitMQ: MQTT Basics

Start