Project Assignment

Cybersecurity Professional Program

IoT and Mobility Security

IoT Final Project

IOT-11-L1

Find the Flag in Firmware

Project Objective

This project involves running various tools against a firmware image to find the flag in the MQTT server.

Project Mission

In this challenge, you will encounter binary firmware, which you will investigate to extract the URL and username. The URL will help you to reach a web-based portal with a reference to *MQTT broker*. The username will allow you to connect to the MQTT broker to explore the sensors until you find the flag.

Requirements

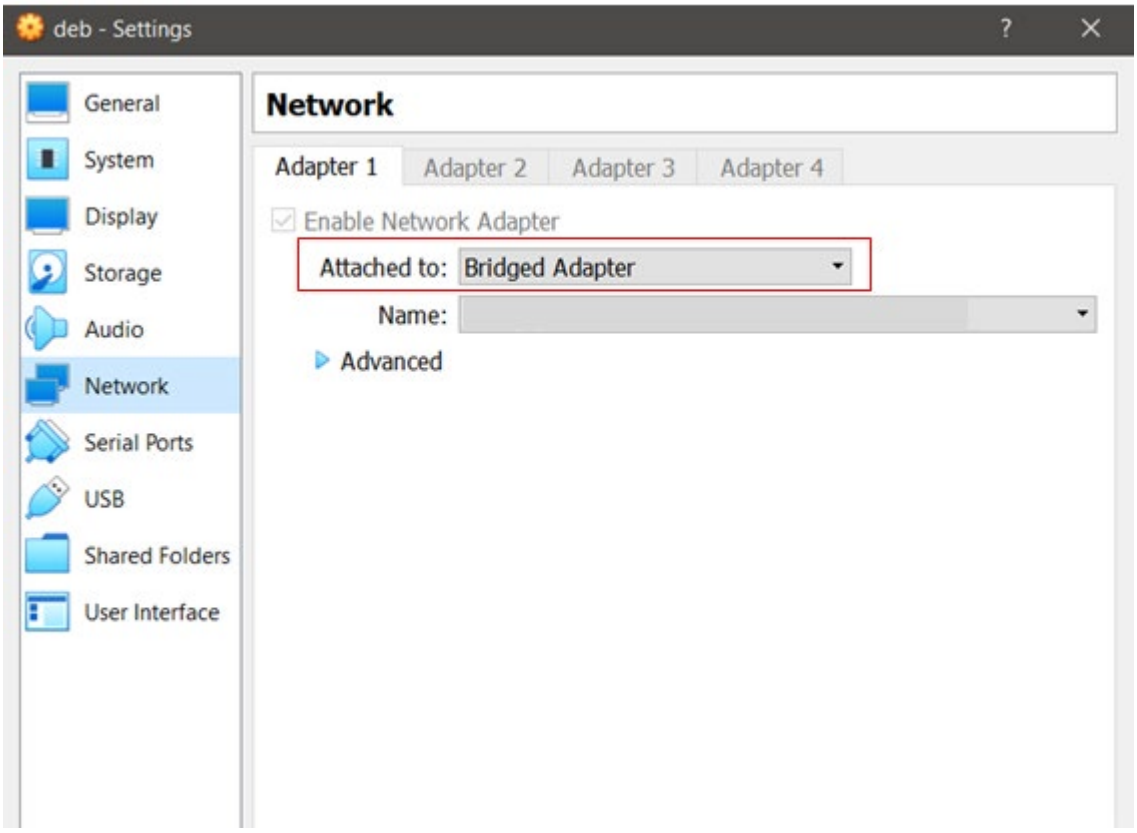
- Basic knowledge of MQTT
- Knowledge of the ***Strings*** tool

Resources

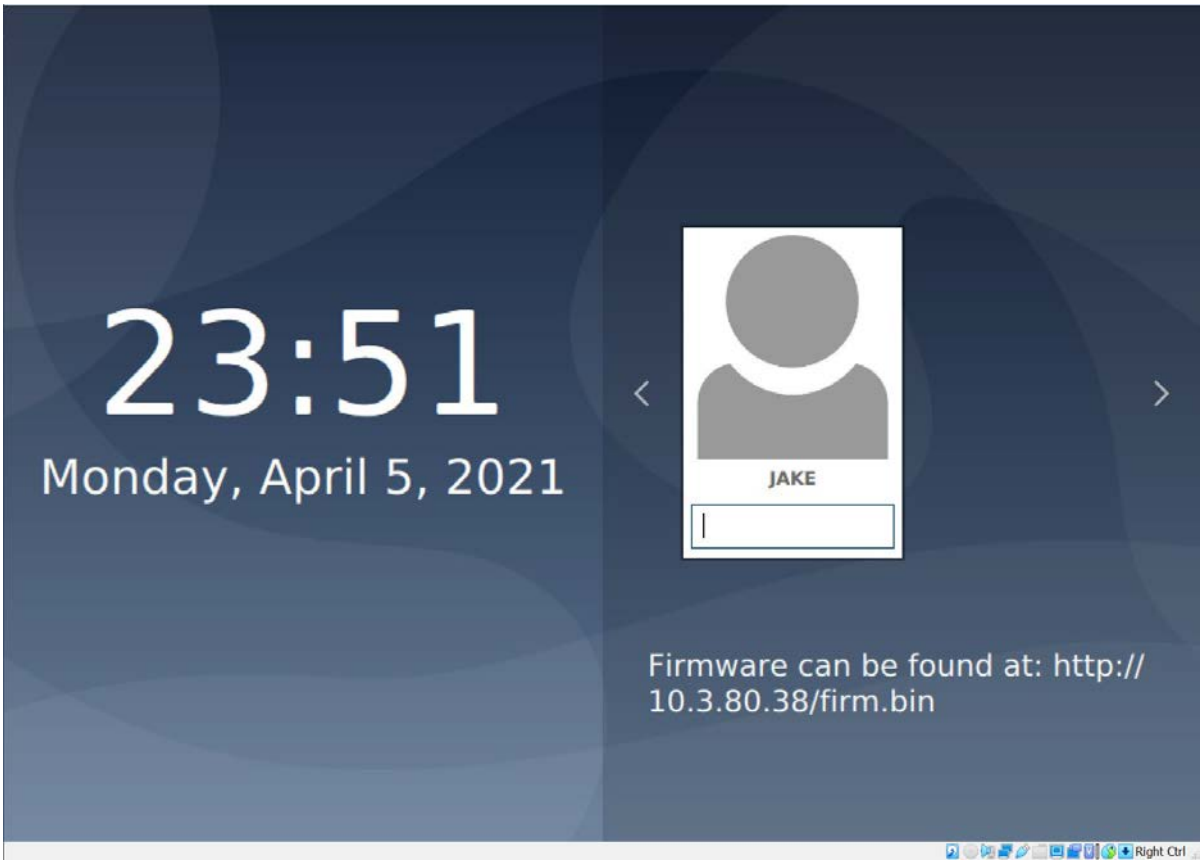
- Environment & Tools
  - MQTT Explorer
  - Strings
- Extra Lab Files
  - ***IoT_Final.ova***

Project Preparation: Importing OVA

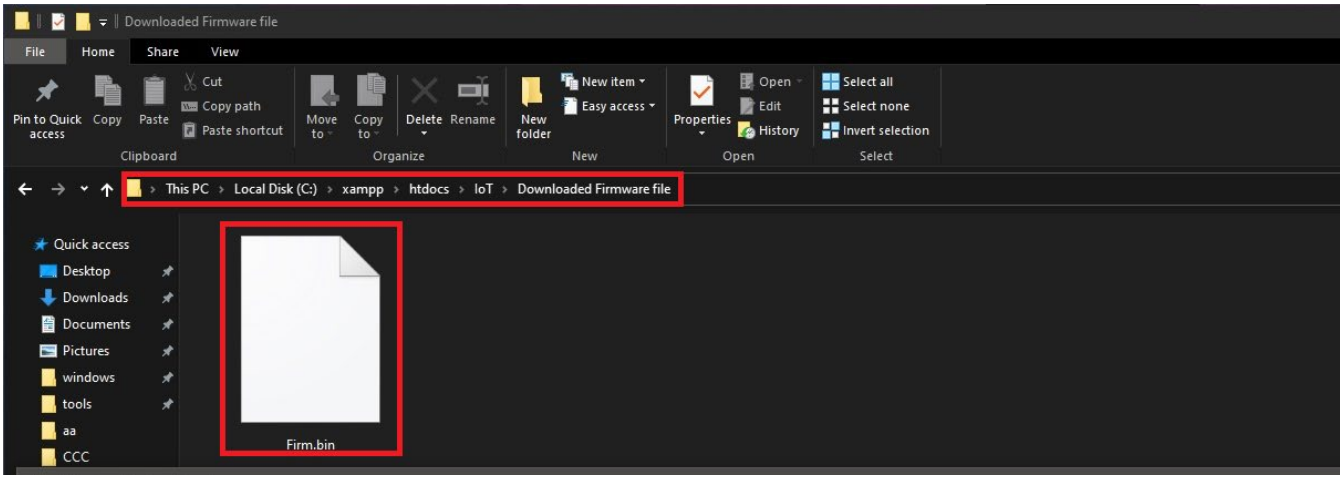
1. Download the ***IoT_Final.ova*** from Canvas. Double-click the file to import the virtual machine into VirtualBox.
2. Right-click the virtual machine in the VirtualBox interface and click **Settings**.



3 Start the virtual machine. When it is fully started, you will be prompted to reboot. Reboot the system, and continue to do so until the firmware address appears as shown below:



4 Confirm that you can locate the ***firm.bin*** file.



Project Tasks

You will perform the following tasks:

1. Access the firmware and locate ***Strings*** (within the firmware) to allow access to the MQTT server. **Hint:** If your firmware shows a loopback IP, use the IP that was designated when you downloaded the firmware.
2. Access the MQTT server with MQTT Explorer.
3. Set up a new MQTT client connected to the server.
4. Analyze the MQTT traffic from the server.
5. Modify the flags to get development debugging information. Make sure your modifications are in all caps (ON vs. on).
6. The flag will tell you that the final project is completed.