**LAB 3: SCADA CONTROL SYSTEM NETWORK ENUMERATION AND DENIAL OF SERVICE**

**Manual**

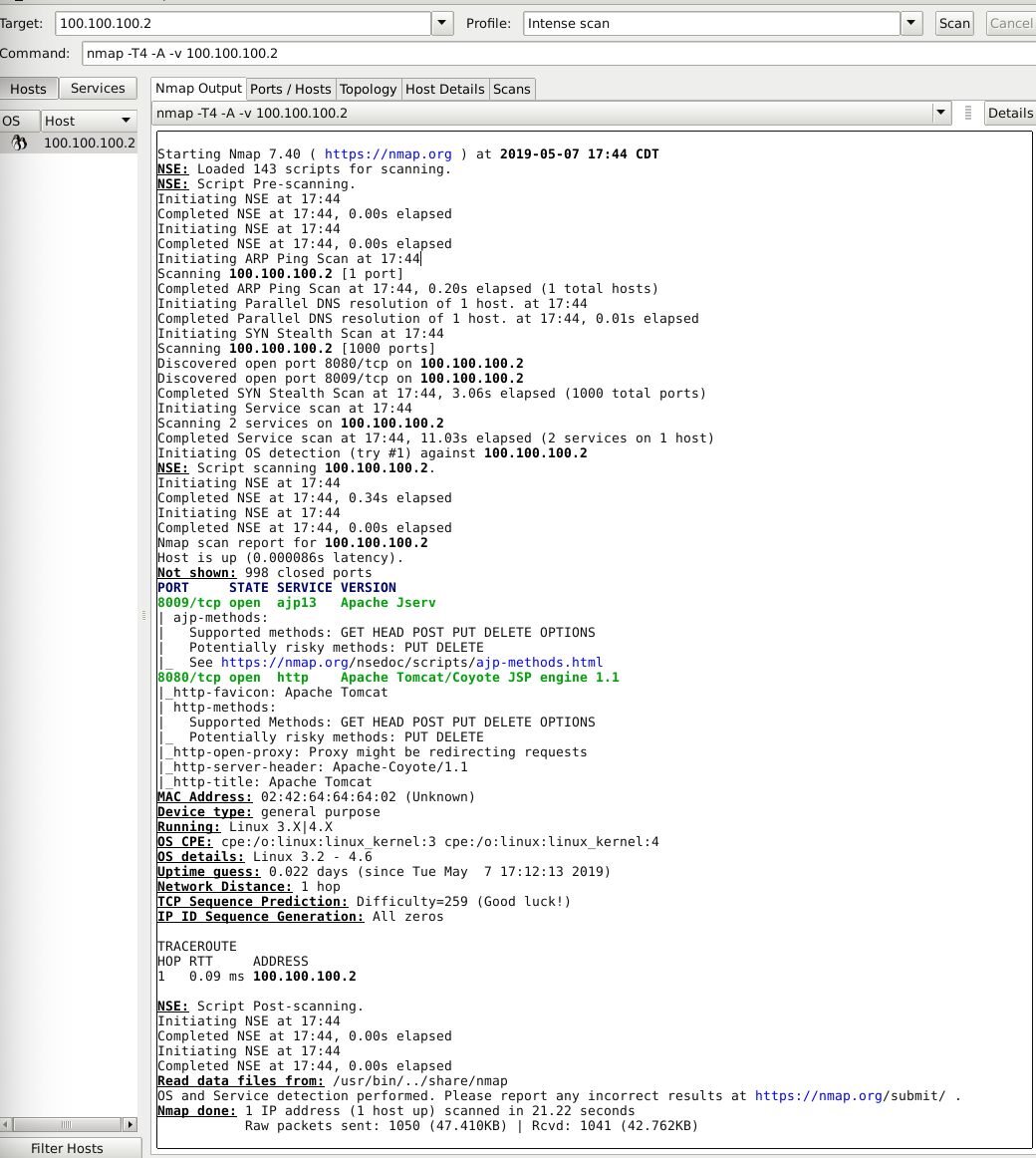
**Pamela Gavojdian**

**pamgavojdian@hotmail.com**

**Exercise #1 - Introduction to NMAP/ZENMAP**

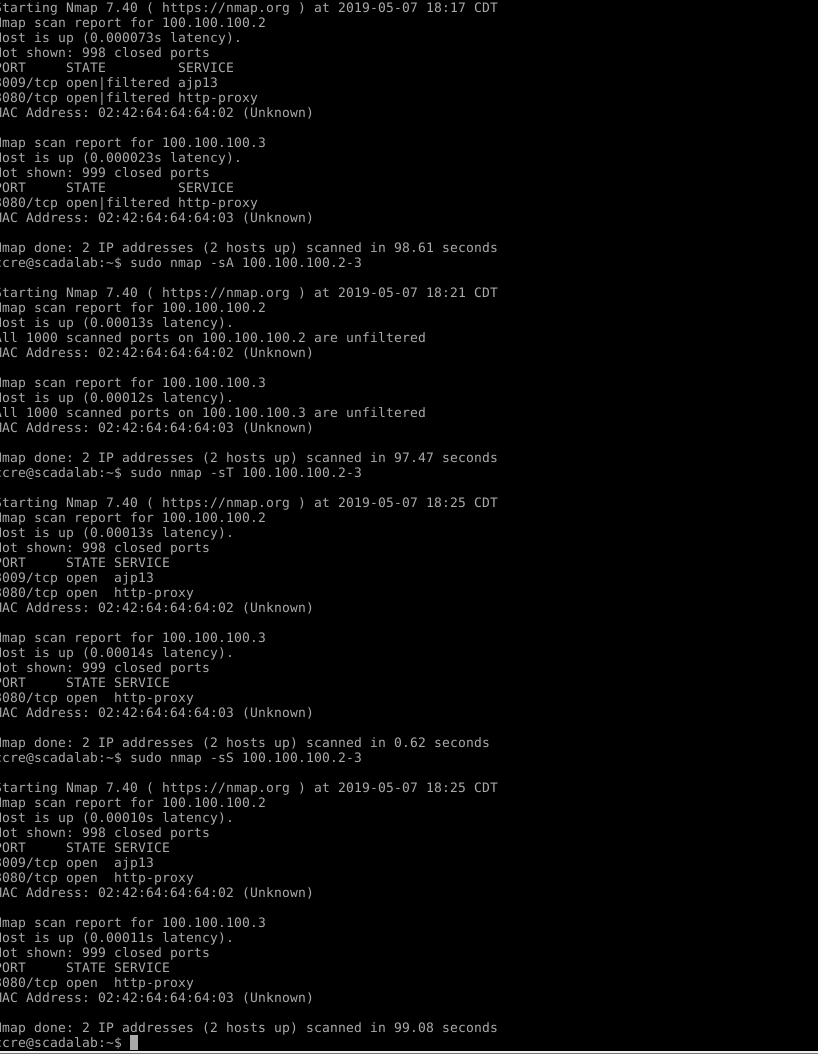
**BASIC USAGE**

**In this step and the step before I had the water pump docker containers running and then I in the target network I added my IP adress of 100.100.100.2 and conducted a full scan to see if all my ports are open and their status.**



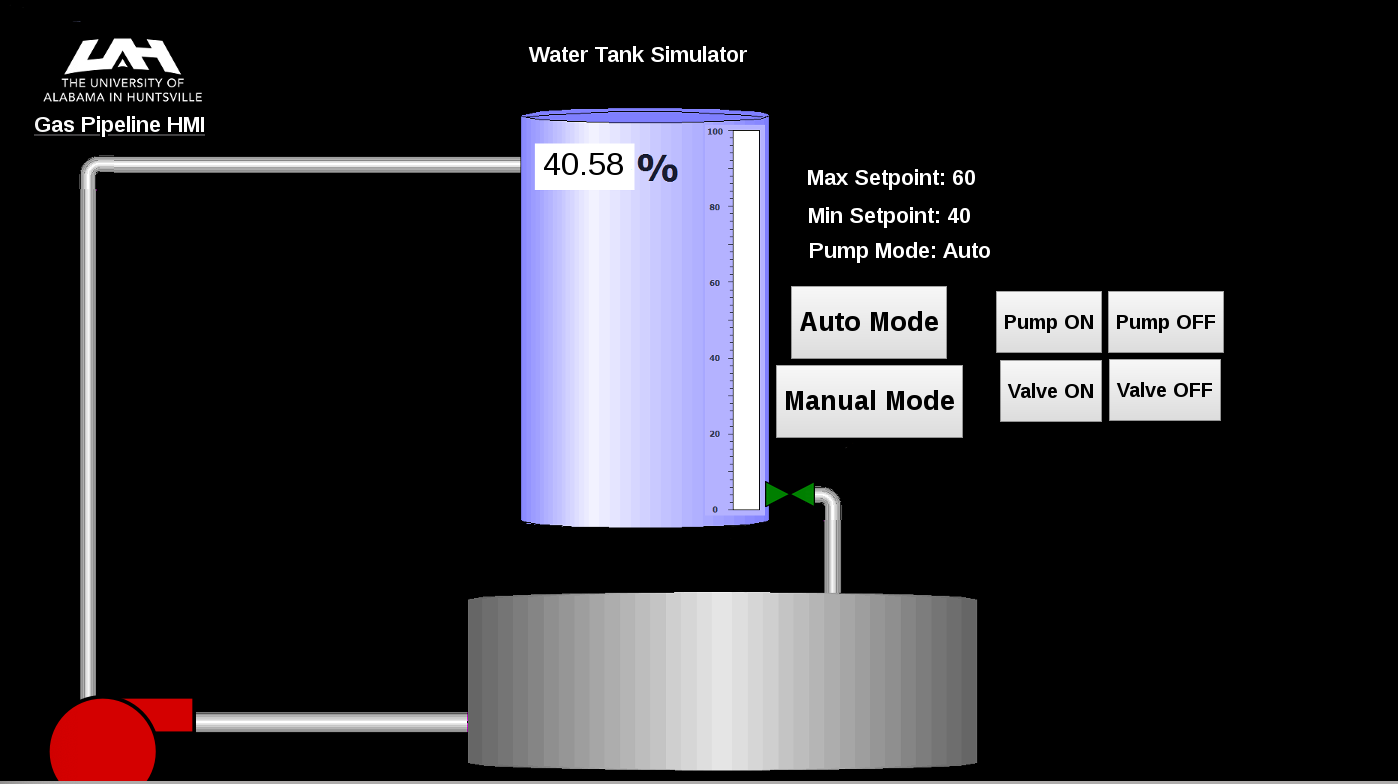
**DIFFERENT KINDS OF SCANS**

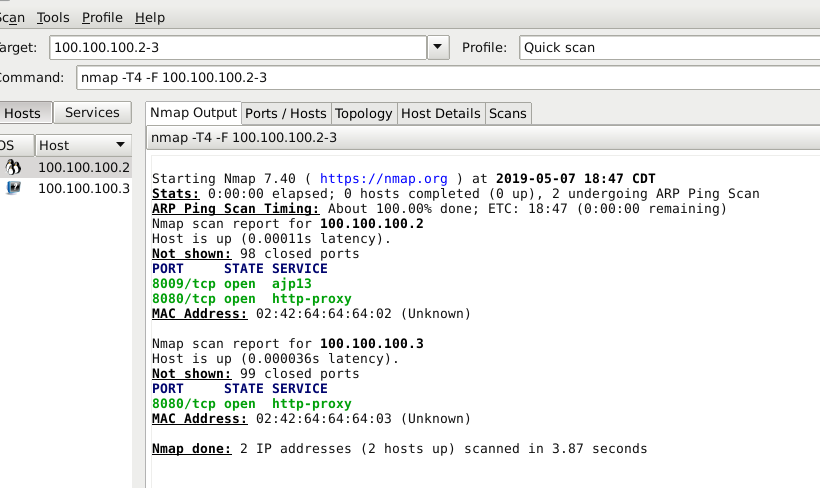
**below I performed different scans after opening and enabling the Water Tank HMI. ou can see the Xmas scan, Null scan, ACK scan and**

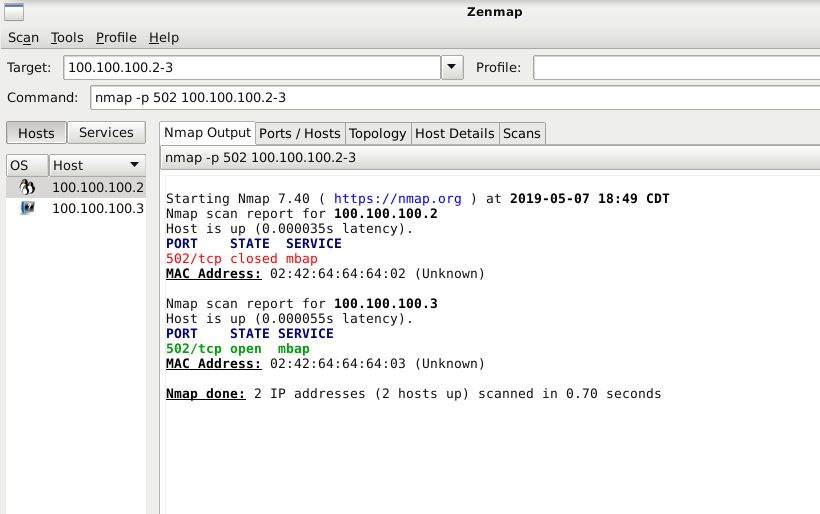


**Exercise #2 - Network Enumeration using Nmap/Zenmap**

below you can observe that the water tank simulator has been turned on and the water levels in the tank are fluctuating.

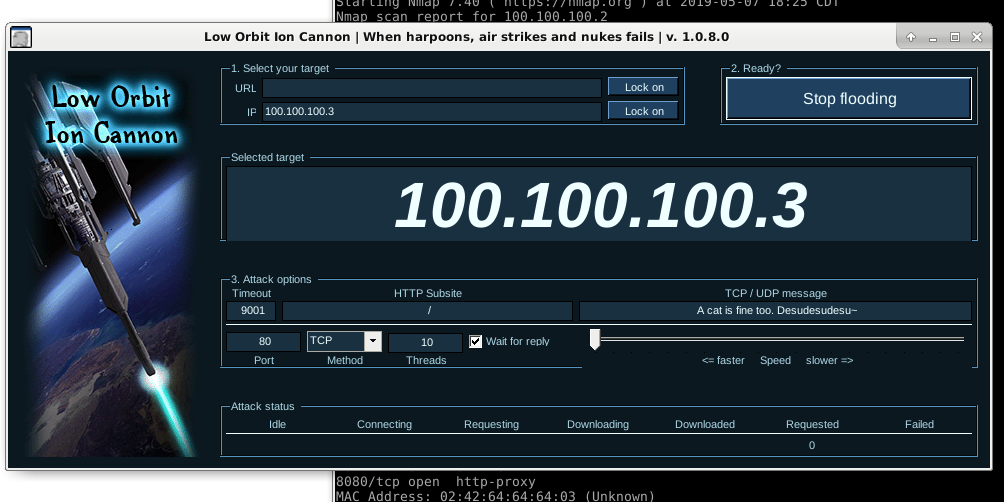






**Exercise #4 - Peform Denial of Service Attack**

once opeing the lab 3 directory I was able to run Low Orbit Ion Cannon and then was able to enter my IP adress and select the TCP mehod to begin flooding the server of the host. The program did end up crashing the VM when it ran.

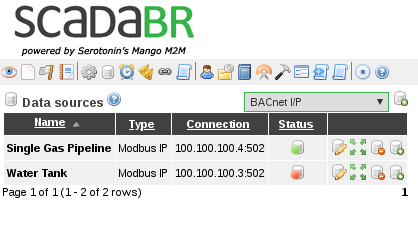


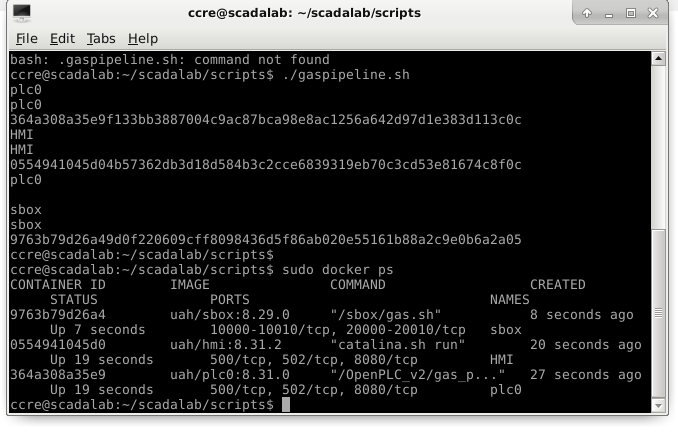
**LAB 2: SCADA Control System Network Packet Alteration and Injection**

**Manual**

**Exercise #1 - MITM Setup and Install ettercap**

**Running a MITM container and installing Ettercap**

Below you can see that I have enabled the Single Gas Pipeline so the pipeline is open and you can see the percentage of gas flowing through when looking at the GUI. You can also see that the Gas Pipelines are being recorded as well. 



While working on lab 4 I was not able to access anything else past this point. I was getting error messages every time I tried. I even tried the clean code and nothing had helped. I have attached the error code below.

