Challenge: Watch Tower

# Challenge Description :

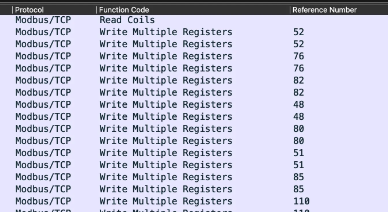
**Our infrastructure monitoring system detected some abnormal behavior and initiated a network capture. We need to identify information the intruders collected and altered in the network.**

# Context :

## We are given a PcaP file to Analyze. Within the Pcap file is a capture of a bunch of Modbus packets.

# Flag :

* **First Install the PcaP file and open it up with Wireshark, the first thing you will notice it that it's not a normal looking TCP steam or http requests packets its Modbus packets**
* **Looking the the packets and the types of packet request function codes they are sending / retrieving.**
* **There are three types of Modbus function codes Being used in this capture file, Two of them are [Write Multiple Coils] and [Read Coil] function codes that seem to not have any data.**
* **The last type of function code being used is the [Write Multiple Registers] function code that does contain a bit of data.**

****

* **Filtering it to only show the [Write Multiple Registers] function codes and then getting the data from each packet variable named [ Reference Number ].**
* **We can see that each Reference number is a Ascii decimal code, which can be converted back to a full string. Giving us the flag and completing this challenge.**
* **You can automate the process of extracting the reference numbers and then converting them.**
* **The Flag after converting it all back is :**

**HTB{3nc2yp710n?\_n3v32\_h342d\_0f\_7h47!@^}**