ICS015 ICS Lab 7 Exploiting a PLC Using Metasploit

Lab Objective

The objective of this lab is to use Kali Linux, Metasploit and Modbusclient to exploit a PLC using Modbus/TCP.

In this lab, you will learn to:

- Scan and enumerate devices on an internal network,

Lab Environment

This lab will require a wireless laptop with Kali Linux flash drive and ICS lab kit.

Lab Duration

25 minutes

Lab Tasks

Use Kali Linux and Metasploit to connect to a PLC device.

Background

Kali Linux is a Debian-derived **Linux** distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd.

The **Metasploit** Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

The Modbus client utility module allows reading and writing data to a PLC using the Modbus protocol. This module is based on the 'modiconstop.rb' Basecamp module from DigitalBond, as well as the **mbtget perl** script.

Lab Scenario

Once the network is scanned and a PLC device is located on the network, the next step is to attempt connection to the device via a remote connection. For this scenario we will attempt to connect to the Do-More PLC and send control commands to coils and registers on the same network as the PLC.

Exploiting A PLC Using Metasploit

1. Insert the provided flash drive that contains Kali Linux. Restart your laptop and choose to boot from USB drive. Select Live USB Persistent from the Kali boot options.
2. Provide username and password from the previous lab
3. Connect to the Buffalo router that is included in your ICS lab kit using an Ethernet cable
4. Launch Metasploit from the left menu. Fig 1

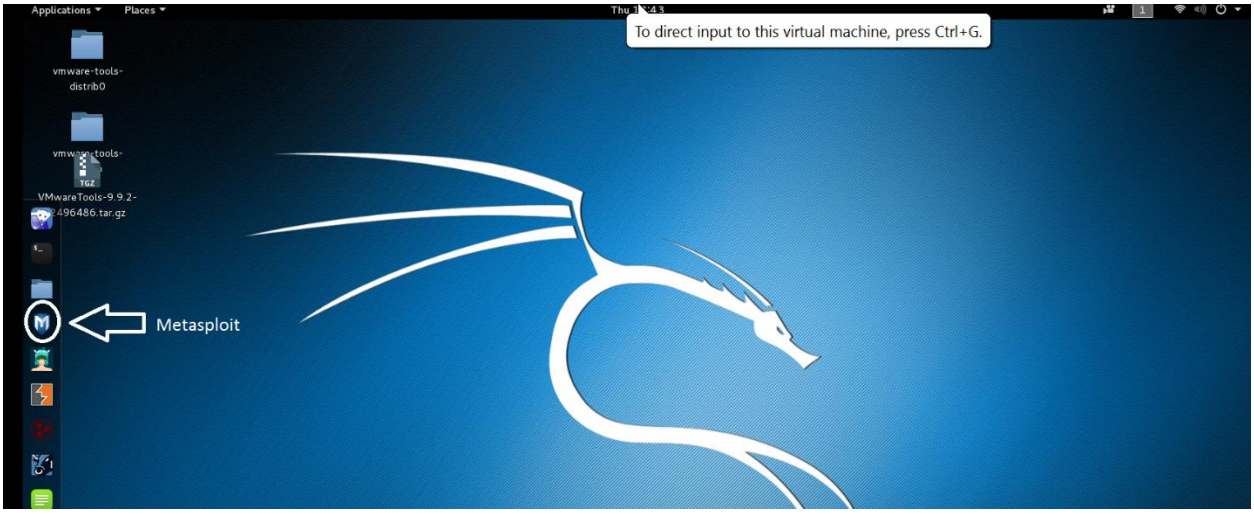

Fig. 1

5. Type command ***use auxiliary/scanner/scada/modbusclient*** into terminal to access the Metasploit auxiliary program that we will be using to exploit the PLC. Fig. 2

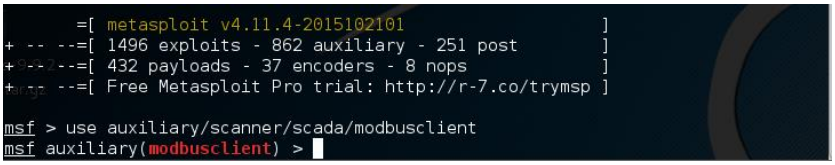

Fig. 2

6. Use the ***show actions*** command to see the parameters for the software options. Fig. 3

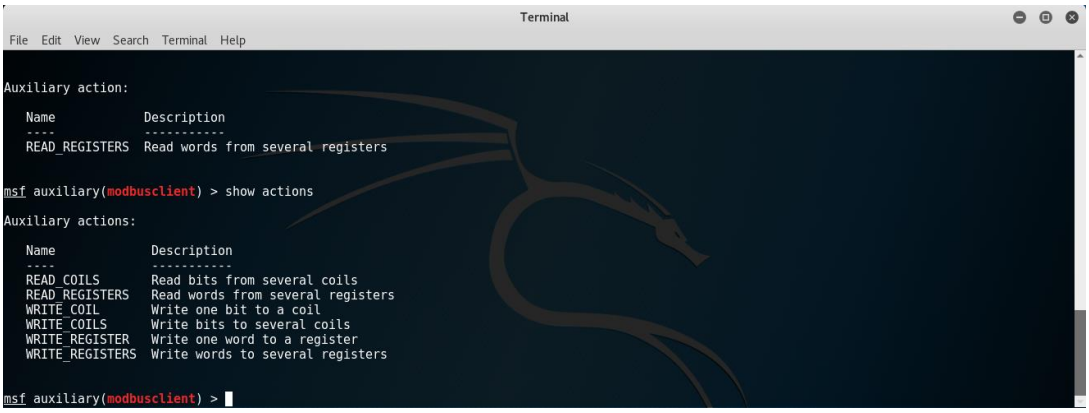

Fig. 3

7. Use the ***show options*** command to see the parameters for the software actions. Fig. 4

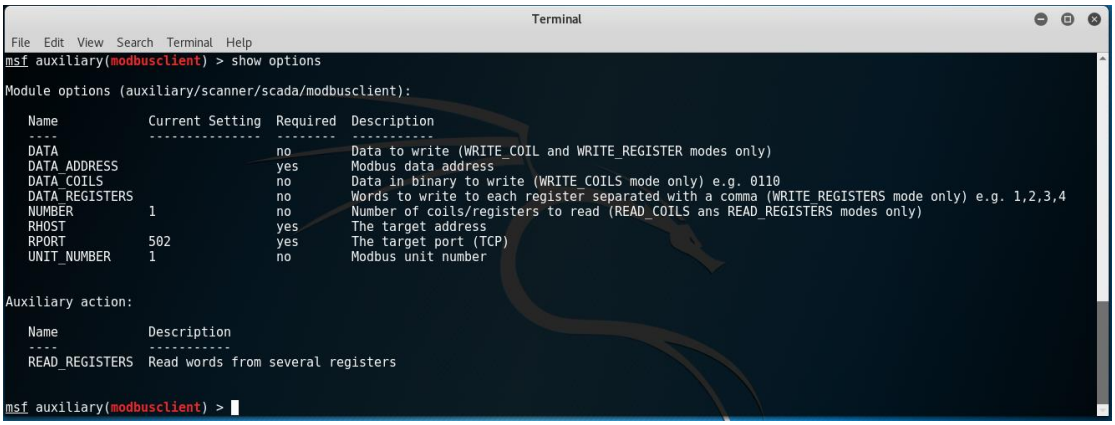

Fig. 4

8. Assign a host to exploit. Use the ***set RHOST 192.168.11.x*** command to select the PLC. Fig. 5

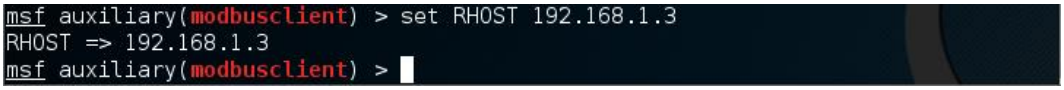

Fig. 5

9. Assign the port that we will be using for the exploitation. Use the *set* ***RPORT 502*** command to select port 502, which is the port that Modbus uses to communicate. Fig. 6

Fig. 6

Reading a Register Value

10. For the first attack scenario, we will read the value of the registers on the PLC. Modbusclient allows the user to read from 0 to 65,535 data addresses and coils.

- The address of the registers in Do-More begin at 1. For this lab, we will use **n-1** to set the address of the registers. I.e. if you want to read the value in memory register 20, you will simply subtract 1 from 20 and enter that value into modbusclient. The same application applies to reading and writing to coils.

11. Assign the address of the register. Enter the selected register value into the command ***set DATA_ADDRESS [selected value]***. *For this read, we will enter* ***0*** *to read register 1*. Fig. 7

Fig. 7

12. Read the address of the selected register by using the ***set action READ_REGISTERS*** command. Fig.8 below.

Fig 8

13. Use the ***run*** command to read the register value. Fig 9

Fig. 9

Reading a Coil Value

14. Assign the address of the coil. Enter the selected coil value into the command ***set DATA_ADDRESS [selected value]***. *Enter 0 (this action will read the first coil in the program).* Fig 10

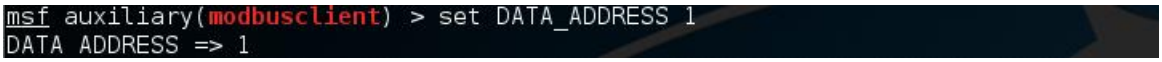

Fig. 10

15. Read the address of the selected coil by using the ***set action READ_COILS*** command. Fig 11
16. Use the ***run*** command to read the coil value. **Fig 12**

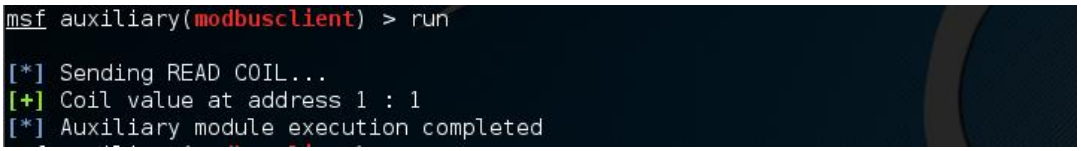

Fig. 12

Write a Value to a Coil

17. Values for the coils with be either ON or OFF, 0 or 1. We will attempt to turn off the coil at the selected address.
18. Type: ***show actions***
19. Type**: *set action WRITE_COILS***

20. Type: ***show options***
21. Select **DATA_COILS** from options using **set action. I.e. *set action DATA_COILS.*** The data to be written to the coil is 0 for ON. Example: ***set action DATA_COILS 0***
22. Use the ***set action WRITE_COILS*** to change the coil value. Fig. 13
23. Use the ***run*** command to read the coil value as shown in FIG 12
24.

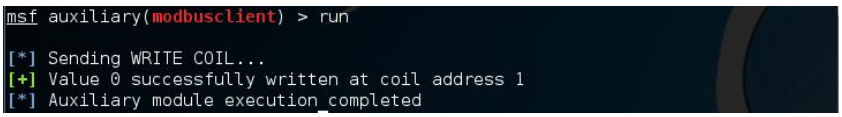

Fig. 15

25. Select a register address or coil address from your PLC program and practice writing and reading values from the PLC remotely.