TRYHACKME CTF|Industrial Intrusion|
June-27-2025 by Ronna Curelea(Ronna0x)

http://www.youtube.com/@ronna0x
https://youtu.be/BrEcdBNpxNE

Bypassing IoT industrial controls by opening gate without HID badge

#1- TASK The Breach

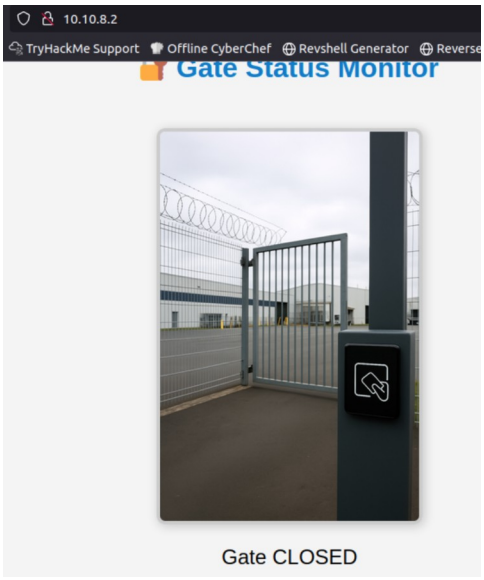
Scan for open ports

rustscan -a 10.10.8.2

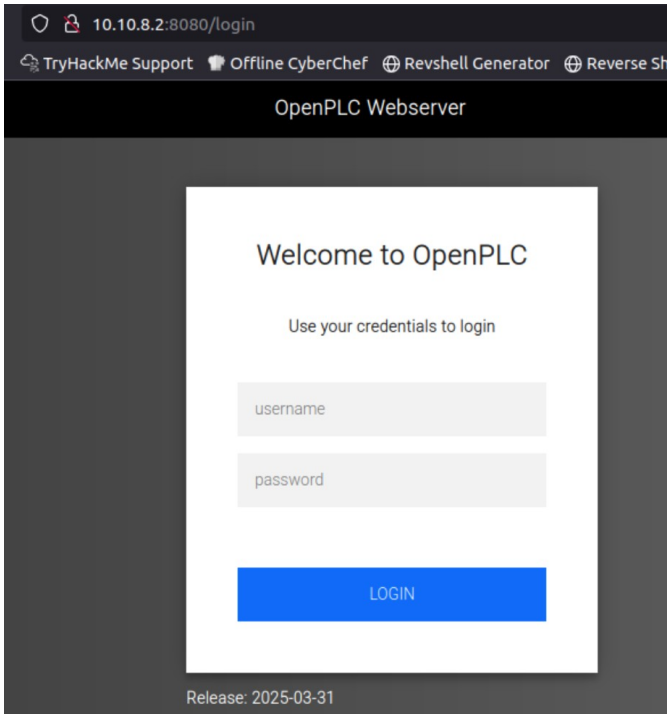
```
Scanned at 2025-06-27 09:43:57 UTC for 0s

PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack
80/tcp    open  http         syn-ack
102/tcp   open  iso-tsap     syn-ack
502/tcp   open  mbap         syn-ack
1880/tcp  open  vsat-control syn-ack
8080/tcp  open  http-proxy   syn-ack
44818/tcp open  EtherNetIP-2 syn-ack
```

Lets first check out these ports; 80, 8080, and 1880.



Port 80



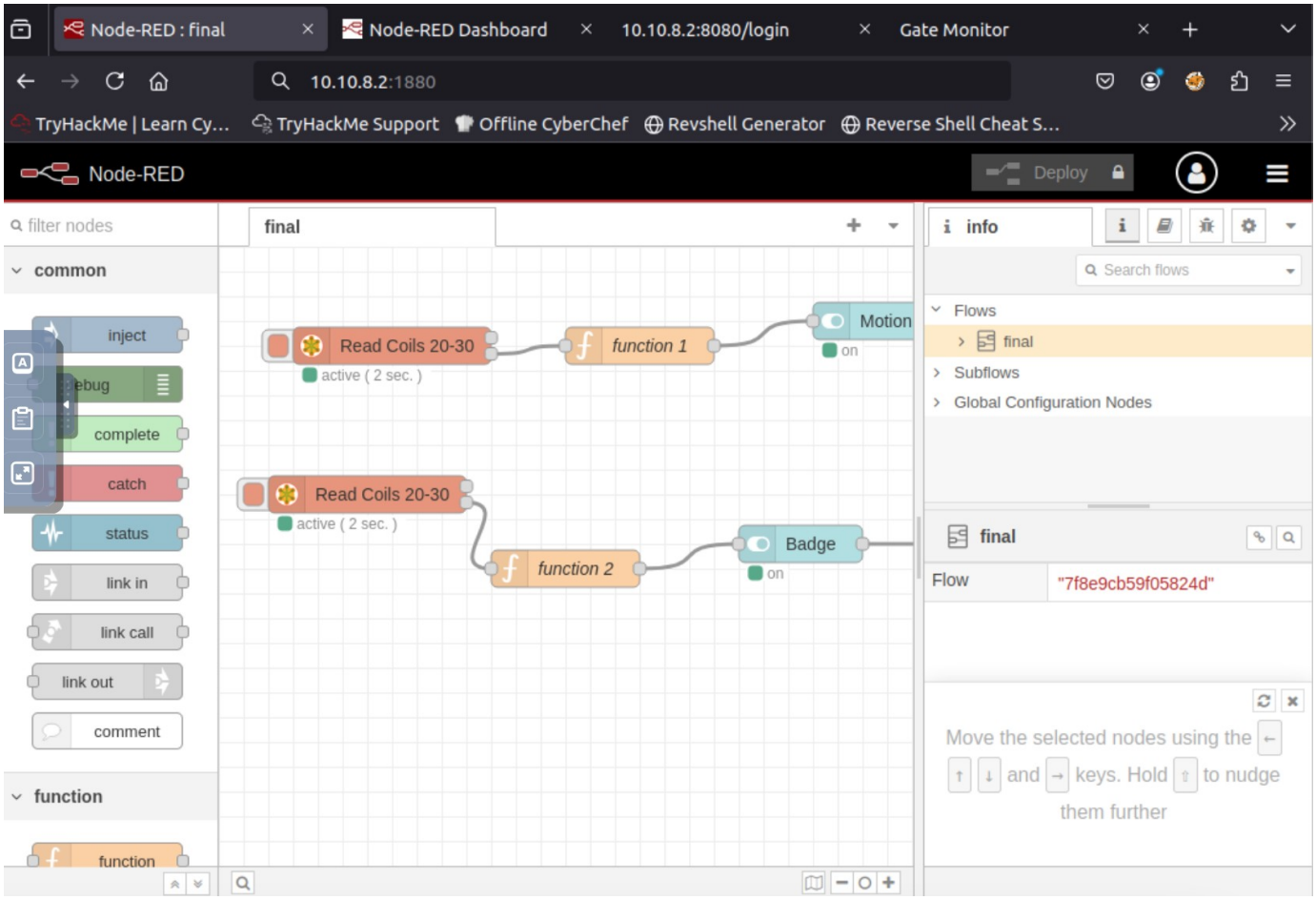
Port 8080

To find out what *OpenPLC* is, I ran an nmap scan of this IoT device.

nmap -sC -sV -A -p- [10.10.8.2]

```
</html>
|_http-server-header: Werkzeug/3.1.3 Python/3.12.3
|_http-title: Gate Monitor
102/tcp   open  iso-tsap      Siemens S7 PLC
| fingerprint-strings:
|   TerminalServerCookie:
|_    Cookie: mstshash=nmap
| s7-info:
|   Module: 6ES7 315-2EH14-0AB0
|   Basic Hardware: 6ES7 315-2EH14-0AB0
|   Version: 3.2.6
|   System Name: SNAP7-SERVER
|   Module Type: CPU 315-2 PN/DP
|   Serial Number: S C-C2UR28922012
|_  Copyright: Original Siemens Equipment
```

MAC Address: 02:58:E0:8D:53:21

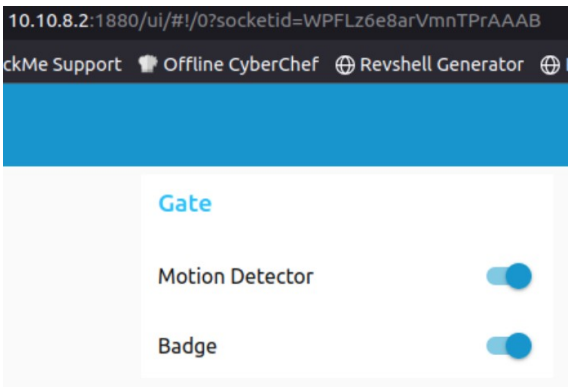


Port 1880

Dashboard of the Gate Opener
Can be interacted with by altering configurations and settings.

I then did a quick manual enumeration on 8080 for common endpoints such as: admin, settings, ui, dashboard, etc

Only http://10.10.8.2:1880/ui/ worked.



If I toggle those options I can change the settings for the gate and it will respond accordingly. At this point I can disable the badge and motion detector and the gate will open by default.