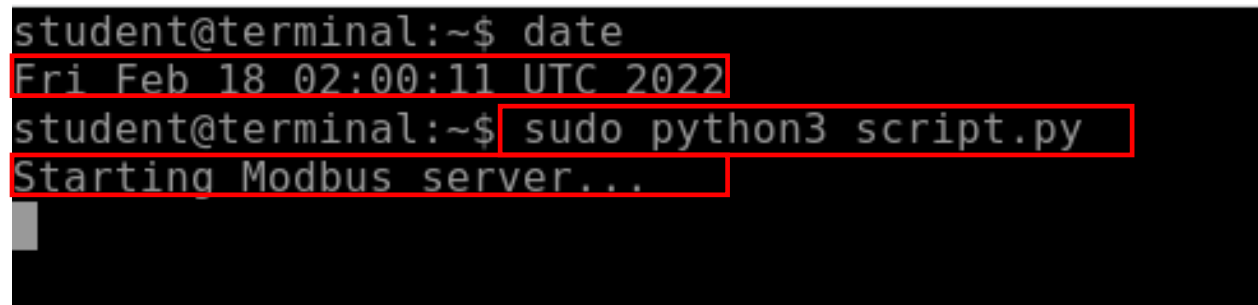


Industrial Control Systems Security

Assignment 1: scanning Modbus server

Roozah Khan

1. Verbally explain the steps you have taken to make the Modbus run. Add a screenshot indicating you are running the Modbus server on **terminal.example.com**, which must include:
 - a. The date and time when you run it (use the `date` command to show the date).
 - b. The command you use to run the Modbus server.
 - c. The output indicating the server is successfully running.



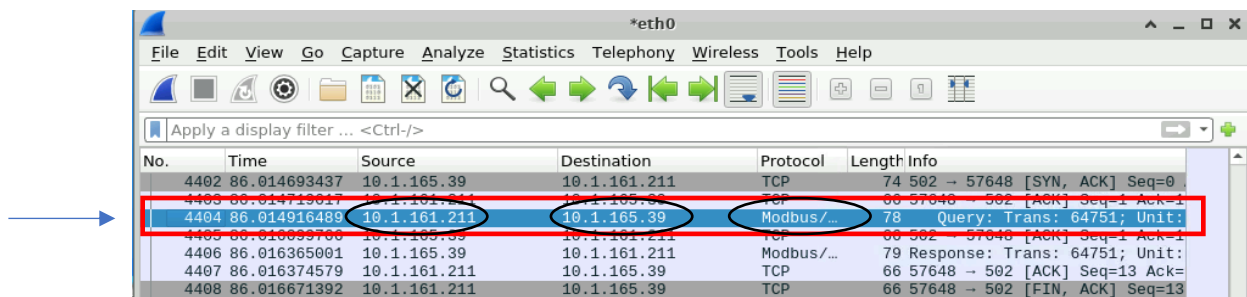
```
student@terminal:~$ date
Fri Feb 18 02:00:11 UTC 2022
student@terminal:~$ sudo python3 script.py
Starting Modbus server...
```

I used the “date” command to show the date and time. After, I used the “Vi” text editor command to copy and paste the script given to us and saved it in a file called “script.py.” I used the “sudo python3 script.py” command to run the script and the output started running the Modbus server successfully.

2. A screenshot that shows you have successfully used the `modbus-cli` to communicate with the Modbus server. The screenshot must include:
 - a. The command you have typed
 - b. The output of the command.

```
student@desktop:~$ modbus 10.1.165.39 h@39/I
Parsed 0 registers definitions from 1 files
39: 1114129 0x110011
student@desktop:~$ date
Fri Feb 18 03:22:27 UTC 2022
student@desktop:~$
```

3. A screenshot of the captured packet (one packet is suffice) in Wireshark, which must include:
 - a. The source and destination IP addresses of the packet.
 - b. The protocol must show it is a Modbus packet.



4. Inspect the captured packet in Wireshark, and answer the following questions.
 - a. What are the values of: Transaction Identifier, Protocol Identifier, Length, and Unit Identifier? Attach a screenshot to support your answer.

No.	Time	Source	Destination	Protocol	Length	Info
4402	86.014693437	10.1.165.39	10.1.161.211	TCP	74	502 → 57648 [SYN, ACK]
4403	86.014719617	10.1.161.211	10.1.165.39	TCP	66	57648 → 502 [ACK] Seq=1
4404	86.014916489	10.1.161.211	10.1.165.39	Modbus/...	78	Query: Trans: 64751;
4405						
4406						
4407						
4408						
4409						
4410						
4411						
4412						
4413						
4414						
4415						
4416						

Wireshark · Packet 4404 · eth0

- Frame 4404: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0
- Ethernet II, Src: 12:a9:0b:b5:bd:25 (12:a9:0b:b5:bd:25), Dst: 12:fa:87:93:7e:31 (12:fa:87:93:7e:31)
- Internet Protocol Version 4, Src: 10.1.161.211, Dst: 10.1.165.39
- Transmission Control Protocol, Src Port: 57648, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
- Modbus/TCP**
 - Transaction Identifier: 64751
 - Protocol Identifier: 0
 - Length: 6
 - Unit Identifier: 255
- Modbus
 - .0000 0011 = Function Code: Read Holding Registers (3)
 - Reference Number: 39
 - Word Count: 2

The value of this modbus protocol is:

Transaction Identifier: 64751

Protocol Identified: 0

Length: 6

Unit Identifier: 255

No.	Time	Source	Destination	Protocol	Length	Info
4404	86.014916489	10.1.161.211	10.1.165.39	Modbus/...	78	Query: Trans: 64751;
4406	86.016365001	10.1.165.39	10.1.161.211	Modbus/...	79	Response: Trans: 64751;

Wireshark · Packet 4406 · eth0

- Frame 4406: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eth0
- Ethernet II, Src: 12:fa:87:93:7e:31 (12:fa:87:93:7e:31), Dst: 12:a9:0b:b5:bd:25 (12:a9:0b:b5:bd:25)
- Internet Protocol Version 4, Src: 10.1.165.39, Dst: 10.1.161.211
- Transmission Control Protocol, Src Port: 502, Dst Port: 57648, Seq: 1, Ack: 1, Len: 12
- Modbus/TCP**
 - Transaction Identifier: 64751
 - Protocol Identifier: 0
 - Length: 7
 - Unit Identifier: 255
- Modbus

The value of this modbus protocol is:

Transaction Identifier: 64751

Protocol Identified: 0

Length: 7

Unit Identifier: 255

- b. Is Modbus using TCP or UDP? What port number is used? Attach a screenshot to support your answer.

```
Transmission Control Protocol, Src Port: 57648, Dst Port: 502,  
Source Port: 57648  
Destination Port: 502
```

The source port is 57648 and Destination port is 502. Modbus uses TCP.

```
Transmission Control Protocol, Src Port: 502, Dst Port: 57648  
Source Port: 502  
Destination Port: 57648
```

The source port is 502 and destination port is 57648. Modbus uses TCP.

5. Answer the following question:
- a. What ports are opened on **terminal.example.com**?

Port 22 and Port 502

- b. What service are provided on these opened ports?

SSH and mbap Service

Then, attach a screenshot that shows your `nmap` scan command and result. The screenshot must include:

- c. The command you have typed.
- d. The complete scan result, displaying all the open ports identified on **terminal.example.com**.

```
student@desktop:~$ nmap -p- 10.1.165.39  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-19 04:03 UTC  
Nmap scan report for ip-10-1-165-39.ec2.internal (10.1.165.39)  
Host is up (0.0083s latency).  
Not shown: 65533 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
502/tcp    open  mbap
```

6. Answer the following question:

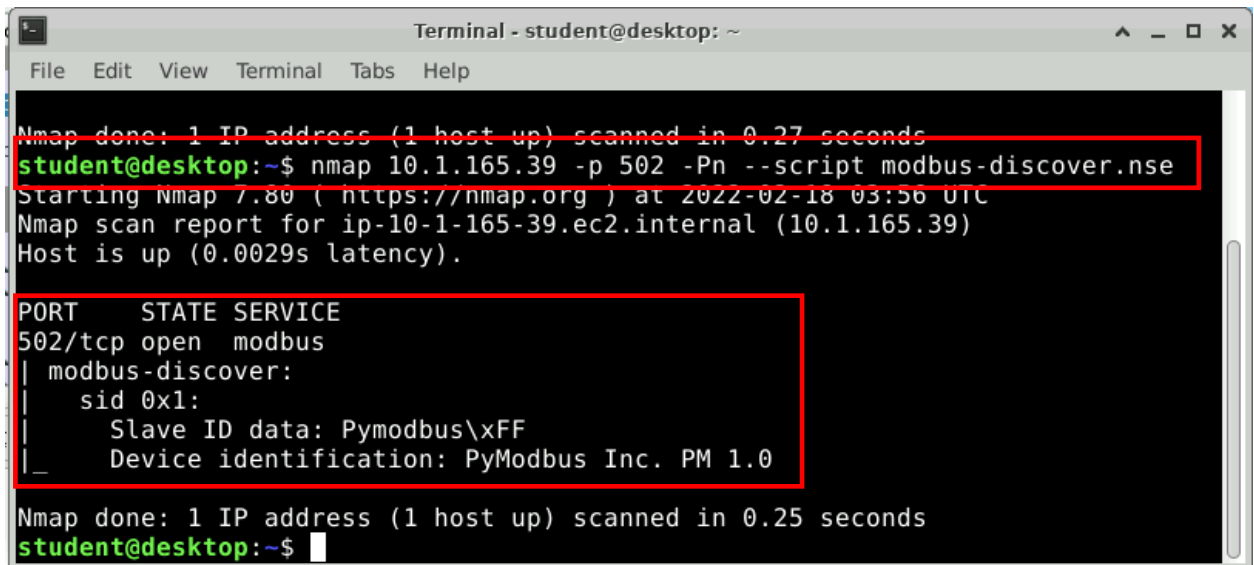
a. What is the Slave ID of the server?

Pymodbus\xFF

b. What is the Device Identification of the server?

Pymodbus Inc. PM 1.0

Then, attach a screenshot of the scan result using the `--script` option, which much include the command you have typed, and the complete scan result.



```
Terminal - student@desktop: ~
File Edit View Terminal Tabs Help

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
student@desktop:~$ nmap 10.1.165.39 -p 502 -Pn --script modbus-discover.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-18 03:56 UTC
Nmap scan report for ip-10-1-165-39.ec2.internal (10.1.165.39)
Host is up (0.0029s latency).

PORT      STATE SERVICE
502/tcp   open  modbus
| modbus-discover:
|   sid 0x1:
|   Slave ID data: Pymodbus\xFF
|_  Device identification: PyModbus Inc. PM 1.0

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
student@desktop:~$
```