SSA IoT Systems Demo

Group 1
Shota Kameyama
Ying Chan
Austin Mundy
Mathew van Beek

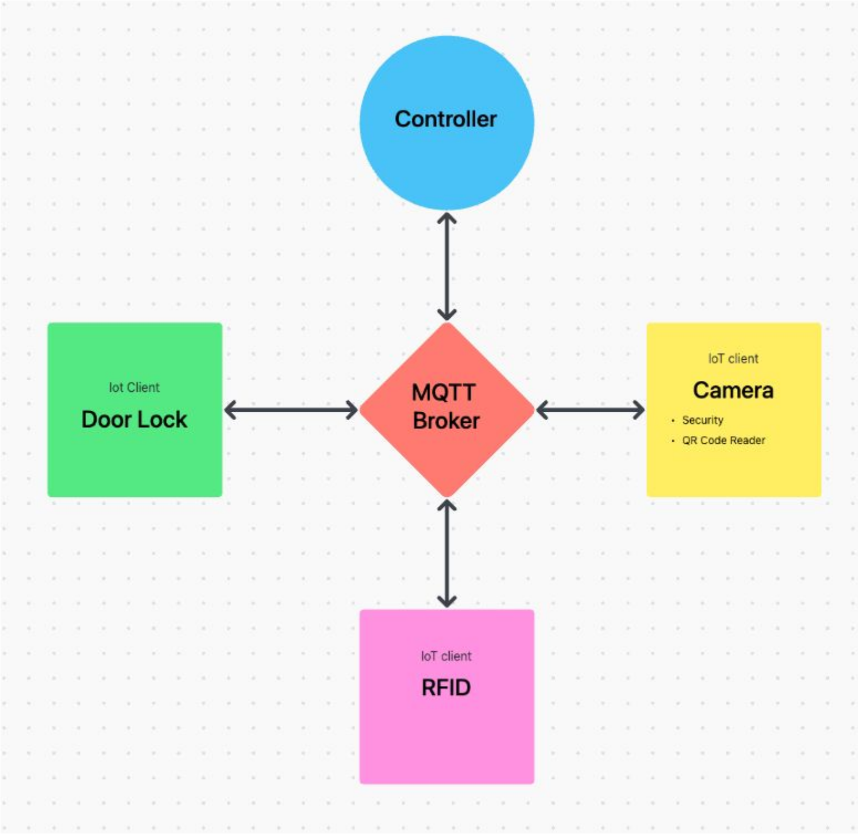
Use Case

- User show QR code or RFID to Open the door to get into the room
    - ex. hotel reservation, AirBnB

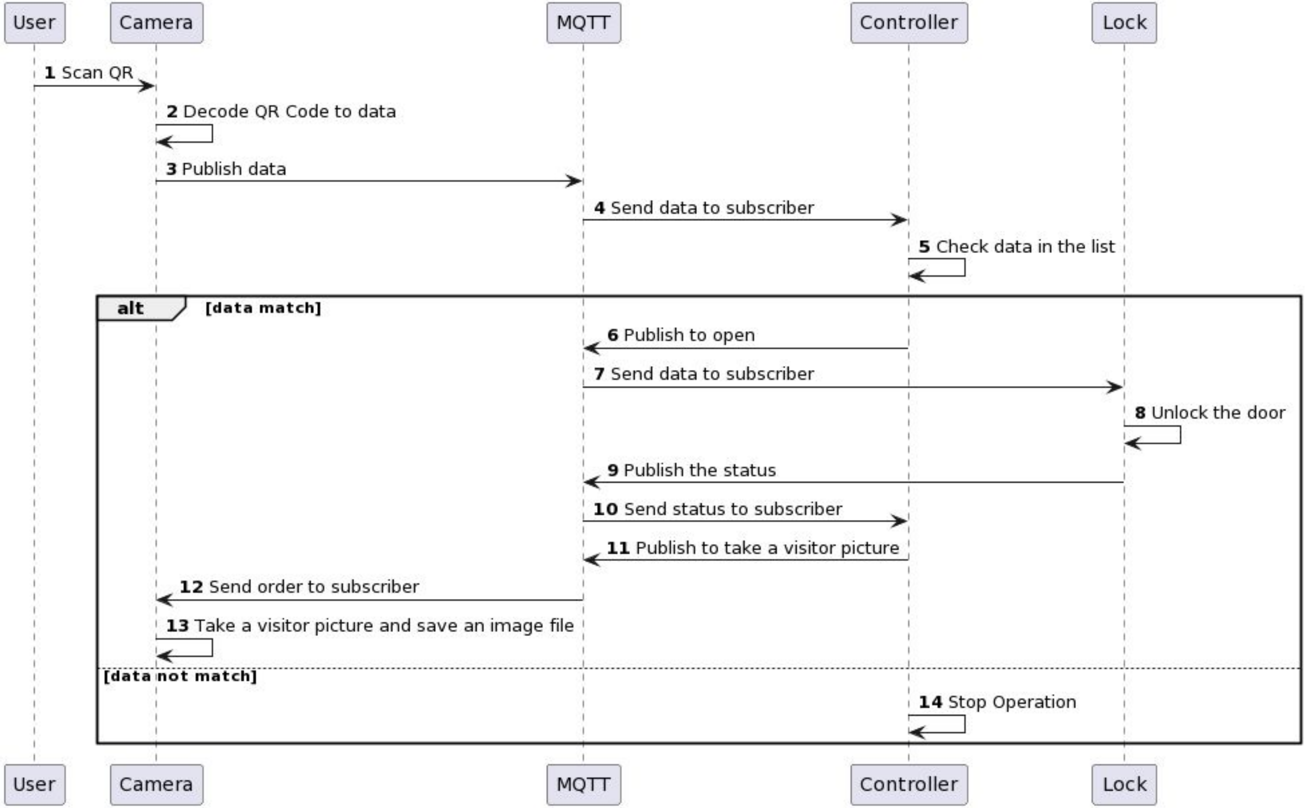
Systems Diagram

Each device communicate with MQTT protocol over TLS.

1. **Controller:** owns logics to order actions to each clients.
2. **Door Lock:** lock/unlock door
3. **Camera:** scan QR code, take visitors' picture
4. **RFID:** QR code scan alternative



Sequence Diagram



Technologies Used

Language

- Python3

MQTT Broker

- Mosquitto

Code Management

- Github

OS

- MacOS
- Windows
- Linux
- Debian (Raspberry Pi)

Libraries:

Python MQTT Connector

- paho-mqtt

Utilities (setup env variables)

- pyaml-env

Performance Testing

- locust
- locust-plugins

Guide Enforcement

- pylint
- flake8

Camera Capture & Decode QR

- opencv-python
- pyzbar

RFID

- spidev
- mfrc522

Test Approaches

Attack Against MQTT

- MQTT pwn

Performance Testing

- Locust

MQTT vulnerability Testing

- Nessus
- IoTSeeker

Traffic Spoofing

- Wireshark

Code Testing

- Snky

Dynamic Application Security Testing (DAST)

- Bandit

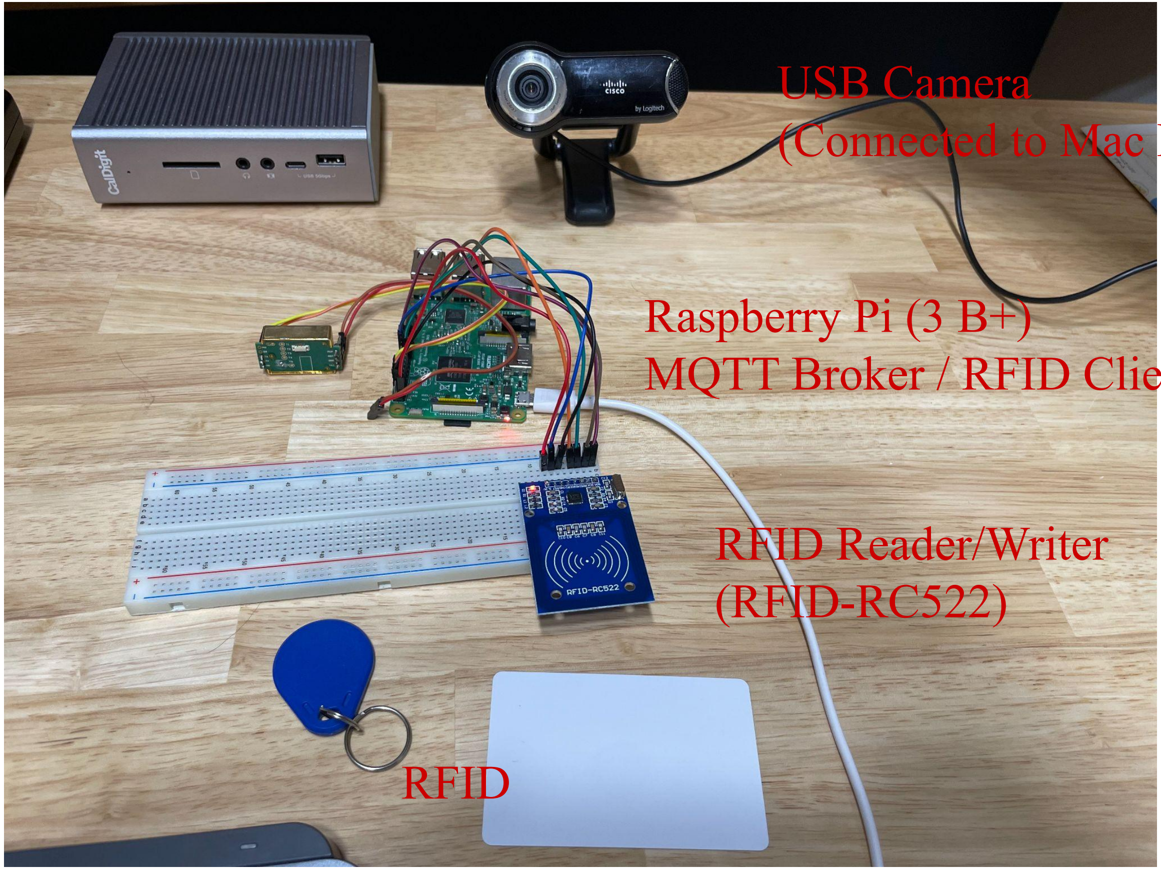
Latency Testing

- Ping
- Traceroute
- Nmap

Demo

Use Case Demo (Shota)

Controller
Camera Client
Door Lock Client



USB Camera
(Connected to Mac Mini)

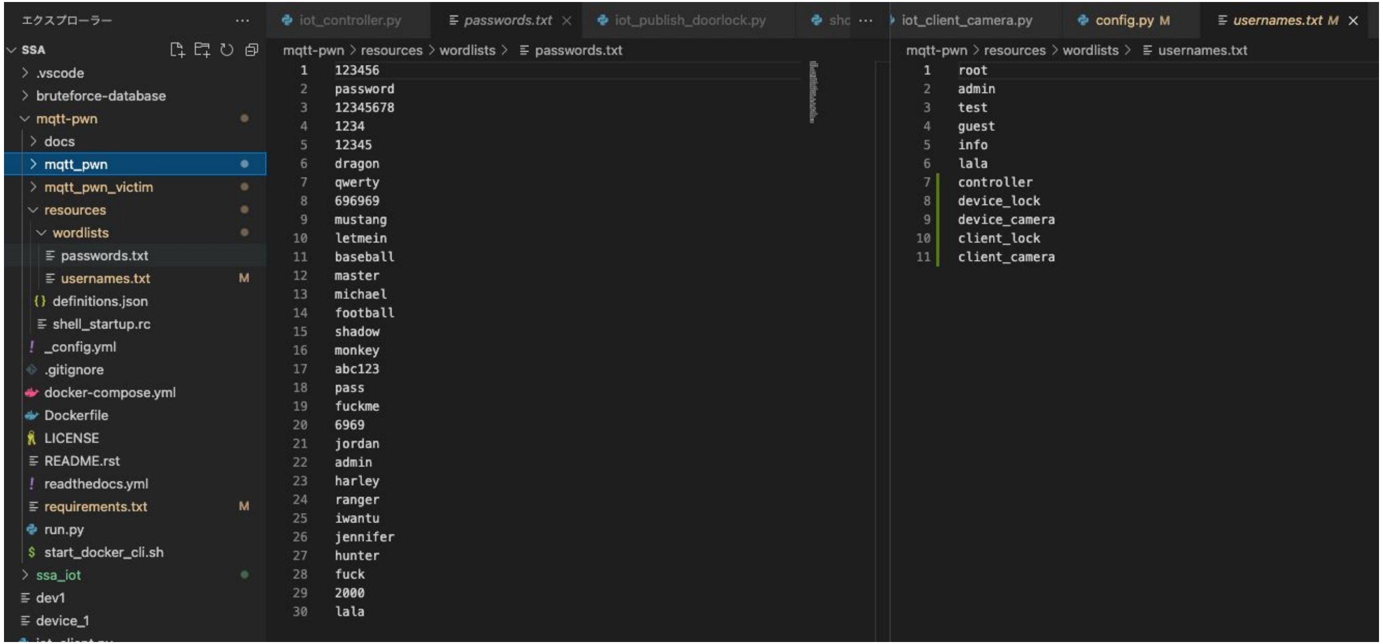
Raspberry Pi (3 B+)
MQTT Broker / RFID Client

RFID Reader/Writer
(RFID-RC522)

RFID

Dictionary Attack with MQTT pwn (Shota)

1. python3 run.py
2. bruteforce
   a. Dictionary Attack



mqtt-pwn > resources > wordlists > passwords.txt

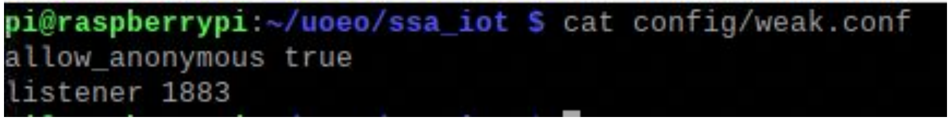
```
123456
password
12345678
1234
12345
dragon
qwerty
696969
mustang
letmein
baseball
master
michael
football
shadow
monkey
abc123
pass
fuckme
6969
jordan
admin
harley
ranger
iwantu
jennifer
hunter
fuck
2000
lala
```

mqtt-pwn > resources > wordlists > usernames.txt

```
root
admin
test
guest
info
lala
controller
device_lock
device_camera
client_lock
client_camera
```

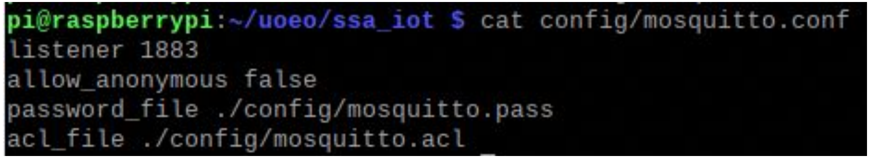
Finding Topics and Messages with MQTT pwn (Shota)

1. mosquitto -c conf/weak.conf
2. python3 run.py
3. connect
4. system_info
5. discovery
6. scans
7. scans -i 5
8. topics
9. messages



```
pi@raspberrypi:~/uoeo/ssa_iot $ cat config/weak.conf
allow_anonymous true
listener 1883
```

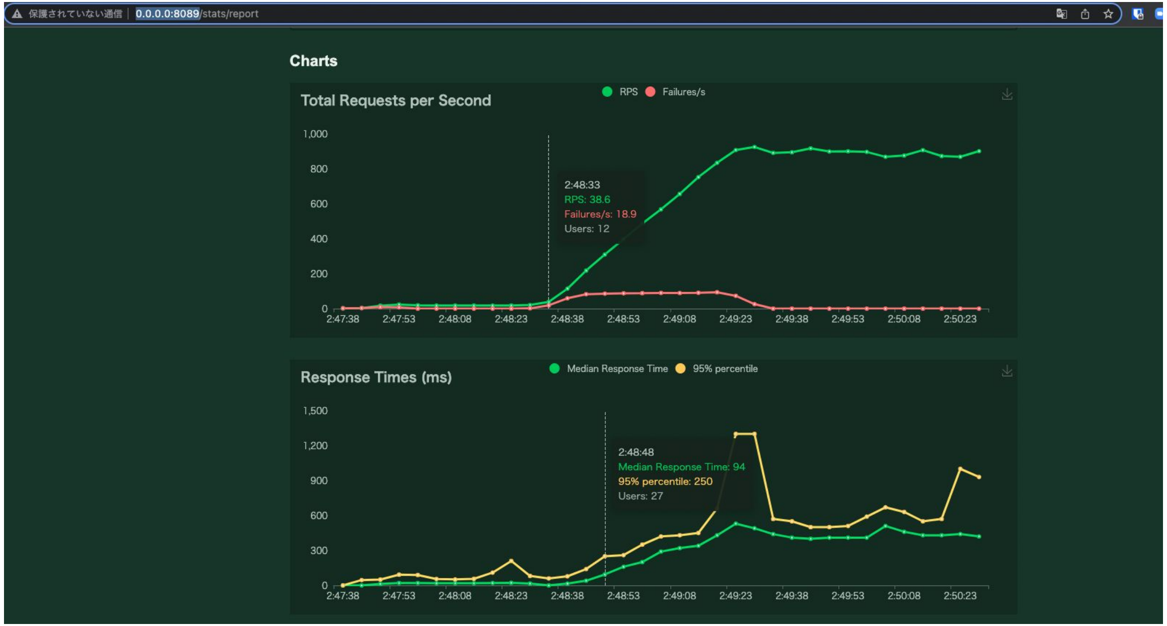
1. mosquitto -c conf/mosquitto.conf
2. python3 run.py
3. connect
4. system_info
5. discovery
6. scans
7. scans -i 5
8. topics
9. messages



```
pi@raspberrypi:~/uoeo/ssa_iot $ cat config/mosquitto.conf
listener 1883
allow_anonymous false
password_file ./config/mosquitto.pass
acl_file ./config/mosquitto.acl
```

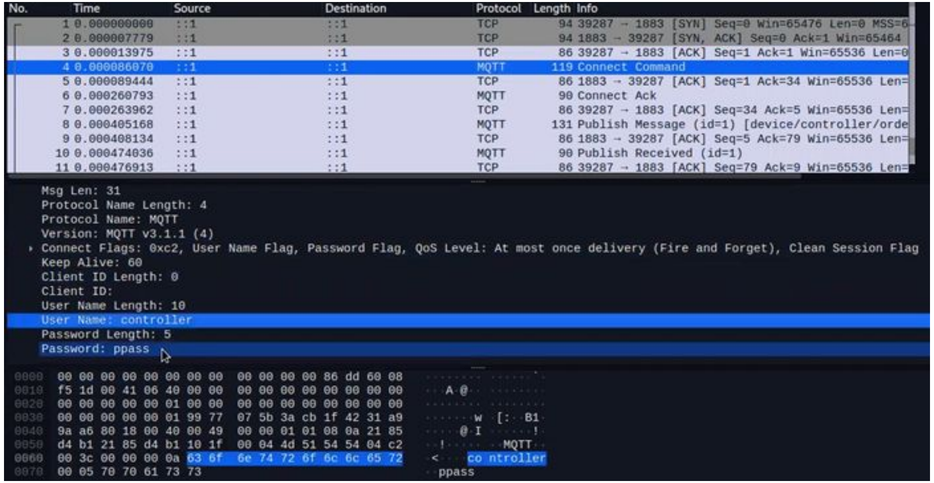
Performance Test with Locust (Shota)

1. locust
2. http://0.0.0.0:8089/



Spoofing Traffic & Encryption (Ying)

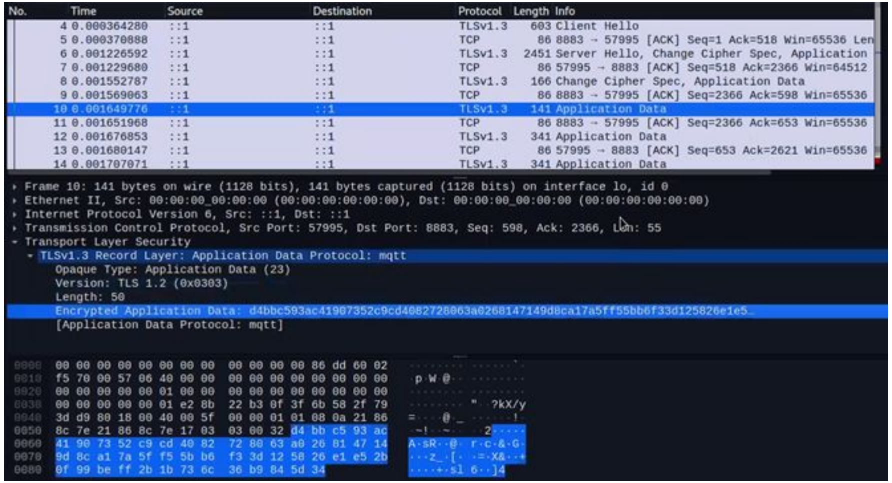
1. Capture network package without TLS
2. Capture network package with TLS



```
No.  Time         Source  Destination  Protocol  Length Info
   1 0.000000000  ::1     ::1          TCP       94 39287 → 1883 [SYN] Seq=0 Win=65476 Len=0 MSS=6
   2 0.000007779  ::1     ::1          TCP       94 1883 → 39287 [SYN, ACK] Seq=0 Ack=1 Win=65464
   3 0.000013975  ::1     ::1          TCP       86 39287 → 1883 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   4 0.000086070  ::1     ::1          MQTT     119 Connect Command
   5 0.000089444  ::1     ::1          TCP       86 1883 → 39287 [ACK] Seq=1 Ack=34 Win=65536 Len=
   6 0.000260793  ::1     ::1          MQTT      90 Connect Ack
   7 0.000263962  ::1     ::1          TCP       86 39287 → 1883 [ACK] Seq=34 Ack=5 Win=65536 Len=
   8 0.000405168  ::1     ::1          MQTT     131 Publish Message (id=1) [device/controller/orde
   9 0.000408134  ::1     ::1          TCP       86 1883 → 39287 [ACK] Seq=5 Ack=79 Win=65536 Len=
  10 0.000474036  ::1     ::1          MQTT      90 Publish Received (id=1)
  11 0.000476913  ::1     ::1          TCP       86 39287 → 1883 [ACK] Seq=79 Ack=9 Win=65536 Len=
```

```
    Msg Len: 31
    Protocol Name Length: 4
    Protocol Name: MQTT
    Version: MQTT v3.1.1 (4)
  › Connect Flags: 0xc2, User Name Flag, Password Flag, QoS Level: At most once delivery (Fire and Forget), Clean Session Flag
    Keep Alive: 60
    Client ID Length: 0
    Client ID:
    User Name Length: 10
    User Name: controller
    Password Length: 5
    Password: ppass
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 08   ········ ······`·
0010  f5 1d 00 41 06 40 00 00  00 00 00 00 00 00 00 00   ···A·@·· ········
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 99 77  07 5b 3a cb 1f 42 31 a9   ·······w ·[:··B1·
0040  9a a6 80 18 00 40 00 49  00 00 01 01 08 0a 21 85   ·····@·I ······!·
0050  d4 b1 21 85 d4 b1 10 1f  00 04 4d 51 54 54 04 c2   ··!····· ··MQTT··
0060  00 3c 00 00 00 0a 63 6f  6e 74 72 6f 6c 6c 65 72   ·<····co ntroller
0070  00 05 70 70 61 73 73                               ··ppass
```



```
No.  Time         Source  Destination  Protocol  Length Info
   4 0.000364280  ::1     ::1          TLSv1.3   603 Client Hello
   5 0.000370888  ::1     ::1          TCP        86 8883 → 57995 [ACK] Seq=1 Ack=518 Win=65536 Len
   6 0.001226592  ::1     ::1          TLSv1.3  2451 Server Hello, Change Cipher Spec, Application
   7 0.001229680  ::1     ::1          TCP        86 57995 → 8883 [ACK] Seq=518 Ack=2366 Win=64512
   8 0.001552787  ::1     ::1          TLSv1.3   166 Change Cipher Spec, Application Data
   9 0.001569063  ::1     ::1          TCP        86 8883 → 57995 [ACK] Seq=2366 Ack=598 Win=65536
  10 0.001649776  ::1     ::1          TLSv1.3   141 Application Data
  11 0.001651968  ::1     ::1          TCP        86 8883 → 57995 [ACK] Seq=2366 Ack=653 Win=65536
  12 0.001676853  ::1     ::1          TLSv1.3   341 Application Data
  13 0.001680147  ::1     ::1          TCP        86 57995 → 8883 [ACK] Seq=653 Ack=2621 Win=65536
  14 0.001707071  ::1     ::1          TLSv1.3   341 Application Data
```

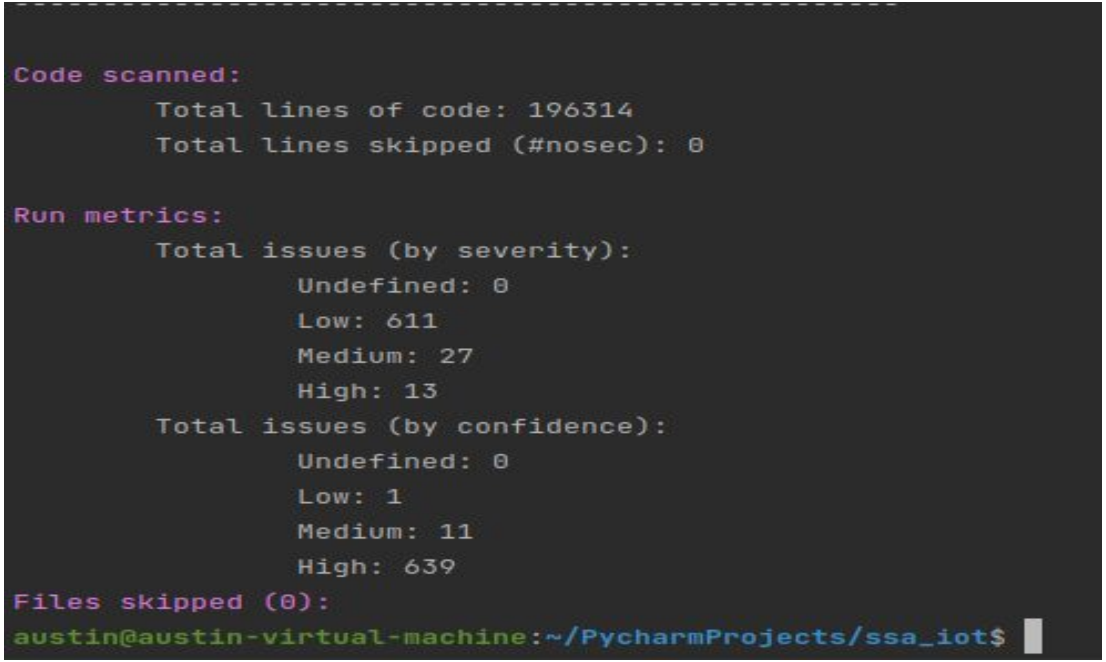
```
› Frame 10: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface lo, id 0
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
› Internet Protocol Version 6, Src: ::1, Dst: ::1
› Transmission Control Protocol, Src Port: 57995, Dst Port: 8883, Seq: 598, Ack: 2366, Len: 55
⌄ Transport Layer Security
  ⌄ TLSv1.3 Record Layer: Application Data Protocol: mqtt
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 50
      Encrypted Application Data: d4bbc593ac41907352c9cd4082728063a0268147149d8ca17a5ff55bb6f33d125826e1e5…
      [Application Data Protocol: mqtt]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 02   ········ ······`·
0010  f5 70 00 57 06 40 00 00  00 00 00 00 00 00 00 00   ·p·W·@·· ········
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 e2 8b  22 b3 0f 3f 6b 58 2f 79   ········ "··?kX/y
0040  3d d9 80 18 00 40 00 5f  00 00 01 01 08 0a 21 86   =····@·_ ······!·
0050  8c 7e 21 86 8c 7e 17 03  03 00 32 d4 bb c5 93 ac   ·~!··~·· ··2·····
0060  41 90 73 52 c9 cd 40 82  72 80 63 a0 26 81 47 14   A·sR··@· r·c·&·G·
0070  9d 8c a1 7a 5f f5 5b b6  f3 3d 12 58 26 e1 e5 2b   ···z_·[· ·=·X&··+
0080  0f 99 be ff 2b 1b 73 6c  36 b9 84 5d 34            ····+·sl 6··]4
```

Bandit Demo and Report (Austin)

Bandit Scan

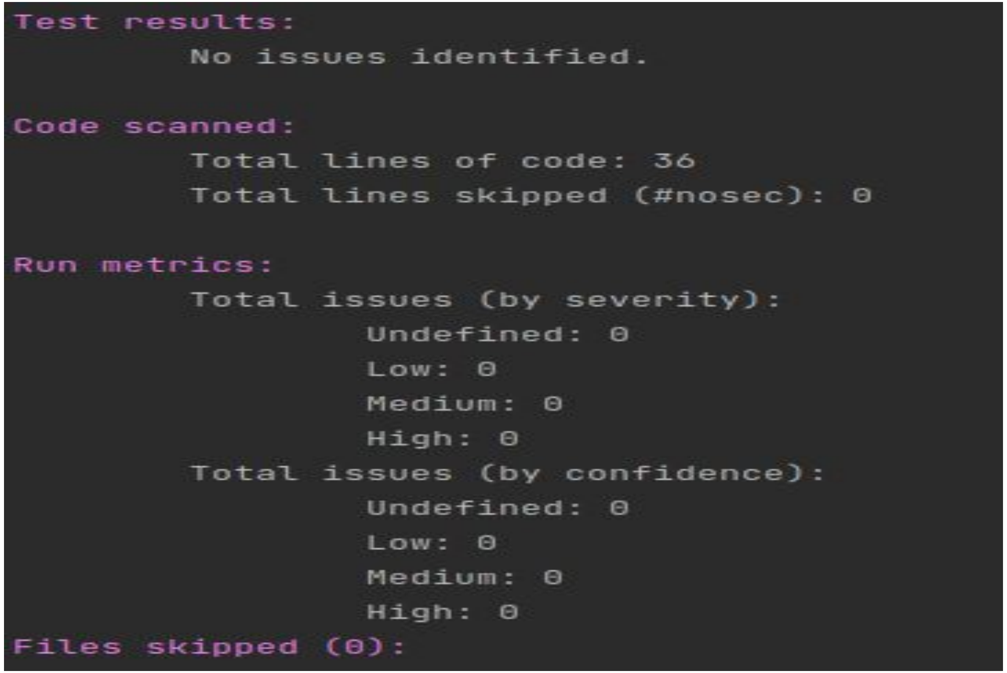
1. The initial band scan resulted in a significant amount of issues. However, these issues were all from external libraries.



```
--------------------------------------------------

Code scanned:
        Total lines of code: 196314
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 611
                Medium: 27
                High: 13
        Total issues (by confidence):
                Undefined: 0
                Low: 1
                Medium: 11
                High: 639
Files skipped (0):
austin@austin-virtual-machine:~/PycharmProjects/ssa_iot$
```

Bandit Scan Cont

1. Individually scanning the clients and controller results in no issues found.

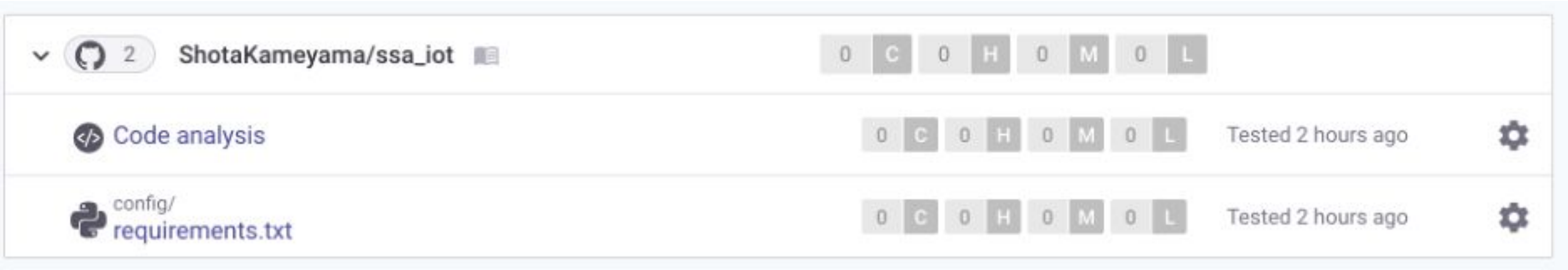


```
Test results:
        No issues identified.

Code scanned:
        Total lines of code: 36
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 0
                Medium: 0
                High: 0
        Total issues (by confidence):
                Undefined: 0
                Low: 0
                Medium: 0
                High: 0
Files skipped (0):
```

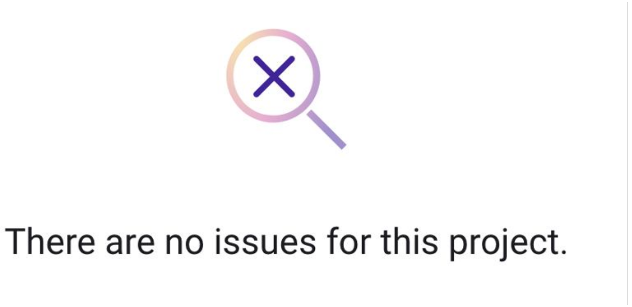
Code Testing
(Mathew)

Synk Scan

Snyk’s helps you find and fix known vulnerabilities in your dependencies, by integrating into GitHub. Results showed no known issues within the code.



2 ShotaKameyama/ssa_iot	0	C	0	H	0	M	0	L		
Code analysis	0	C	0	H	0	M	0	L	Tested 2 hours ago	
config/ requirements.txt	0	C	0	H	0	M	0	L	Tested 2 hours ago	



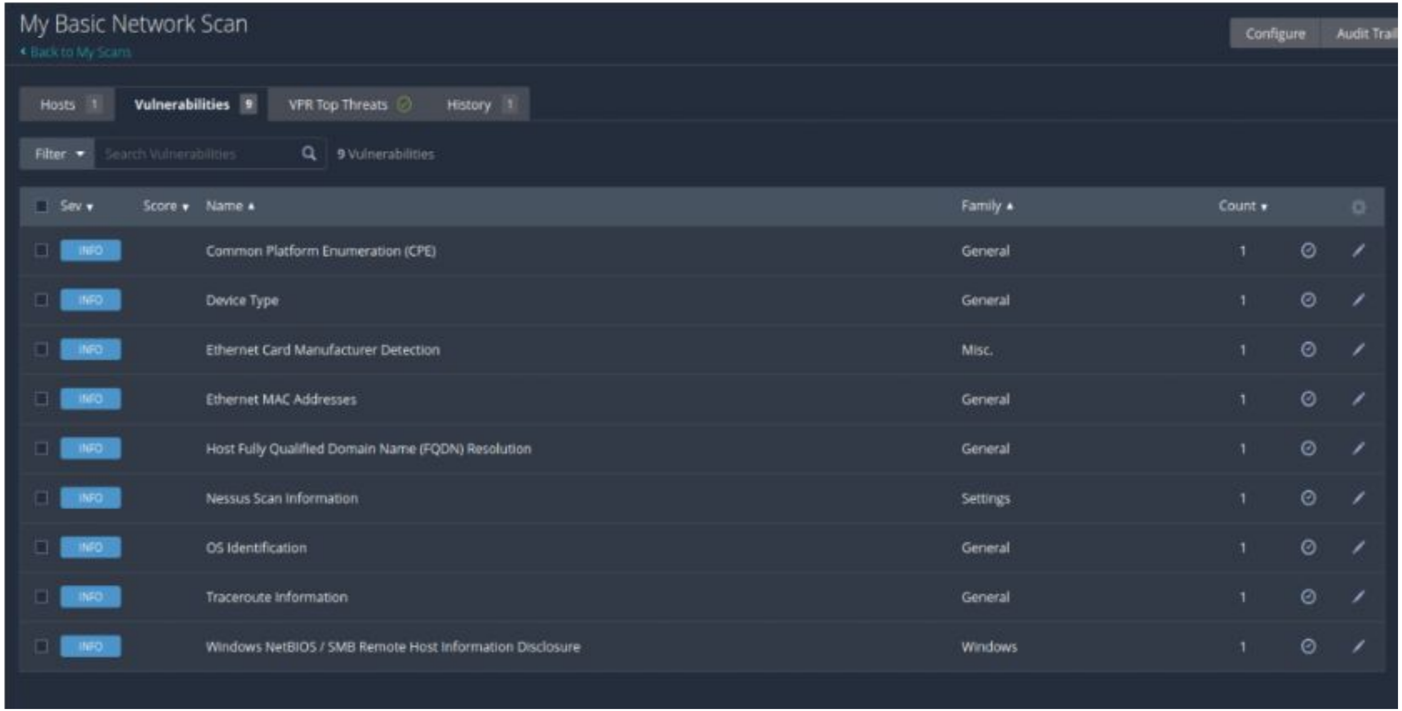
There are no issues for this project.

MQTT Vulnerability Testing
(Mathew)

Nessus Scan

Nessus is the gold standard of vulnerability testing.

No vulnerabilities were detected within the scope of the project.

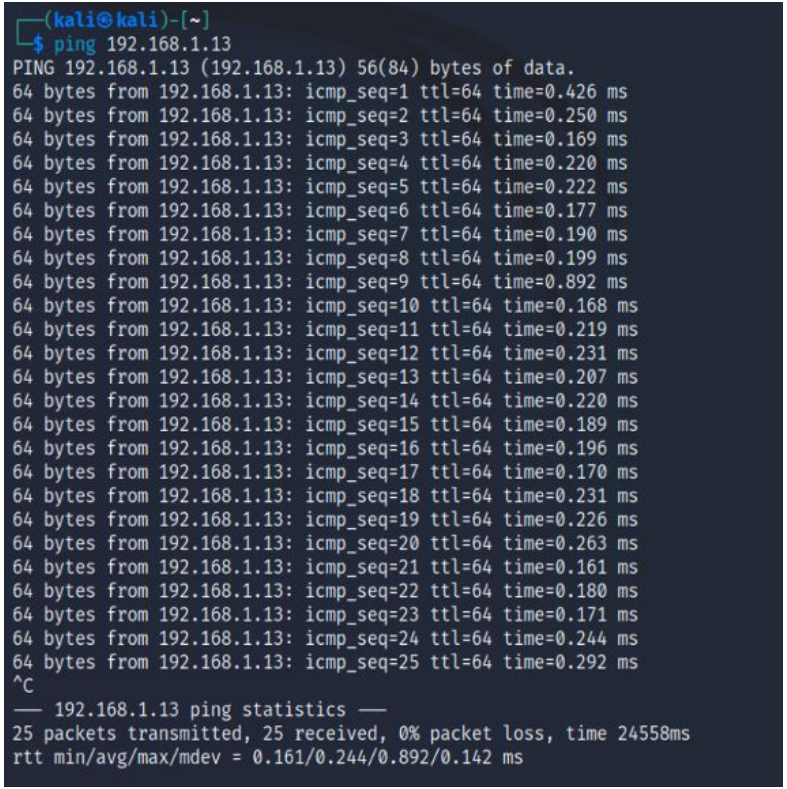


■	Sev ▾	Score ▾	Name ▴	Family ▴	Count ▾		
□	INFO		Common Platform Enumeration (CPE)	General	1	✓	✎
□	INFO		Device Type	General	1	✓	✎
□	INFO		Ethernet Card Manufacturer Detection	Misc.	1	✓	✎
□	INFO		Ethernet MAC Addresses	General	1	✓	✎
□	INFO		Host Fully Qualified Domain Name (FQDN) Resolution	General	1	✓	✎
□	INFO		Nessus Scan Information	Settings	1	✓	✎
□	INFO		OS Identification	General	1	✓	✎
□	INFO		Traceroute Information	General	1	✓	✎
□	INFO		Windows NetBIOS / SMB Remote Host Information Disclosure	Windows	1	✓	✎
)

Latency Testing
(Mathew)

Ping

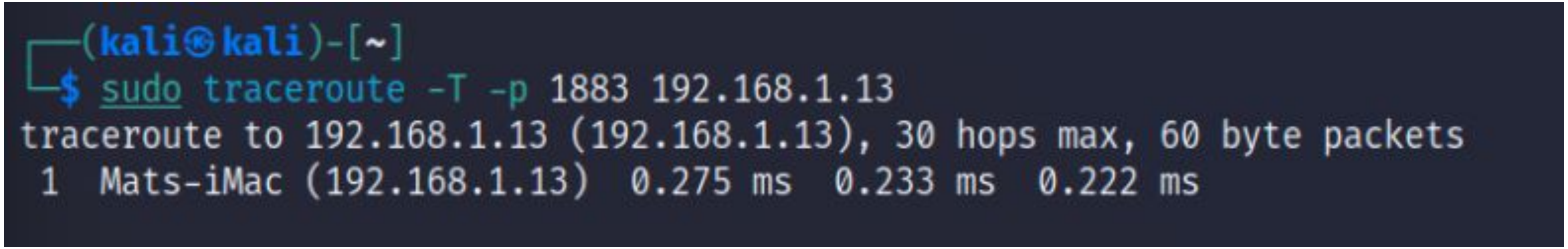
Standard test for latency, run while opening and closing the IoT door.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.13
PING 192.168.1.13 (192.168.1.13) 56(84) bytes of data.
64 bytes from 192.168.1.13: icmp_seq=1 ttl=64 time=0.426 ms
64 bytes from 192.168.1.13: icmp_seq=2 ttl=64 time=0.250 ms
64 bytes from 192.168.1.13: icmp_seq=3 ttl=64 time=0.169 ms
64 bytes from 192.168.1.13: icmp_seq=4 ttl=64 time=0.220 ms
64 bytes from 192.168.1.13: icmp_seq=5 ttl=64 time=0.222 ms
64 bytes from 192.168.1.13: icmp_seq=6 ttl=64 time=0.177 ms
64 bytes from 192.168.1.13: icmp_seq=7 ttl=64 time=0.190 ms
64 bytes from 192.168.1.13: icmp_seq=8 ttl=64 time=0.199 ms
64 bytes from 192.168.1.13: icmp_seq=9 ttl=64 time=0.892 ms
64 bytes from 192.168.1.13: icmp_seq=10 ttl=64 time=0.168 ms
64 bytes from 192.168.1.13: icmp_seq=11 ttl=64 time=0.219 ms
64 bytes from 192.168.1.13: icmp_seq=12 ttl=64 time=0.231 ms
64 bytes from 192.168.1.13: icmp_seq=13 ttl=64 time=0.207 ms
64 bytes from 192.168.1.13: icmp_seq=14 ttl=64 time=0.220 ms
64 bytes from 192.168.1.13: icmp_seq=15 ttl=64 time=0.189 ms
64 bytes from 192.168.1.13: icmp_seq=16 ttl=64 time=0.196 ms
64 bytes from 192.168.1.13: icmp_seq=17 ttl=64 time=0.170 ms
64 bytes from 192.168.1.13: icmp_seq=18 ttl=64 time=0.231 ms
64 bytes from 192.168.1.13: icmp_seq=19 ttl=64 time=0.226 ms
64 bytes from 192.168.1.13: icmp_seq=20 ttl=64 time=0.263 ms
64 bytes from 192.168.1.13: icmp_seq=21 ttl=64 time=0.161 ms
64 bytes from 192.168.1.13: icmp_seq=22 ttl=64 time=0.180 ms
64 bytes from 192.168.1.13: icmp_seq=23 ttl=64 time=0.171 ms
64 bytes from 192.168.1.13: icmp_seq=24 ttl=64 time=0.244 ms
64 bytes from 192.168.1.13: icmp_seq=25 ttl=64 time=0.292 ms
^C
── 192.168.1.13 ping statistics ──
25 packets transmitted, 25 received, 0% packet loss, time 24558ms
rtt min/avg/max/mdev = 0.161/0.244/0.892/0.142 ms
```

Traceroute

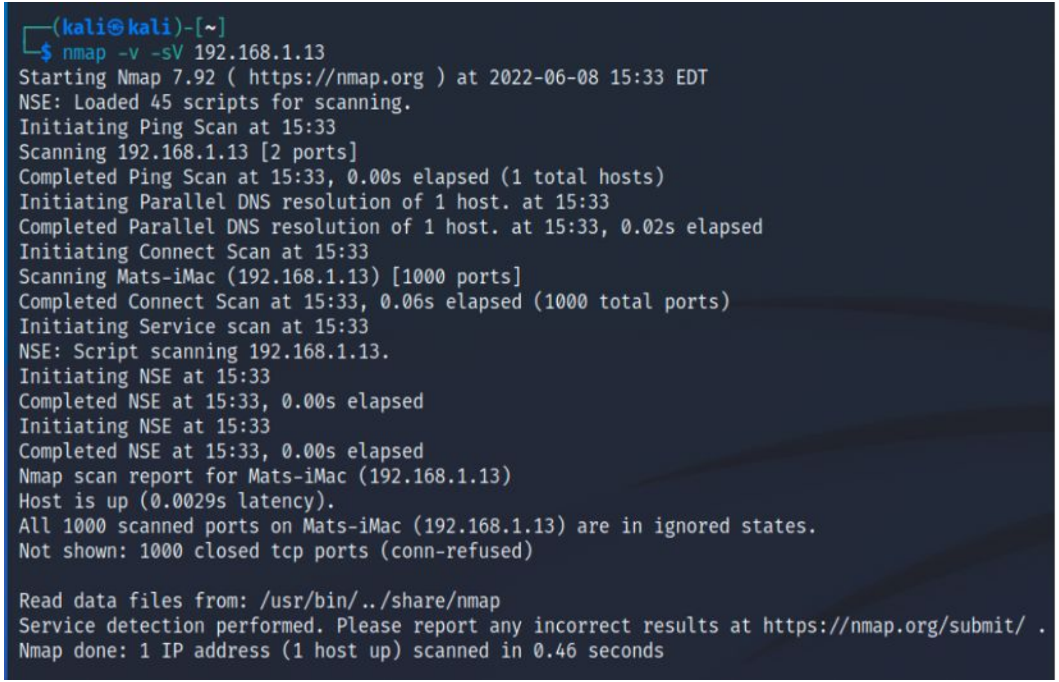
Standard test for latency, run while opening and closing the IoT door.



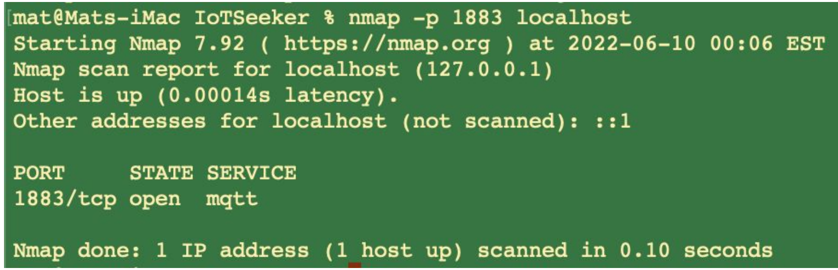
```
┌──(kali㉿kali)-[~]
└─$ sudo traceroute -T -p 1883 192.168.1.13
traceroute to 192.168.1.13 (192.168.1.13), 30 hops max, 60 byte packets
 1  Mats-iMac (192.168.1.13)  0.275 ms  0.233 ms  0.222 ms
```

NMAP

NMAP very popular tool for used for viewing open listening ports and latency testing. Ports actively ignoring scan, but when changing from IP to Localhost nmap shows port 1883 is open for mqtt.



```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sV 192.168.1.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-08 15:33 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 15:33
Scanning 192.168.1.13 [2 ports]
Completed Ping Scan at 15:33, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:33
Completed Parallel DNS resolution of 1 host. at 15:33, 0.02s elapsed
Initiating Connect Scan at 15:33
Scanning Mats-iMac (192.168.1.13) [1000 ports]
Completed Connect Scan at 15:33, 0.06s elapsed (1000 total ports)
Initiating Service scan at 15:33
NSE: Script scanning 192.168.1.13.
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Nmap scan report for Mats-iMac (192.168.1.13)
Host is up (0.0029s latency).
All 1000 scanned ports on Mats-iMac (192.168.1.13) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```



```
mat@Mats-iMac IoTSeeker % nmap -p 1883 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 00:06 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE
1883/tcp open  mqtt

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```