Akshay Galgali
2060882

CIS 6357 - MODBUS ATTACK & PACKET INJECTION LAB REPORT

Experiment Learnings:

How to setup two VMs and configured them as Master and Slave Systems. Established connection of Master and Slave system over a private LAN (Local Area Network) using MODBUS protocol, port number 502 and IP addresses, obtaining PLC information, and how to set up the PLC onto the listen mode, how to read and write into PLCs, and lastly how to add, read and how to inject packet into Slave system using its hexadump value.

Experiment:

In this experiment, we have used Modsak Simulator to simulate the Modbus Master and Modbus Slave environment. Firstly, I configured Modbus Slave System by setting it to Slave mode in and saved its Slave ID as 2, and opened a connection by setting its Ip address and port number as 502 into Interface to Master, and started tracing and running the Slave system. Secondly, I configured Modbus Master system by following same procedure by with different values. After this I tested the Master Slave communication by sending packets through Master to Slave system by using define command - 17 report slave Id command and the communication was successful we can observe this by tracing the packets on Slave system. Lastly, created a register on Slave system by add register command and configuring it by specified values, and I read this registry from Master system using – Read holding Registry command and providing same values used before, and read the values in Received Data window. And wrote a Slave registry from Master system using – Write holding registry and altered the values as required and read the registry from Slave system. In packet Injection I followed same steps as before and after establishing proper communication between Master and Slave system, I started live packet capture on Slave system and attacked the Slave system using Attacker's system (Ubuntu) using Hexaedit attack where I provided the Hexadump value (Modbus/TCP) generated during most recent packet capture onto Slave system. Then, I created an attack file which included specific Slave's Hexadump value used previously and attacked the Slave system by injection packets.

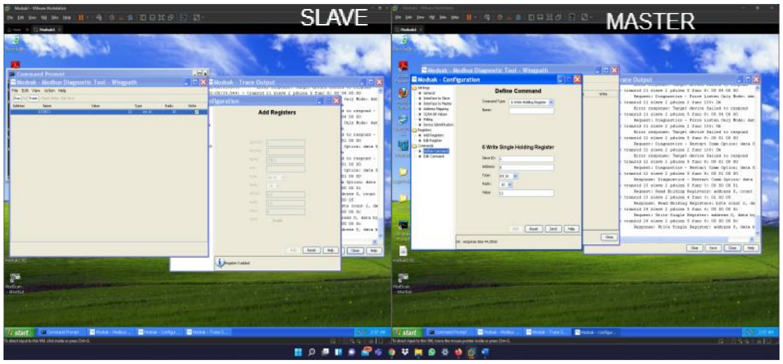
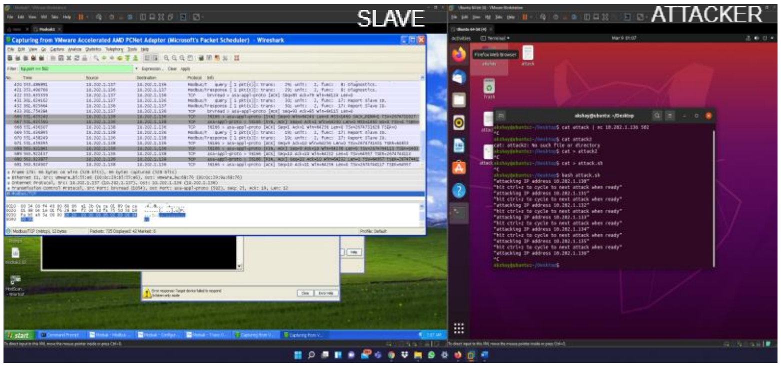


Fig 1: Adding new registry onto Master system and reading it on Slave system.


SLAVE
ATTACKER
Capturing from VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark
Activities
Terminal
attack
Trash

```
akshay@ubuntu:~/Desktop$ cat attack | nc 10.202.1.130 502
^C
akshay@ubuntu:~/Desktop$ cat attack2
cat: attack2: No such file or directory
akshay@ubuntu:~/Desktop$ cat > attack2
^C
akshay@ubuntu:~/Desktop$ cat > attack.sh
^C
akshay@ubuntu:~/Desktop$ bash attack.sh
"attacking IP address 10.202.1.130"
"hit ctrl+z to cycle to next attack when ready"
"attacking IP address 10.202.1.131"
"hit ctrl+z to cycle to next attack when ready"
"attacking IP address 10.202.1.132"
"hit ctrl+z to cycle to next attack when ready"
"attacking IP address 10.202.1.133"
"hit ctrl+z to cycle to next attack when ready"
"attacking IP address 10.202.1.134"
"hit ctrl+z to cycle to next attack when ready"
"attacking IP address 10.202.1.135"
"hit ctrl+z to cycle to next attack when ready"
"attacking IP address 10.202.1.130"
^C
akshay@ubuntu:~/Desktop$
```

Fig 2: Attacker System injecting packet through attack file execution into Slave system.

Challenges:

The challenges I faced during this experiment was to configure two VMs and configure them as Master and Slave system using Modsak Simulator. I struggled to build a connection and communication between the Master and Slave system because their Ip addresses were clashing at first, after sometime I modified required setting, which helped in establishing proper communication between Master and Slave system. Once, the communication was established it was now an uncomplicated task to perform the specified experiment.