Presentation

Presentation of Tibor Molnar

Project name: hmnx

Computer Systems & Networks module

Physical work

I have assembled a raspberry pi with a sense hat attached to the top of the device. Installed micro sd card.
I have cable connected my pc so I'm using multiple way of connections types to the main router.

Prerequisite for main scripts and requests

pip3 install nmap
pip3 install paho-mqtt
sudo apt install net-tools

Project walthrough

The project is done on my own private network where I have few IoT devices and number of other devices connected to the gateway router over wifi but one device over cat5 patch cable.

The main goal of the project is to discover how many devices are being used or in other worlds how many devices/IoT devices are on my network. If I would know for example that a particular phone is connected to the network then that person is home.

I have located my raspberry pi on network by searching it's ip (ping it), but before I had run a simple arp request. arp -a and recognized the device from its MAC address using https://macvendors.com/
Using the ip address of the device I was able to "ssh" to the device.

I'm using Nmap to locate all the devices, their IP address, MAC address and return the vendor also from the first three bytes of MAC addresses.
I'm interacting layer2 technologies here by using MAC address in Networking.

In order to be able to communicate outside my network I have created a virtual machine using Openstack and assigned a public ip of 87.44.17.139 to it. I have created this vm for demonstration purposes, it could have been a phone also.

I'm saving all the mac addresses in a separate file called output.txt and compare them against
https://macvendors.com/api
or
https://standards.ieee.org/products-programs/regauth/

Using IP addresses and TCP/IP, ICMP allowed me to interact with layer 3 technologies in Networking.

Scripts

The first python script I have created is on the raspberry pi with the sense hat. The script reads a number out of a file and displays it on sense hat.

The second python script is also on the raspberry pi and it is a publisher for MQTT. I'm sending nmap results in json format using broker.emqx.io over a reserved TCP port 1883(formerly MQ Telemetry Transport).This script also creates 2 files. The first file holds the number of devices discovered on public network. The second file stores raw data about mac addresses.

The third python script is a subscriber script for MQTT which is sitting on the external VM I have created with IP address 87.44.17.139. open TCP ports 22 and 1883.

The fourth script is sitting on the external VM also and it is looking after the json data that has arrived on subscriber. The script put json data to SQLITE database.

While I was dealing with the different file formats like json, py I was using layer 6 technologies.

I belive I could give plenty of examples for using layer 7 technologies but the obvious ones in this project is ssh, github.

How to run the project

1. First script should be executed is the pub.py script on the raspberry pi which would querry the data from nmap and publish it,
2. The second script should be executed is piread.py which reads a value and shows on senshe hat.
3. Third Script could be executed from any choosen device that can run the subscription script. (sub.py) this script pulls the database script if needed (pushDataToDB.py), otherwise some code must be commented out in sub.py to be able to run it without error.

References

https://iotbytes.wordpress.com/store-mqtt-data-from-sensors-into-sql-database/ - accessed on 2022-12-12
https://sqlite.org/forum/info/0e4a6066495b160c - accessed on 2022-12-5