6.1

Node	IP Address	MAC Address
1	10.0.2.1	52:54:00:12:35:00
2	10.0.2.2	52:54:00:12:35:00
3	10.0.2.3	08:00:27:93:DC:8B
4	10.0.2.4	08:00:27:9E:E1:A4
5	10.0.2.15	08:00:27:30:6E:C0
6	10.0.2.5	N/A

6.2

Node	IP	MAC	Port	Service
1	10.0.2.1	52:54:00:12:35:00	N/A	N/A
2	10.0.2.2	52:54:00:12:35:00	135/tcp	msrpc
3	10.0.2.2	52:54:00:12:35:00	445/tcp	Microsoft-ds
4	10.0.2.2	52:54:00:12:35:00	2343/tcp	Nati-logos
5	10.0.2.2	52:54:00:12:35:00	8000/tcp	http-alt
6	10.0.2.3	08:00:27:93:DC:8B	N/A	N/A
7	10.0.2.4	08:00:27:9E:E1:A4	8009/tcp	Ajp13
8	10.0.2.4	08:00:27:9E:E1:A4	8080/tcp	http-proxy
9	10.0.2.4	08:00:27:9E:E1:A4	9090/tcp	Zeus-admin
10	10.0.2.15	08:00:27:30:6E:C0	502/tcp	Mbap
11	10.0.2.15	08:00:27:30:6E:C0	8080/tcp	http-proxy

6.3

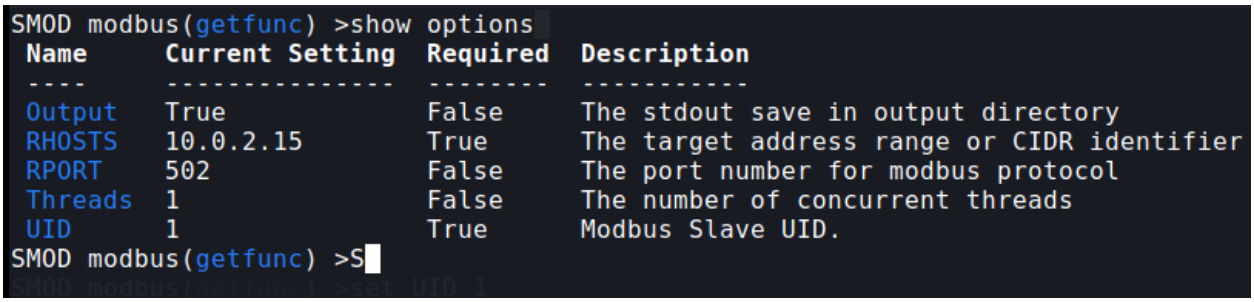
Read coils, read discrete outputs, read holding registers, read input registers, write single coil, write single holding register, write multiple coils, write multiple holding registers.

6.4

No. The purpose of a recon attack is to simply gather information. While it is certainly possible to change the values of registers and coils, this does not entail a recon attack.

6.5

The values that were read from SMOD were the same as the values that were read from the HMI. SMOD functions similarly to Metasploit. It is specific to exploiting Modbus protocol. You first give SMOD a function to execute, and then you supply options. The IP that I used for the exercise is shown in the screenshot below.



To view the coils, I could supply RHOSTS to be 10.0.2.15, UID to be 1, STARTADDR to be 0x0000, and quantity to be 0x0001.

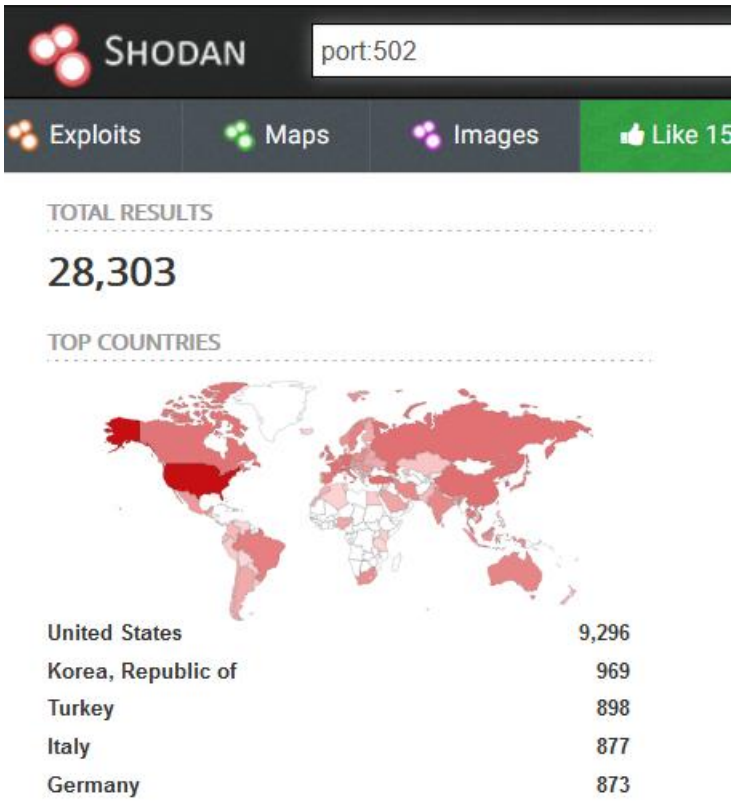
To view the holding registers, , I could supply RHOSTS to be 10.0.2.15, UID to be 1, STARTADDR to be 0x0400, and quantity to be 0x0006.

The readCoil answer will only provide an answer for bit 1, 2, or 4 since only one light can be on at once.

The readHoldingRedister function will return an array. It will be [0, red_count_ns, yellow_count_ns, 0, green_count_ns, 0, red_count_ew, 0, yellow_count_ew, 0, green_count_ew].

6.6

I found 28,303 Modbus ports.



6.7

I found 336 ports. It is unlikely that these are used for SCADA because security personnel will have most likely made sure that this port is not discoverable from the internet.