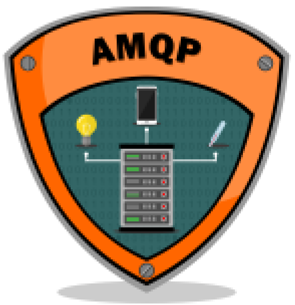
‹ Dashboard



AMQP
Network Attacks

Advanced Message Queuing Protocol (AMQP) is a standard protocol for passing messages between applications. It is mostly used in business related applications and provides buffer capacity for incoming/outgoing messages. However, with IoT devices entering the enterprise space, the AMQP implementations like RabbitMQ are being used to send/receive/buffer the messages.

In this section, we will learn the basics of AMQP protocol, interact with AMQP servers, perform enumeration and launch dictionary attacks, and interact with dummy ICS setup.

What will you learn?

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

References:

1. AMQP (https://www.amqp.org/about/what)
2. RabbitMQ (https://www.rabbitmq.com/)
3. Node-RED (https://nodered.org/)

Labs:

- Basic Recon and Interaction
  Scan, fingerprint and interact with an AMQP service running on RabbitMQ.

- Interacting with RabbitMQ UI
  Interact with the RabbiMQ web interface to enumerate queues/topics, create new topics/queues and send/receive messages.

- Authentication
  Interact with an AMQP service protected with user credentials. Launch a dictionary attack on it to figure out the correct password for a valid username.

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

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

Basic Recon and Interaction

Start

Interacting with RabbitMQ UI

Start