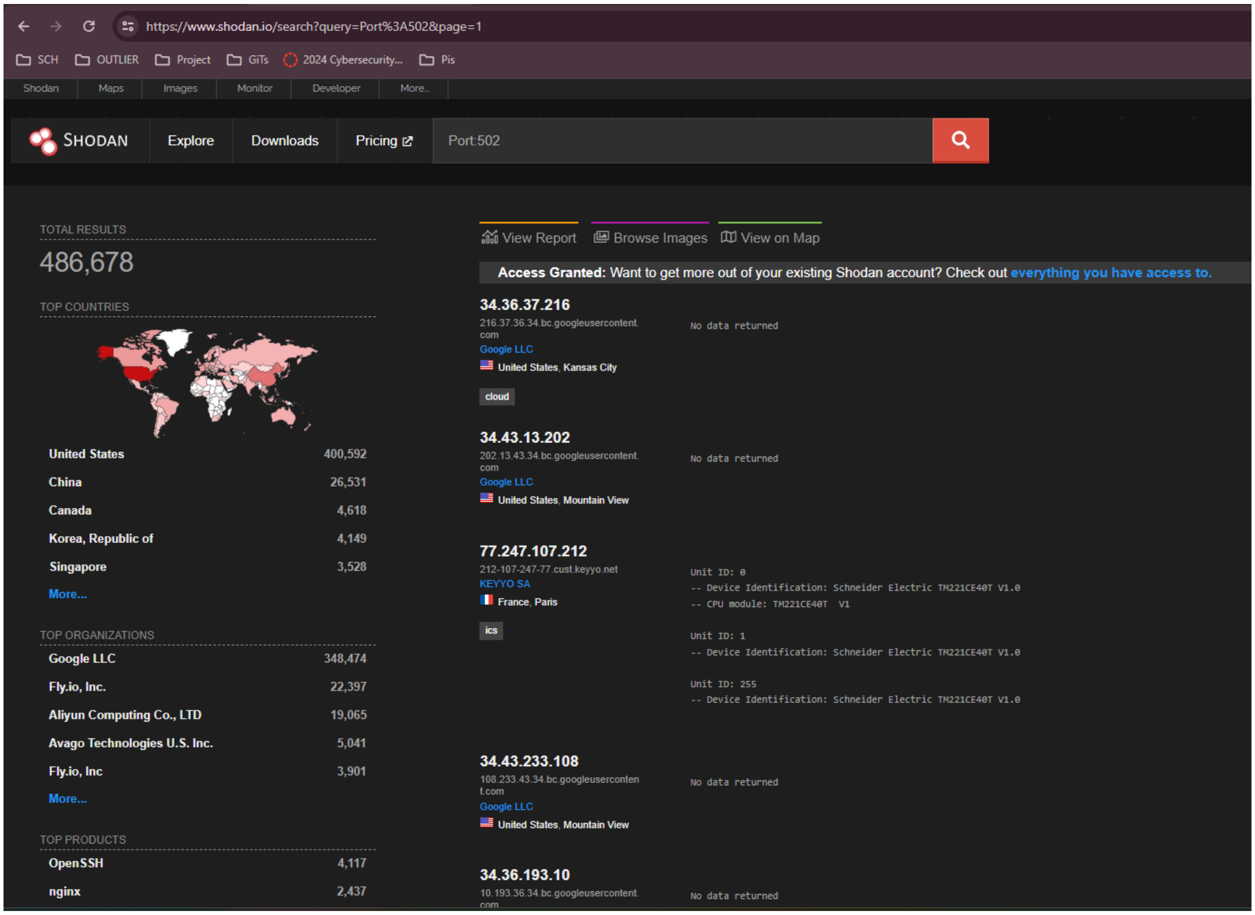
Dan Otieno
CPE 459
Spring 2024.

LAB REPORT – RECONNAISANCE.



https://www.shodan.io/search?query=Port%3A502&page=1

TOTAL RESULTS

486,678

TOP COUNTRIES

United States	400,592
China	26,531
Canada	4,618
Korea, Republic of	4,149
Singapore	3,528

More...

TOP ORGANIZATIONS

Google LLC	348,474
Fly.io, Inc.	22,397
Aliyun Computing Co., LTD	19,065
Avago Technologies U.S. Inc.	5,041
Fly.io, Inc	3,901

More...

TOP PRODUCTS

OpenSSH	4,117
nginx	2,437

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

34.36.37.216
216.37.36.34.bc.googleusercontent.com
Google LLC
United States, Kansas City
cloud

```
No data returned
```

34.43.13.202
202.13.43.34.bc.googleusercontent.com
Google LLC
United States, Mountain View

```
No data returned
```

77.247.107.212
212-107-247-77.cust.keyyo.net
KEYYO SA
France, Paris
ics

```
Unit ID: 0
-- Device Identification: Schneider Electric TM221CE40T V1.0
-- CPU module: TM221CE40T  V1

Unit ID: 1
-- Device Identification: Schneider Electric TM221CE40T V1.0

Unit ID: 255
-- Device Identification: Schneider Electric TM221CE40T V1.0
```

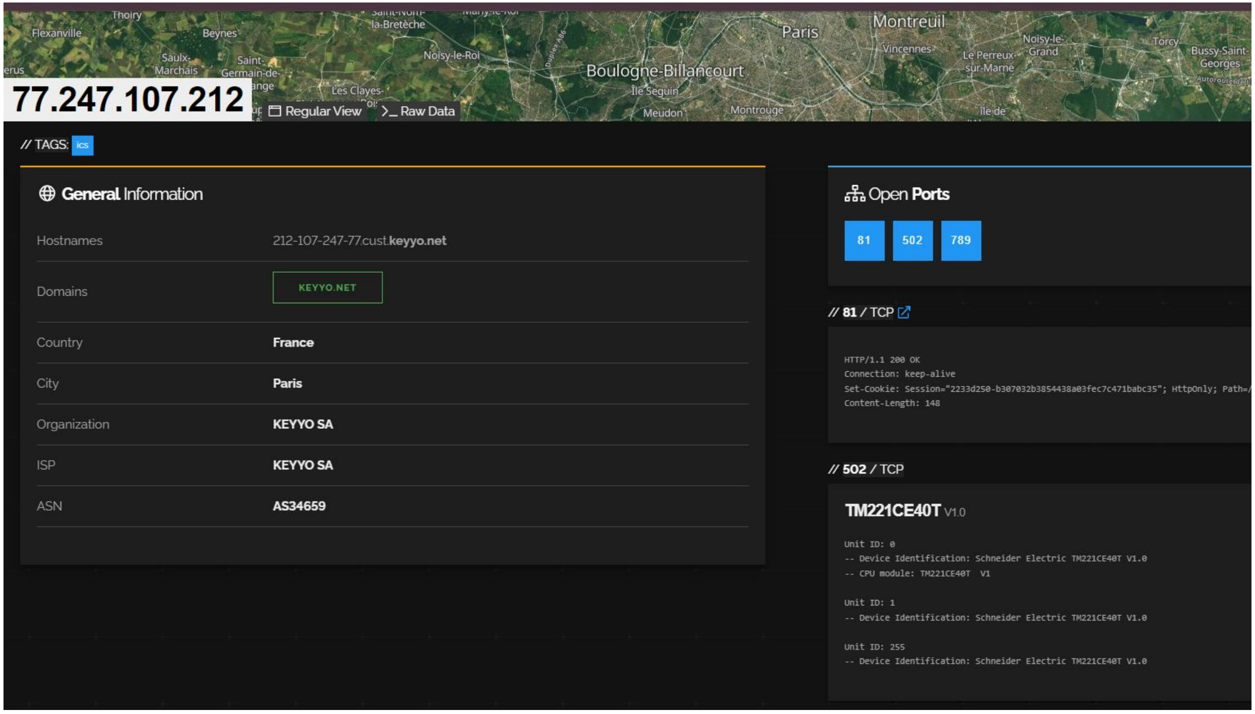
34.43.233.108
108.233.43.34.bc.googleusercontent.com
Google LLC
United States, Mountain View

```
No data returned
```

34.36.193.10
10.193.36.34.bc.googleusercontent.com

```
No data returned
```

Dan Otieno
CPE 459
Spring 2024.



77.247.107.212

General Information

Hostnames	212-107-247-77.cust.keyyo.net
Domains	KEYYO.NET
Country	France
City	Paris
Organization	KEYYO SA
ISP	KEYYO SA
ASN	AS34659

Open Ports

81 502 789

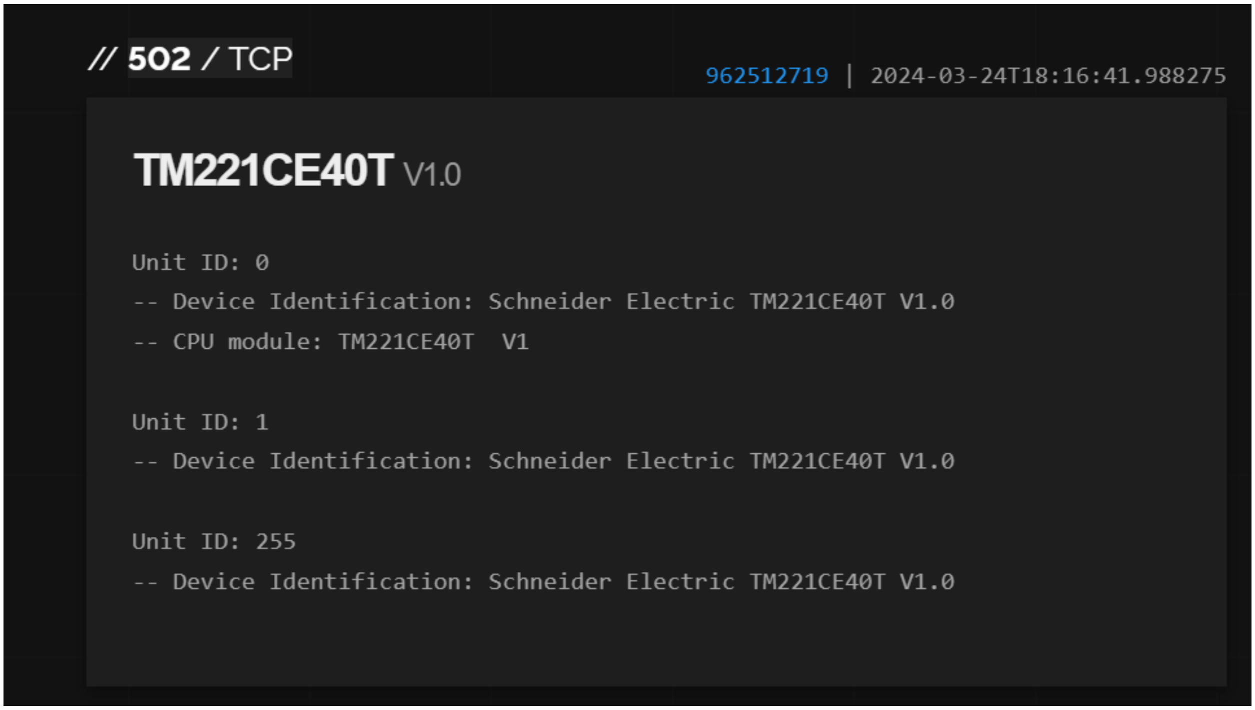
// 81 / TCP

```
HTTP/1.1 200 OK
Connection: keep-alive
Set-Cookie: Session="2233d250-b307032b3854438a03fec7c471babc35"; HttpOnly; Path=/
Content-Length: 148
```

// 502 / TCP

TM221CE40T V1.0

```
Unit ID: 0
-- Device Identification: Schneider Electric TM221CE40T V1.0
-- CPU module: TM221CE40T  V1

Unit ID: 1
-- Device Identification: Schneider Electric TM221CE40T V1.0

Unit ID: 255
-- Device Identification: Schneider Electric TM221CE40T V1.0
```



// 502 / TCP

962512719 | 2024-03-24T18:16:41.988275

TM221CE40T V1.0

```
Unit ID: 0
-- Device Identification: Schneider Electric TM221CE40T V1.0
-- CPU module: TM221CE40T  V1

Unit ID: 1
-- Device Identification: Schneider Electric TM221CE40T V1.0

Unit ID: 255
-- Device Identification: Schneider Electric TM221CE40T V1.0
```

IP address: 77.247.107.212.

Product: TM221CE40T.

Manufacturer: Schneider Electric.

Country the system is based in: France.

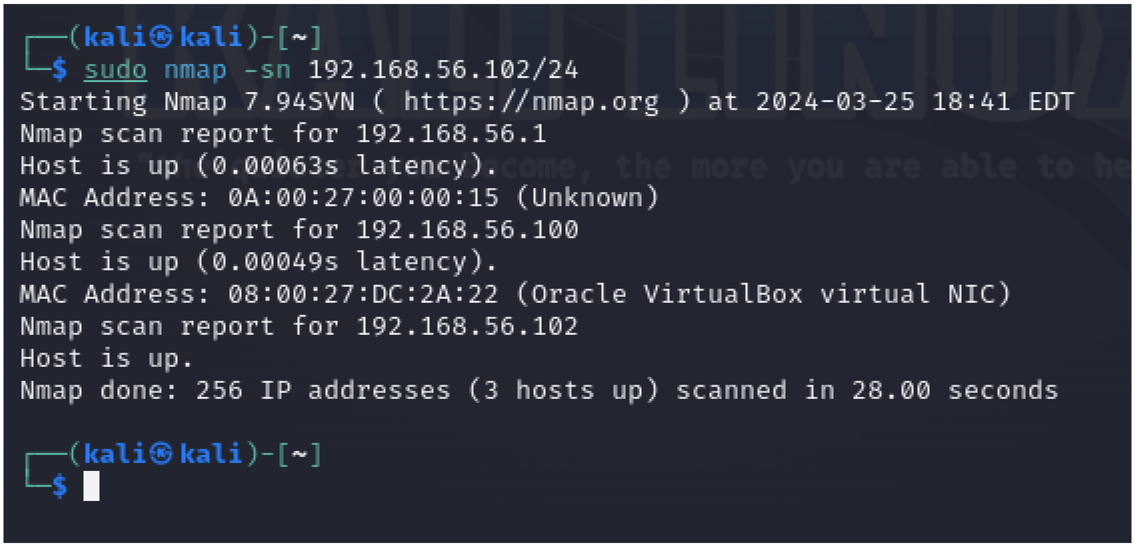
Dan Otieno
CPE 459
Spring 2024.

Organization it is part of: Keyyo SA.

Type of device: Logic Controller - Click Here for Product description from Manufacturer Website.

What they are typically used for: This is a PLC device, used for automation in cyber physical systems, or rather, in a SCADA architecture. It provides a link between physical infrastructure and an HMI for industrial control. The Organization listed here (https://www.keyyo.com/fr/) is a large telecommunications company based in France, providing phone and internet services, and therefore maintains physical infrastructure comprised of cables, servers, routers, network switches, wireless towers, among other necessary components required to deliver those services to an entire country.

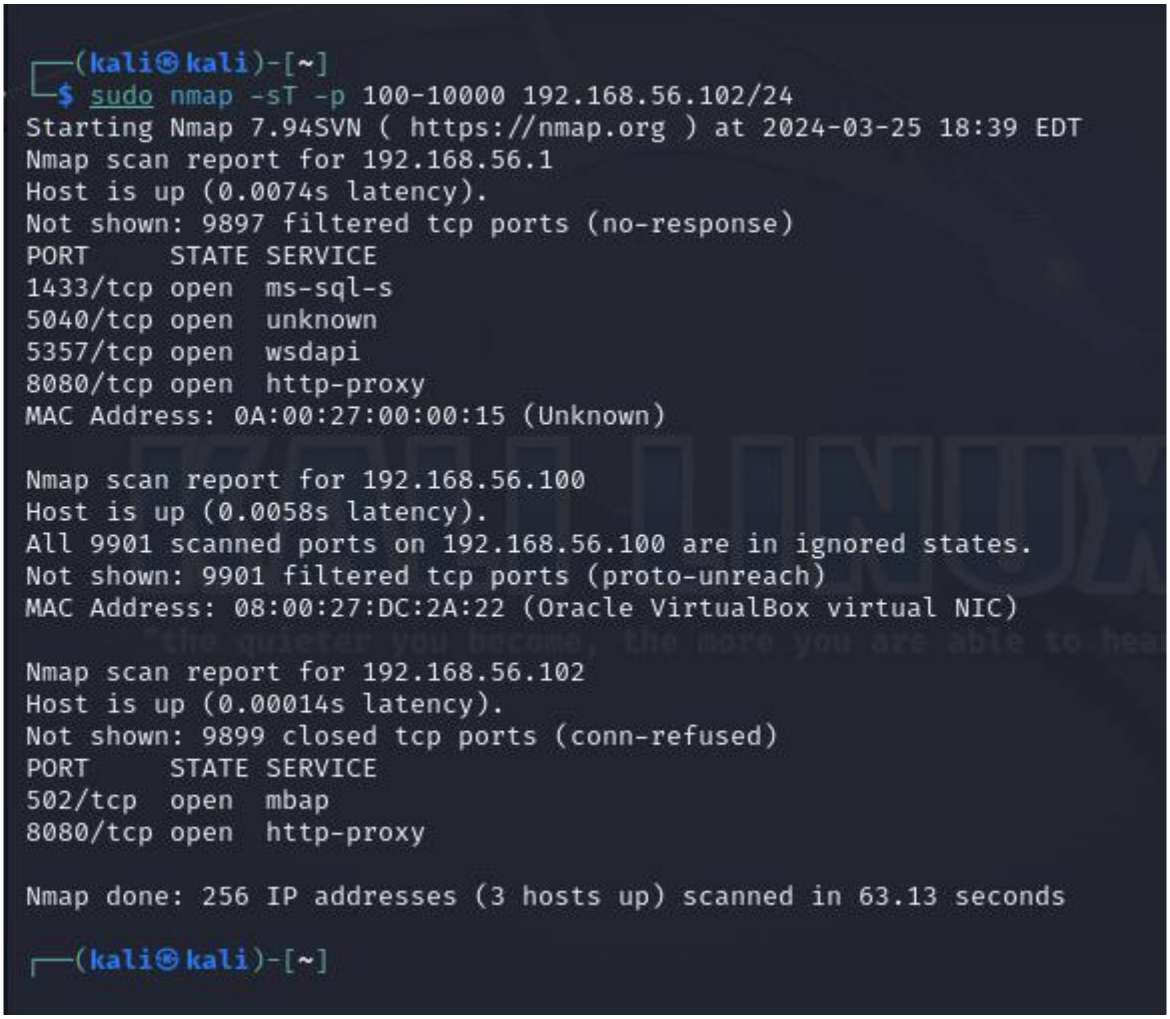
3.2



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.102/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-25 18:41 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00063s latency).
MAC Address: 0A:00:27:00:00:15 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00049s latency).
MAC Address: 08:00:27:DC:2A:22 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 28.00 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Dan Otieno
CPE 459
Spring 2024.

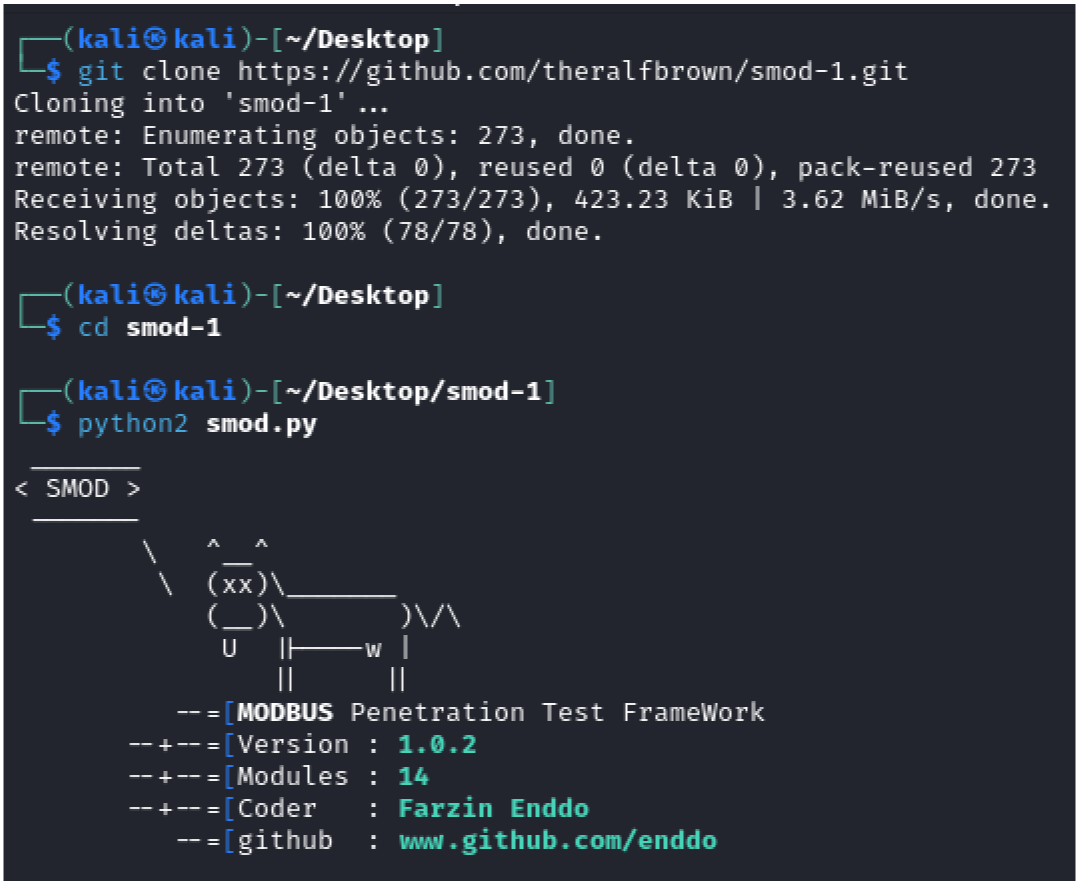
3.3



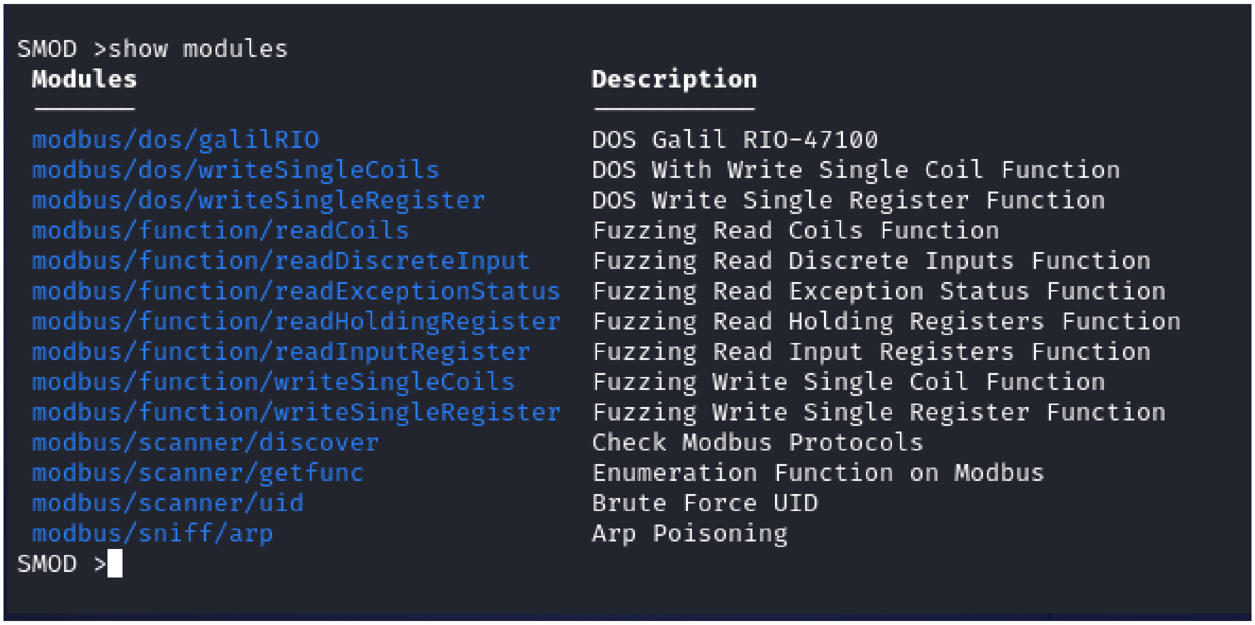
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p 100-10000 192.168.56.102/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-25 18:39 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0074s latency).
Not shown: 9897 filtered tcp ports (no-response)
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
5040/tcp open  unknown
5357/tcp open  wsdapi
8080/tcp open  http-proxy
MAC Address: 0A:00:27:00:00:15 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.0058s latency).
All 9901 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 9901 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:DC:2A:22 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00014s latency).
Not shown: 9899 closed tcp ports (conn-refused)
PORT     STATE SERVICE
502/tcp  open  mbap
8080/tcp open  http-proxy

Nmap done: 256 IP addresses (3 hosts up) scanned in 63.13 seconds

┌──(kali㉿kali)-[~]
```

Dan Otieno
CPE 459
Spring 2024.

3.4



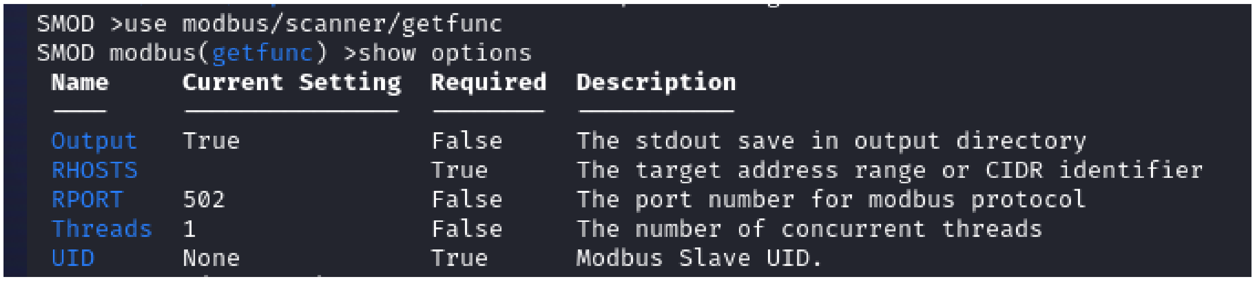
```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/theralfbrown/smod-1.git
Cloning into 'smod-1'...
remote: Enumerating objects: 273, done.
remote: Total 273 (delta 0), reused 0 (delta 0), pack-reused 273
Receiving objects: 100% (273/273), 423.23 KiB | 3.62 MiB/s, done.
Resolving deltas: 100% (78/78), done.

┌──(kali㉿kali)-[~/Desktop]
└─$ cd smod-1

┌──(kali㉿kali)-[~/Desktop/smod-1]
└─$ python2 smod.py
 ______
< SMOD >
 ------
          \   ^__^
           \  (xx)\_______
              (__)\       )\/\
               U  ||----w |
                  ||     ||
           --=[MODBUS Penetration Test FrameWork
        --+--=[Version : 1.0.2
        --+--=[Modules : 14
        --+--=[Coder   : Farzin Enddo
           --=[github  : www.github.com/enddo
```



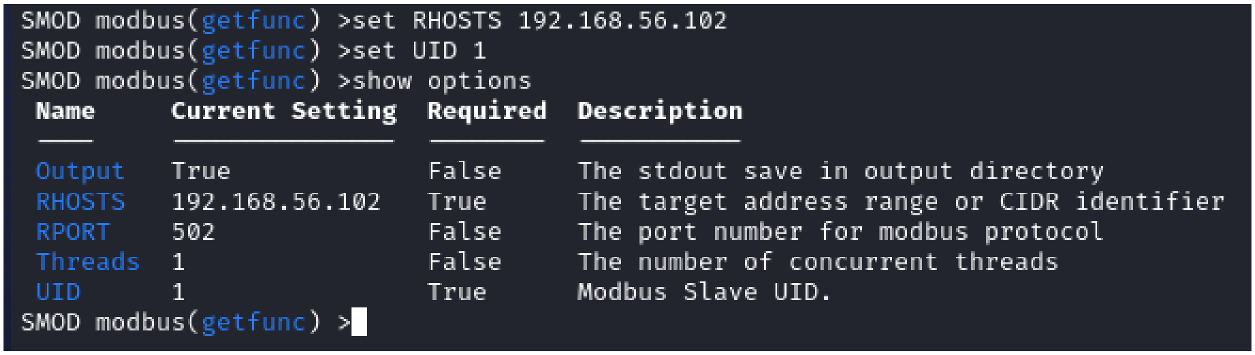
```
SMOD >show modules
 Modules                                   Description
 -------                                   -----------
 modbus/dos/galilRIO                       DOS Galil RIO-47100
 modbus/dos/writeSingleCoils               DOS With Write Single Coil Function
 modbus/dos/writeSingleRegister            DOS Write Single Register Function
 modbus/function/readCoils                 Fuzzing Read Coils Function
 modbus/function/readDiscreteInput         Fuzzing Read Discrete Inputs Function
 modbus/function/readExceptionStatus       Fuzzing Read Exception Status Function
 modbus/function/readHoldingRegister       Fuzzing Read Holding Registers Function
 modbus/function/readInputRegister         Fuzzing Read Input Registers Function
 modbus/function/writeSingleCoils          Fuzzing Write Single Coil Function
 modbus/function/writeSingleRegister       Fuzzing Write Single Register Function
 modbus/scanner/discover                   Check Modbus Protocols
 modbus/scanner/getfunc                    Enumeration Function on Modbus
 modbus/scanner/uid                        Brute Force UID
 modbus/sniff/arp                          Arp Poisoning
SMOD >
```

Dan Otieno
CPE 459
Spring 2024.

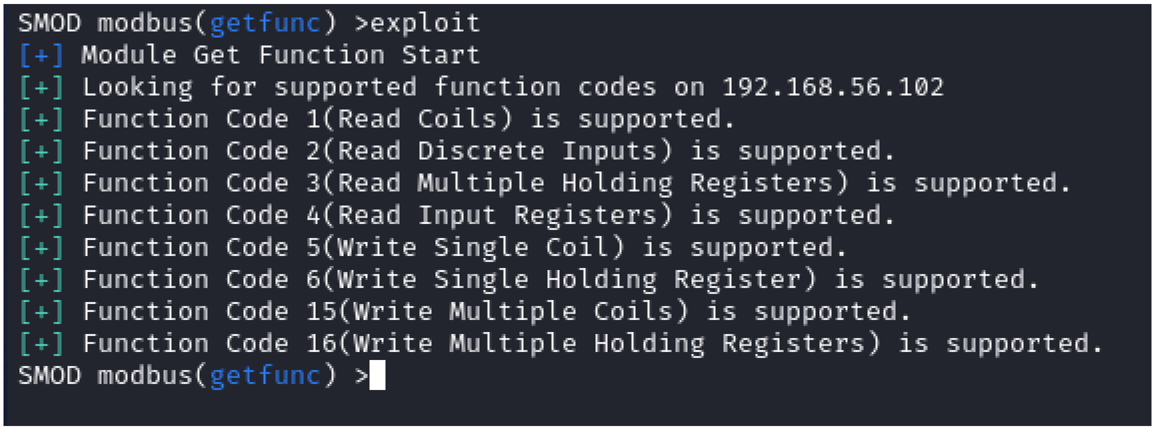
3.5



```
SMOD >use modbus/scanner/getfunc
SMOD modbus(getfunc) >show options
 Name      Current Setting  Required  Description
 ----      ---------------  --------  -----------

 Output    True             False     The stdout save in output directory
 RHOSTS                     True      The target address range or CIDR identifier
 RPORT     502              False     The port number for modbus protocol
 Threads   1                False     The number of concurrent threads
 UID       None             True      Modbus Slave UID.
```



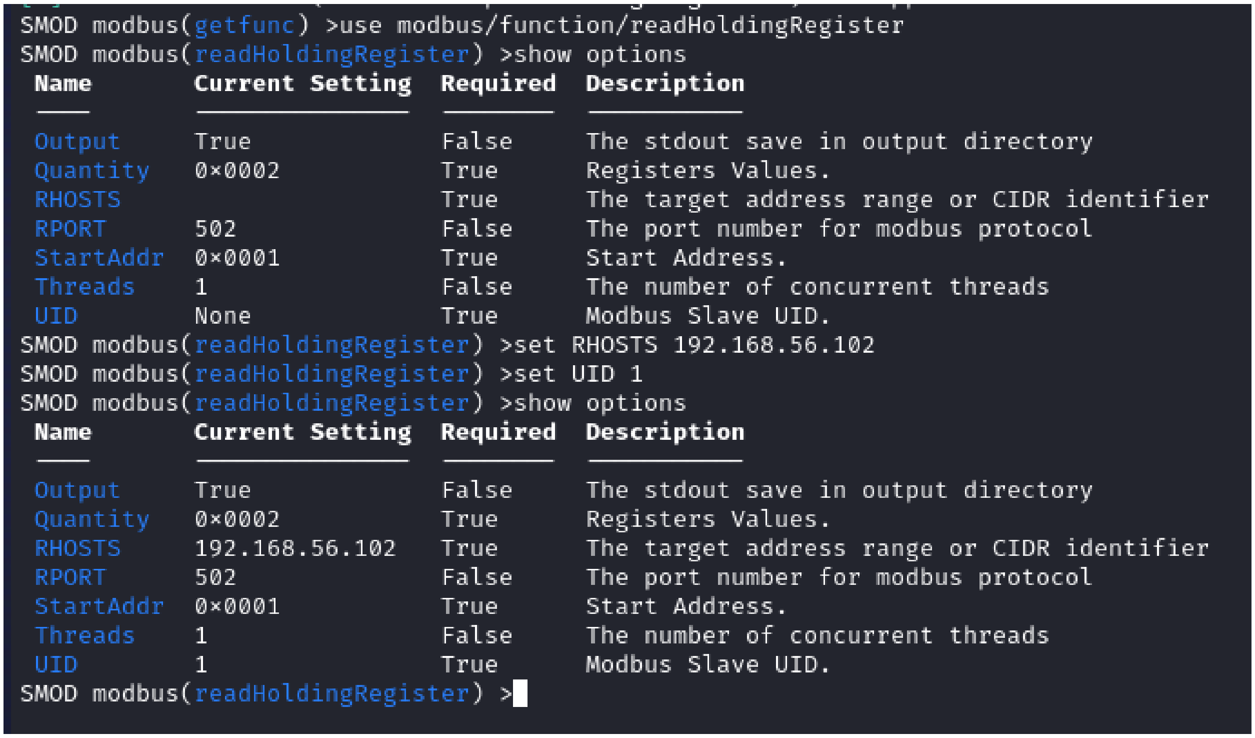
```
SMOD modbus(getfunc) >set RHOSTS 192.168.56.102
SMOD modbus(getfunc) >set UID 1
SMOD modbus(getfunc) >show options
 Name      Current Setting  Required  Description
 ----      ---------------  --------  -----------

 Output    True             False     The stdout save in output directory
 RHOSTS    192.168.56.102   True      The target address range or CIDR identifier
 RPORT     502              False     The port number for modbus protocol
 Threads   1                False     The number of concurrent threads
 UID       1                True      Modbus Slave UID.
SMOD modbus(getfunc) >
```



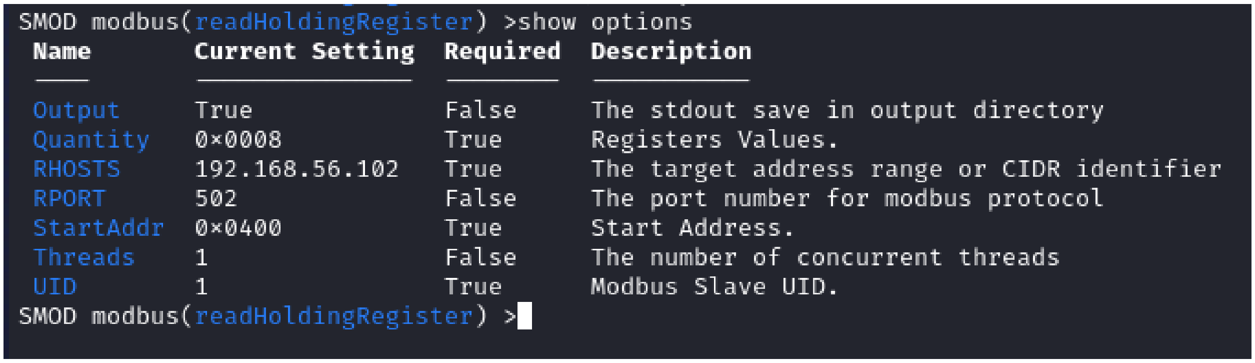
```
SMOD modbus(getfunc) >exploit
[+] Module Get Function Start
[+] Looking for supported function codes on 192.168.56.102
[+] Function Code 1(Read Coils) is supported.
[+] Function Code 2(Read Discrete Inputs) is supported.
[+] Function Code 3(Read Multiple Holding Registers) is supported.
[+] Function Code 4(Read Input Registers) is supported.
[+] Function Code 5(Write Single Coil) is supported.
[+] Function Code 6(Write Single Holding Register) is supported.
[+] Function Code 15(Write Multiple Coils) is supported.
[+] Function Code 16(Write Multiple Holding Registers) is supported.
SMOD modbus(getfunc) >
```

Dan Otieno
CPE 459
Spring 2024.

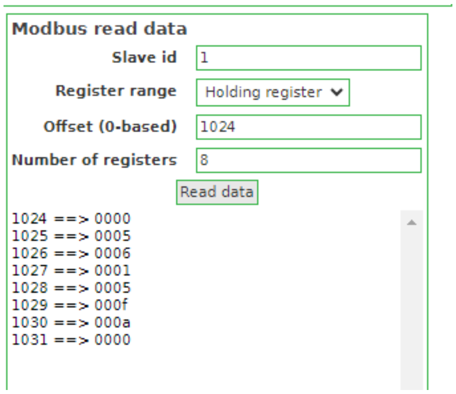
3.6



```
SMOD modbus(getfunc) >use modbus/function/readHoldingRegister
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x0002           True      Registers Values.
 RHOSTS                       True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         None             True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >set RHOSTS 192.168.56.102
SMOD modbus(readHoldingRegister) >set UID 1
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x0002           True      Registers Values.
 RHOSTS      192.168.56.102   True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >
```



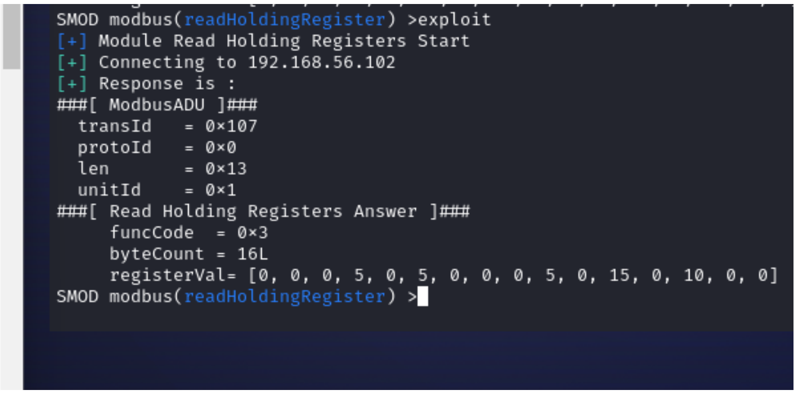
```
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x0008           True      Registers Values.
 RHOSTS      192.168.56.102   True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0400           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >
```



Modbus read data

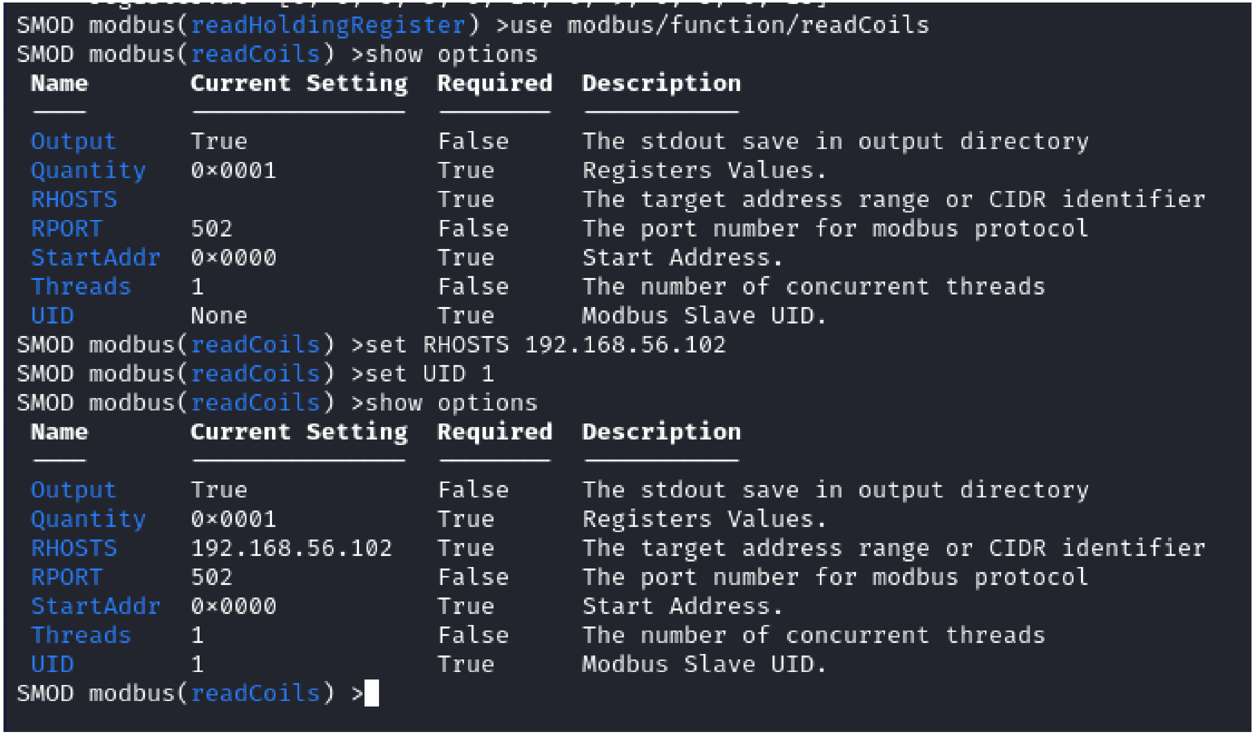
Slave id	1
Register range	Holding register
Offset (0-based)	1024
Number of registers	8

```
1024 ==> 0000
1025 ==> 0005
1026 ==> 0006
1027 ==> 0001
1028 ==> 0005
1029 ==> 000f
1030 ==> 000a
1031 ==> 0000
```

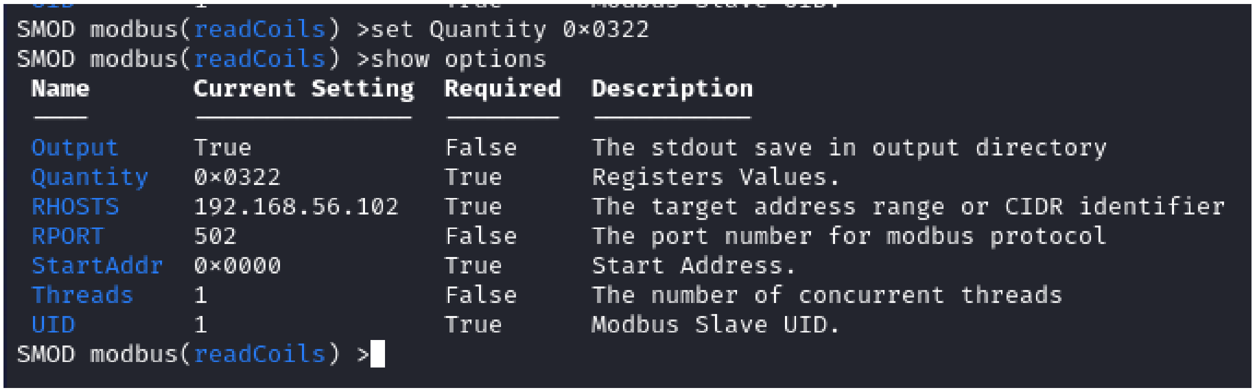


```
SMOD modbus(readHoldingRegister) >exploit
[+] Module Read Holding Registers Start
[+] Connecting to 192.168.56.102
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x107
  protoId   = 0x0
  len       = 0x13
  unitId    = 0x1
###[ Read Holding Registers Answer ]###
     funcCode  = 0x3
     byteCount = 16L
     registerVal= [0, 0, 0, 5, 0, 5, 0, 0, 0, 5, 0, 15, 0, 10, 0, 0]
SMOD modbus(readHoldingRegister) >
```

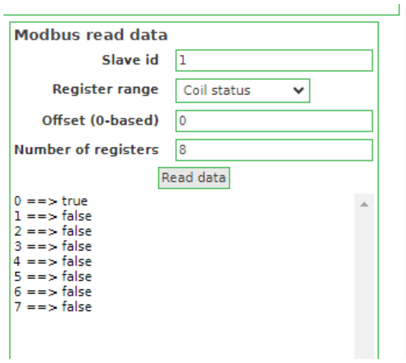
Dan Otieno
CPE 459
Spring 2024.



```
SMOD modbus(readHoldingRegister) >use modbus/function/readCoils
SMOD modbus(readCoils) >show options
 Name         Current Setting  Required  Description
 ----         ---------------  --------  -----------
 Output       True             False     The stdout save in output directory
 Quantity     0×0001           True      Registers Values.
 RHOSTS                        True      The target address range or CIDR identifier
 RPORT        502              False     The port number for modbus protocol
 StartAddr    0×0000           True      Start Address.
 Threads      1                False     The number of concurrent threads
 UID          None             True      Modbus Slave UID.
SMOD modbus(readCoils) >set RHOSTS 192.168.56.102
SMOD modbus(readCoils) >set UID 1
SMOD modbus(readCoils) >show options
 Name         Current Setting  Required  Description
 ----         ---------------  --------  -----------
 Output       True             False     The stdout save in output directory
 Quantity     0×0001           True      Registers Values.
 RHOSTS       192.168.56.102   True      The target address range or CIDR identifier
 RPORT        502              False     The port number for modbus protocol
 StartAddr    0×0000           True      Start Address.
 Threads      1                False     The number of concurrent threads
 UID          1                True      Modbus Slave UID.
SMOD modbus(readCoils) >
```



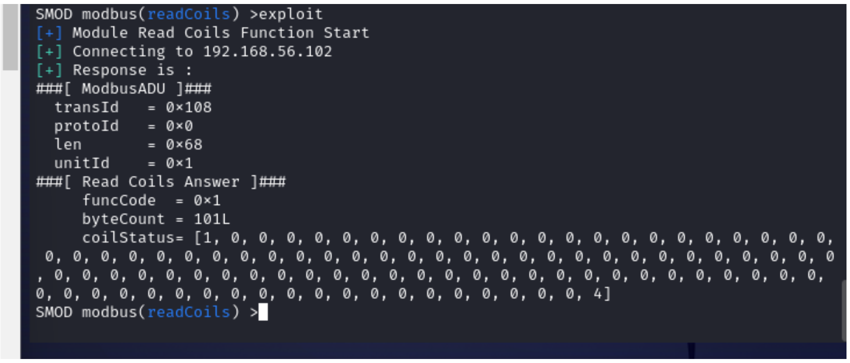
```
SMOD modbus(readCoils) >set Quantity 0×0322
SMOD modbus(readCoils) >show options
 Name         Current Setting  Required  Description
 ----         ---------------  --------  -----------
 Output       True             False     The stdout save in output directory
 Quantity     0×0322           True      Registers Values.
 RHOSTS       192.168.56.102   True      The target address range or CIDR identifier
 RPORT        502              False     The port number for modbus protocol
 StartAddr    0×0000           True      Start Address.
 Threads      1                False     The number of concurrent threads
 UID          1                True      Modbus Slave UID.
SMOD modbus(readCoils) >
```



Modbus read data

Slave id	1
Register range	Coil status
Offset (0-based)	0
Number of registers	8

```
0 ==> true
1 ==> false
2 ==> false
3 ==> false
4 ==> false
5 ==> false
6 ==> false
7 ==> false
```



```
SMOD modbus(readCoils) >exploit
[+] Module Read Coils Function Start
[+] Connecting to 192.168.56.102
[+] Response is :
###[ ModbusADU ]###
  transId   = 0×108
  protoId   = 0×0
  len       = 0×68
  unitId    = 0×1
###[ Read Coils Answer ]###
     funcCode  = 0×1
     byteCount = 101L
     coilStatus= [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4]
SMOD modbus(readCoils) >
```

Dan Otieno
CPE 459
Spring 2024.

4.

1. Using what you found in section 3.2, please fill out the table below:

IP ADDRESS	MAC ADDRESS
192.168.56.1	0A:00:27:00:00:15
192.168.56.100	08:00:27:DC:2A:22
192.168.56.102	None

2. Using what you found in section 3.3, please fill out the table below:

IP	MAC	Port(s)	Service
192.168.56.1	0A:00:27:00:00:15	1433	ms-sql-s
		5040	unknown
		5357	wsdapi
		8080	http-proxy
192.168.56.100	08:00:27:DC:2A:22	Not shown	All ports in ignored states.
192.168.56.102	None	502	mbap
		8080	http-proxy

a. What are the function codes used in your system?

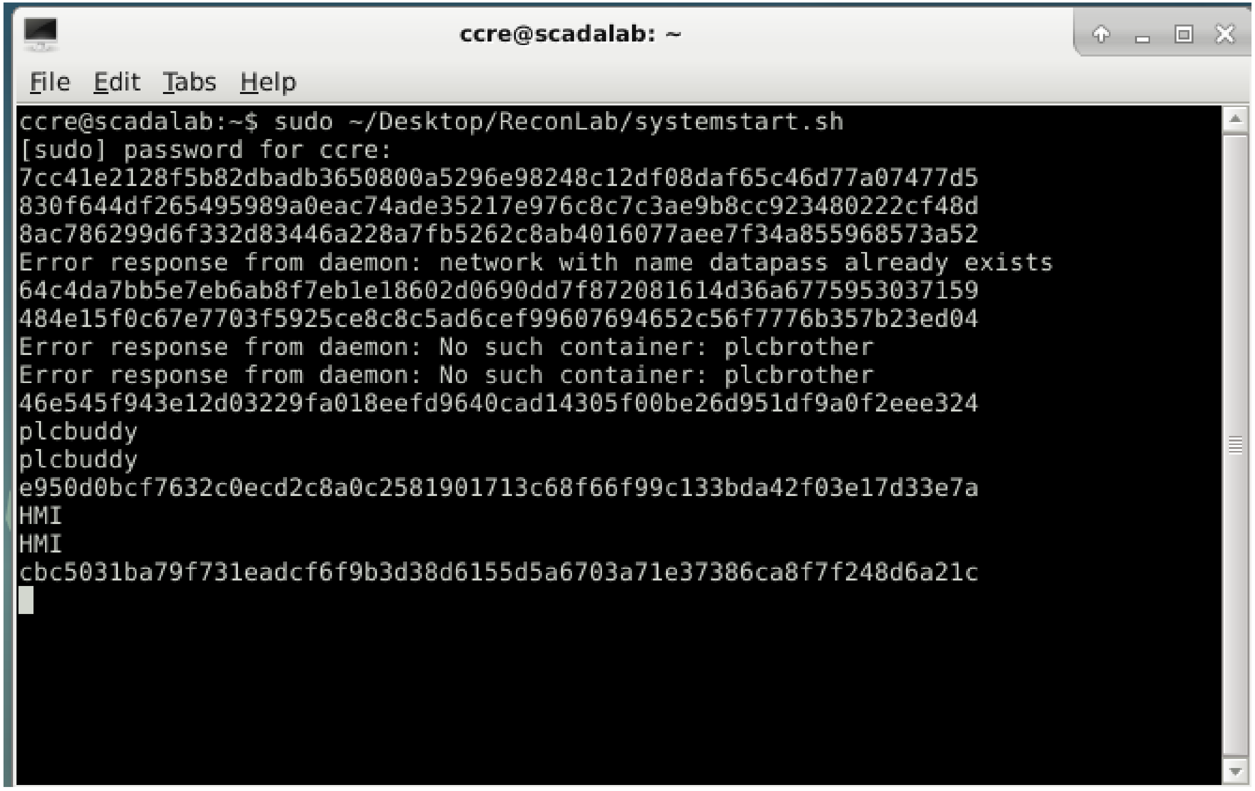
- **Function Code 1 – Read Coils.**
- **Function Code 3 – Read Multiple Holding Registers.**

b. Is it possible to create an attack to change the values of registers or coils using function codes 5 through 16? Why or why not? Explain. (10 points) HINT: Remember that the values are in decimal, but they are stored in binary/hexadecimal. **Yes, function codes 5, 6, 15 and 16 are write functions to modify the values of single and multiple coils and registers. An attacker can write data to specific coils or registers in a Modbus slave device. Modbus protocol defines data in terms of binary values (coils) or numerical values (registers), but the communication is in hexadecimal or binary form. The attacker would need to convert their decimal values to the appropriate binary or hexadecimal format before crafting the Modbus packets to manipulate the coils or registers, but once they do so, and if they gain access, they can change the values.**

c. For Section 3.6, you read the registers and coils. For each of them, compare what you see on the HMI with what you see using S-Mod. Are they the same? Why or why not? Explain. **Yes, values on the HMI match those in S-Mod, because with each test, we set the RHOSTS configuration in S-Mod to match the PLC IP address. Because SCADA reads values in HEX and S-Mod reads in decimal, to verify if they match, we take the modbus read data values that are represented in decimal and convert them to hex to compare with the output values in S-Mod.**

RECONNAISANCE ATTACK OF UNKNOWN SYSTEM.

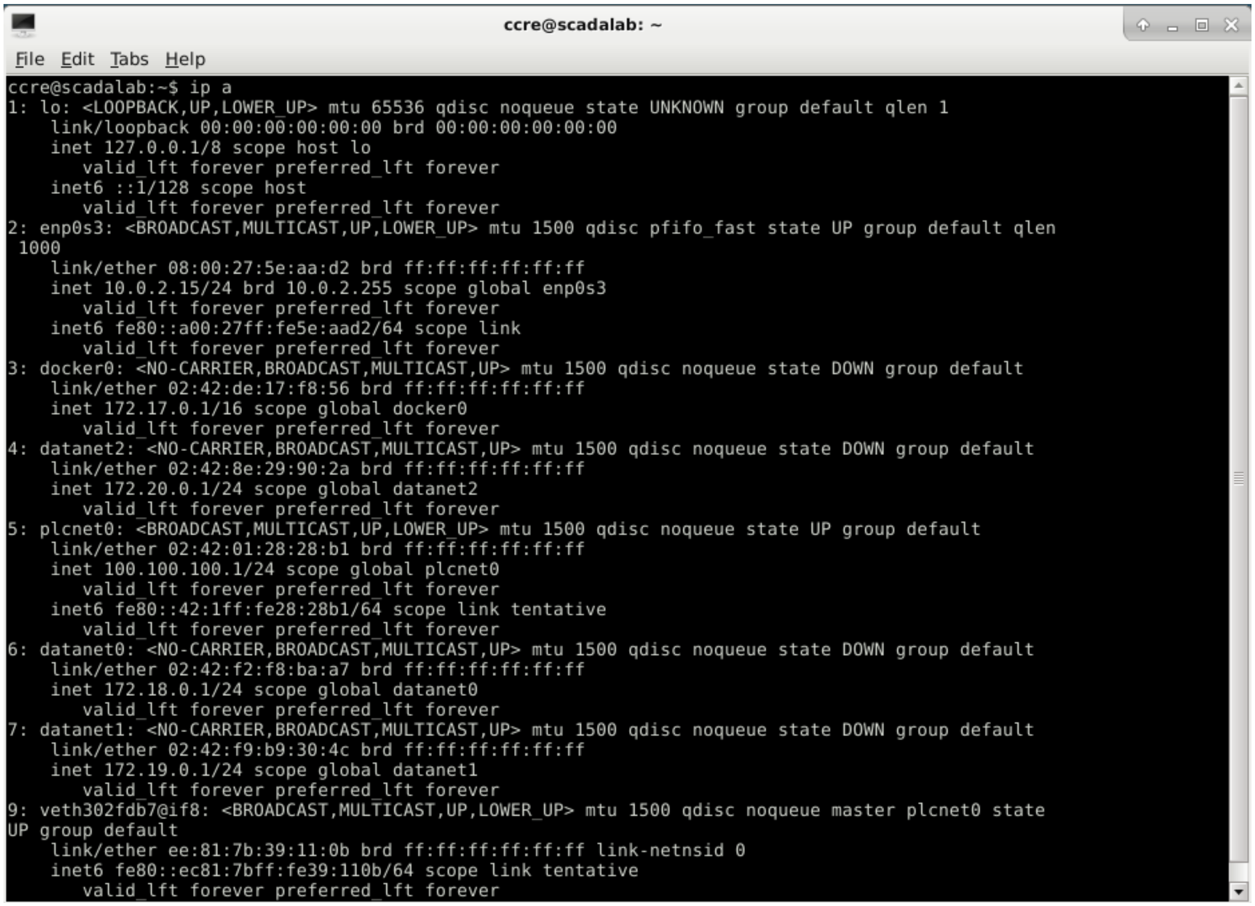
Dan Otieno
CPE 459
Spring 2024.



```
ccre@scadalab:~$ sudo ~/Desktop/ReconLab/systemstart.sh
[sudo] password for ccre:
7cc41e2128f5b82dbadb3650800a5296e98248c12df08daf65c46d77a07477d5
830f644df265495989a0eac74ade35217e976c8c7c3ae9b8cc923480222cf48d
8ac786299d6f332d83446a228a7fb5262c8ab4016077aee7f34a855968573a52
Error response from daemon: network with name datapass already exists
64c4da7bb5e7eb6ab8f7eb1e18602d0690dd7f872081614d36a6775953037159
484e15f0c67e7703f5925ce8c8c5ad6cef99607694652c56f7776b357b23ed04
Error response from daemon: No such container: plcbrother
Error response from daemon: No such container: plcbrother
46e545f943e12d03229fa018eefd9640cad14305f00be26d951df9a0f2eee324
plcbuddy
plcbuddy
e950d0bcf7632c0ecd2c8a0c2581901713c68f66f99c133bda42f03e17d33e7a
HMI
HMI
cbc5031ba79f731eadcf6f9b3d38d6155d5a6703a71e37386ca8f7f248d6a21c
```

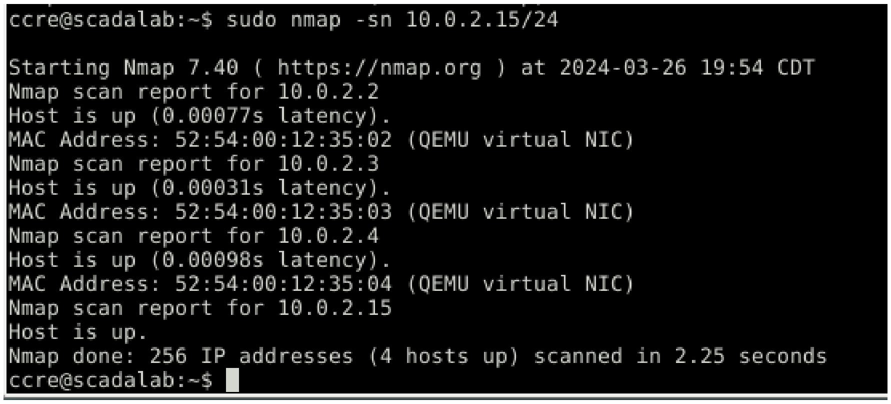
1. Identify the network(s) that the systems are running on.

Dan Otieno
CPE 459
Spring 2024.



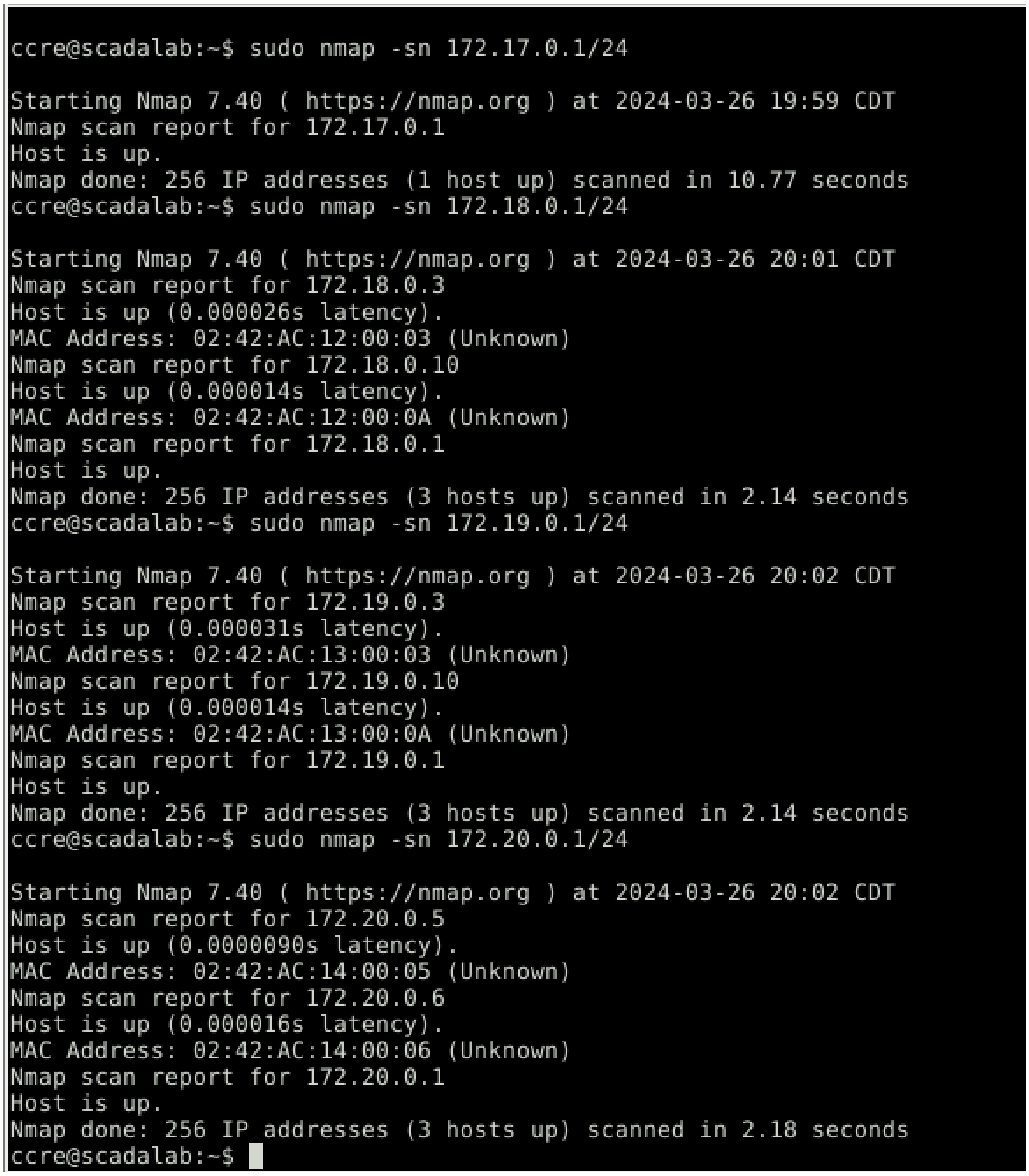
```
ccre@scadalab:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
 1000
    link/ether 08:00:27:5e:aa:d2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe5e:aad2/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:de:17:f8:56 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 scope global docker0
       valid_lft forever preferred_lft forever
4: datanet2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:8e:29:90:2a brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.1/24 scope global datanet2
       valid_lft forever preferred_lft forever
5: plcnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:01:28:28:b1 brd ff:ff:ff:ff:ff:ff
    inet 100.100.100.1/24 scope global plcnet0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:1ff:fe28:28b1/64 scope link tentative
       valid_lft forever preferred_lft forever
6: datanet0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:f2:f8:ba:a7 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/24 scope global datanet0
       valid_lft forever preferred_lft forever
7: datanet1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:f9:b9:30:4c brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.1/24 scope global datanet1
       valid_lft forever preferred_lft forever
9: veth302fdb7@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master plcnet0 state
UP group default
    link/ether ee:81:7b:39:11:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::ec81:7bff:fe39:110b/64 scope link tentative
       valid_lft forever preferred_lft forever
```

2. Find all active hosts and their IP addresses on each network(s).

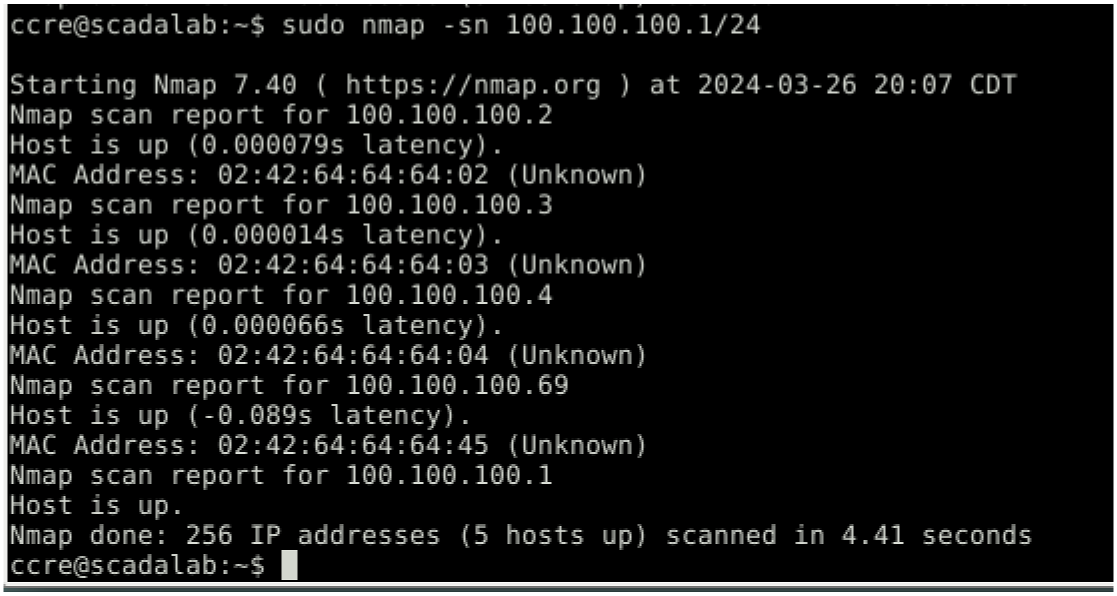


```
ccre@scadalab:~$ sudo nmap -sn 10.0.2.15/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 19:54 CDT
Nmap scan report for 10.0.2.2
Host is up (0.00077s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00031s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00098s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.25 seconds
ccre@scadalab:~$
```

Dan Otieno
CPE 459
Spring 2024.



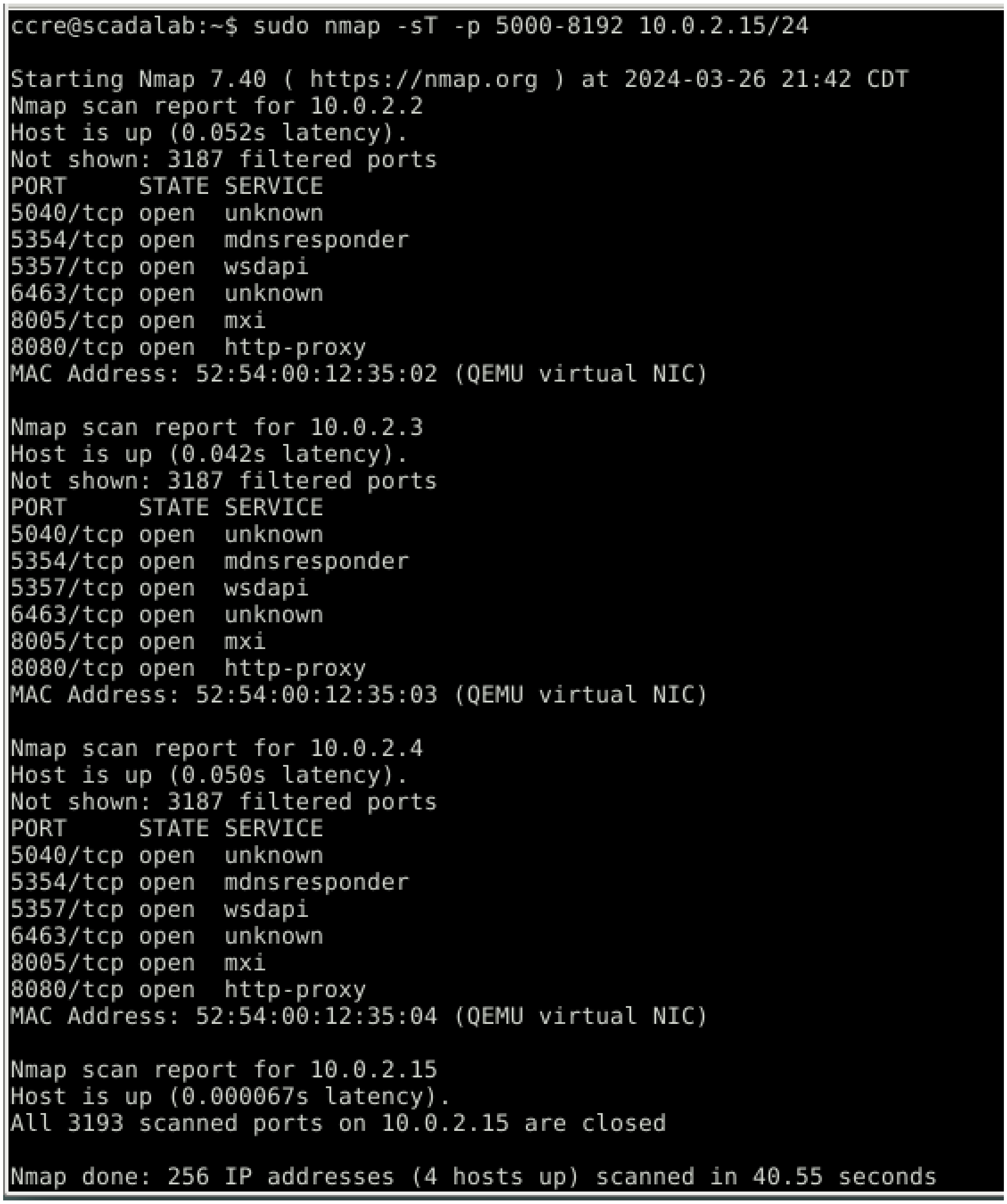
```
ccre@scadalab:~$ sudo nmap -sn 172.17.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 19:59 CDT
Nmap scan report for 172.17.0.1
Host is up.
Nmap done: 256 IP addresses (1 host up) scanned in 10.77 seconds
ccre@scadalab:~$ sudo nmap -sn 172.18.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:01 CDT
Nmap scan report for 172.18.0.3
Host is up (0.000026s latency).
MAC Address: 02:42:AC:12:00:03 (Unknown)
Nmap scan report for 172.18.0.10
Host is up (0.000014s latency).
MAC Address: 02:42:AC:12:00:0A (Unknown)
Nmap scan report for 172.18.0.1
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.14 seconds
ccre@scadalab:~$ sudo nmap -sn 172.19.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:02 CDT
Nmap scan report for 172.19.0.3
Host is up (0.000031s latency).
MAC Address: 02:42:AC:13:00:03 (Unknown)
Nmap scan report for 172.19.0.10
Host is up (0.000014s latency).
MAC Address: 02:42:AC:13:00:0A (Unknown)
Nmap scan report for 172.19.0.1
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.14 seconds
ccre@scadalab:~$ sudo nmap -sn 172.20.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:02 CDT
Nmap scan report for 172.20.0.5
Host is up (0.0000090s latency).
MAC Address: 02:42:AC:14:00:05 (Unknown)
Nmap scan report for 172.20.0.6
Host is up (0.000016s latency).
MAC Address: 02:42:AC:14:00:06 (Unknown)
Nmap scan report for 172.20.0.1
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.18 seconds
ccre@scadalab:~$
```



```
ccre@scadalab:~$ sudo nmap -sn 100.100.100.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:07 CDT
Nmap scan report for 100.100.100.2
Host is up (0.000079s latency).
MAC Address: 02:42:64:64:64:02 (Unknown)
Nmap scan report for 100.100.100.3
Host is up (0.000014s latency).
MAC Address: 02:42:64:64:64:03 (Unknown)
Nmap scan report for 100.100.100.4
Host is up (0.000066s latency).
MAC Address: 02:42:64:64:64:04 (Unknown)
Nmap scan report for 100.100.100.69
Host is up (-0.089s latency).
MAC Address: 02:42:64:64:64:45 (Unknown)
Nmap scan report for 100.100.100.1
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 4.41 seconds
ccre@scadalab:~$ 
```

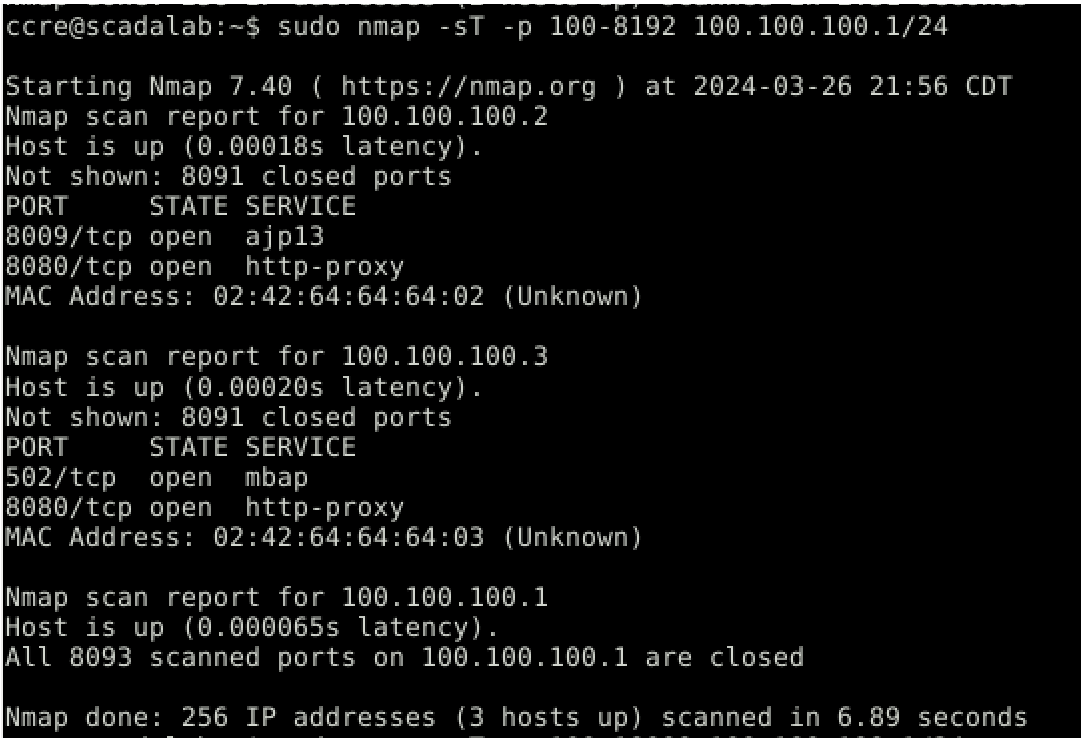
3. Find all open ports for each device you can find at each network.

Dan Otieno
CPE 459
Spring 2024.

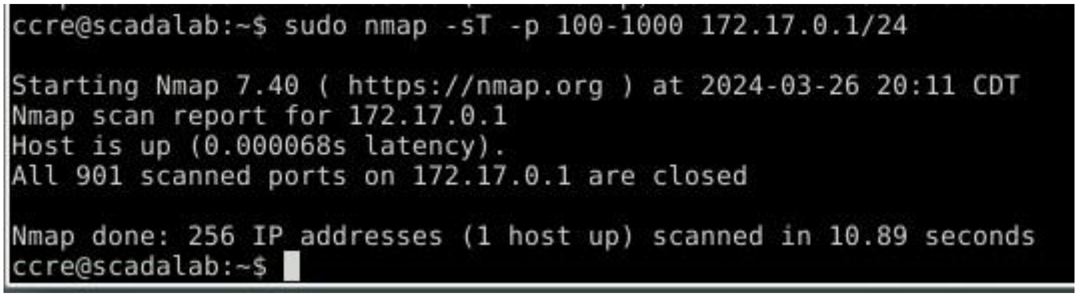


```
ccre@scadalab:~$ sudo nmap -sT -p 5000-8192 10.0.2.15/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 21:42 CDT
Nmap scan report for 10.0.2.2
Host is up (0.052s latency).
Not shown: 3187 filtered ports
PORT     STATE SERVICE
5040/tcp open  unknown
5354/tcp open  mdnsresponder
5357/tcp open  wsdapi
6463/tcp open  unknown
8005/tcp open  mxi
8080/tcp open  http-proxy
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.042s latency).
Not shown: 3187 filtered ports
PORT     STATE SERVICE
5040/tcp open  unknown
5354/tcp open  mdnsresponder
5357/tcp open  wsdapi
6463/tcp open  unknown
8005/tcp open  mxi
8080/tcp open  http-proxy
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.050s latency).
Not shown: 3187 filtered ports
PORT     STATE SERVICE
5040/tcp open  unknown
5354/tcp open  mdnsresponder
5357/tcp open  wsdapi
6463/tcp open  unknown
8005/tcp open  mxi
8080/tcp open  http-proxy
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.000067s latency).
All 3193 scanned ports on 10.0.2.15 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 40.55 seconds
```

Dan Otieno
CPE 459
Spring 2024.

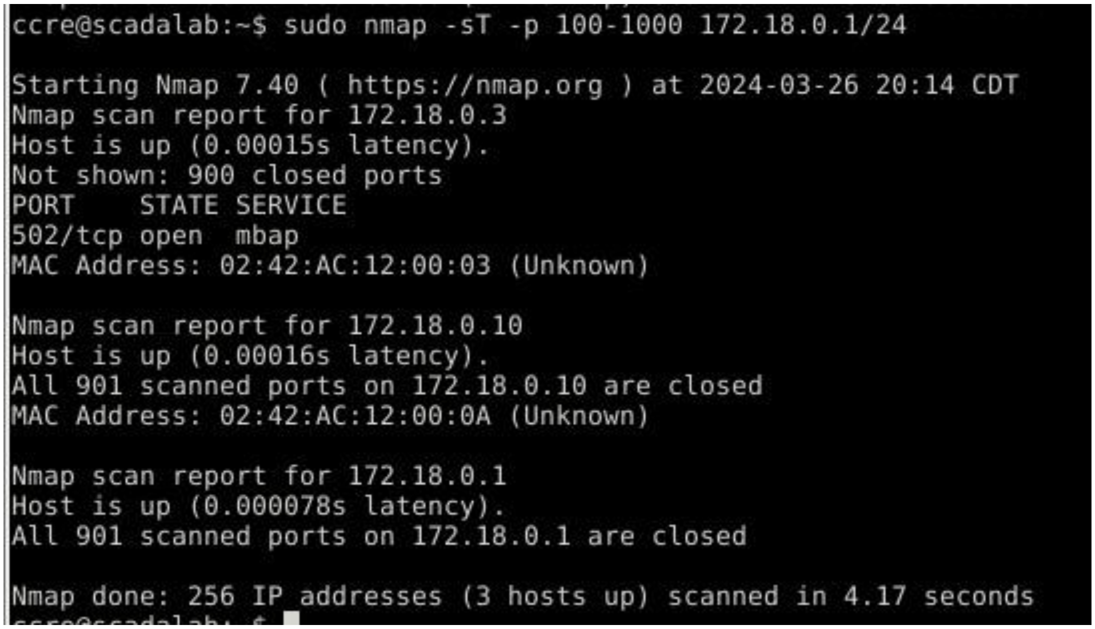


```
ccre@scadalab:~$ sudo nmap -sT -p 100-8192 100.100.100.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 21:56 CDT
Nmap scan report for 100.100.100.2
Host is up (0.00018s latency).
Not shown: 8091 closed ports
PORT     STATE SERVICE
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:42:64:64:64:02 (Unknown)

Nmap scan report for 100.100.100.3
Host is up (0.00020s latency).
Not shown: 8091 closed ports
PORT     STATE SERVICE
502/tcp  open  mbap
8080/tcp open  http-proxy
MAC Address: 02:42:64:64:64:03 (Unknown)

Nmap scan report for 100.100.100.1
Host is up (0.000065s latency).
All 8093 scanned ports on 100.100.100.1 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.89 seconds
```

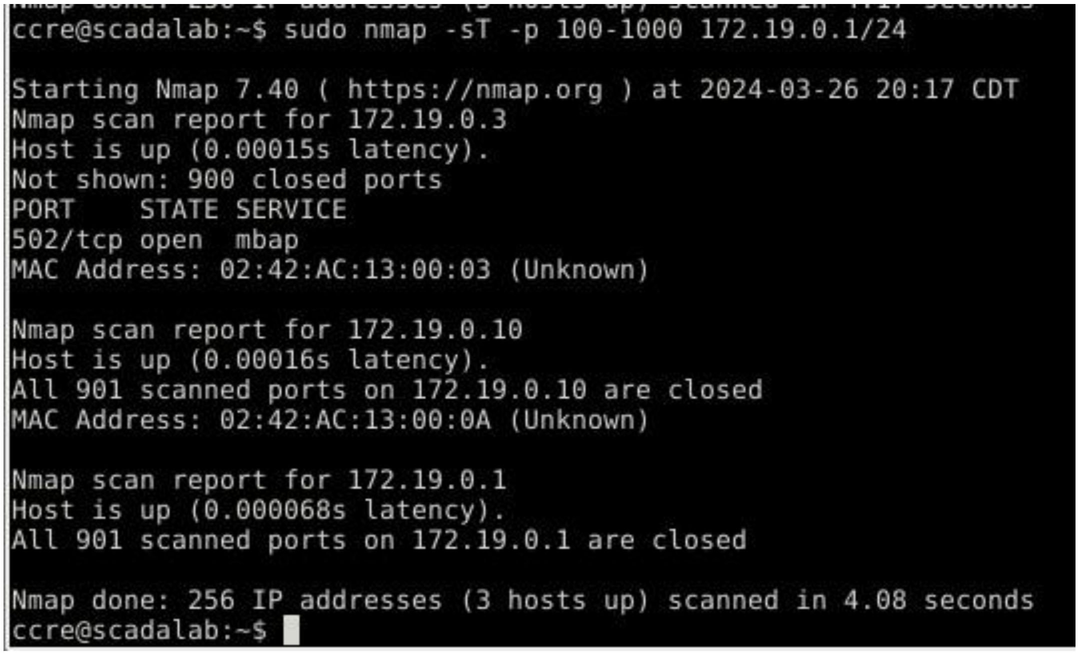


```
ccre@scadalab:~$ sudo nmap -sT -p 100-1000 172.17.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:11 CDT
Nmap scan report for 172.17.0.1
Host is up (0.000068s latency).
All 901 scanned ports on 172.17.0.1 are closed

Nmap done: 256 IP addresses (1 host up) scanned in 10.89 seconds
ccre@scadalab:~$ 
```

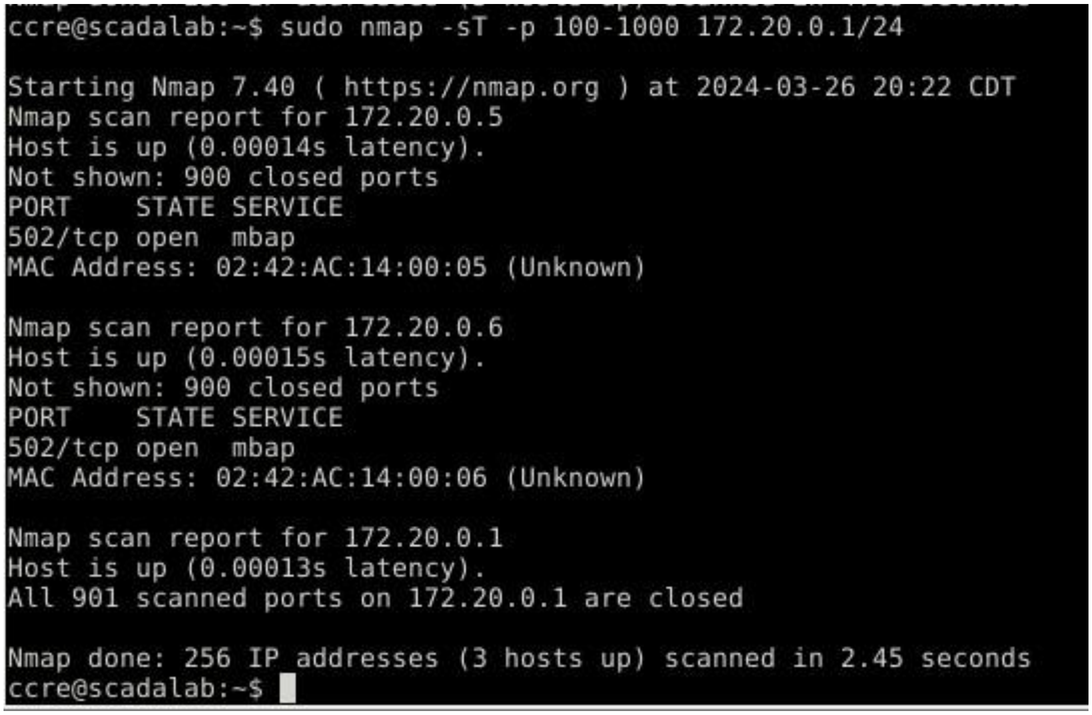
Dan Otieno
CPE 459
Spring 2024.



```
ccre@scadalab:~$ sudo nmap -sT -p 100-1000 172.18.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:14 CDT
Nmap scan report for 172.18.0.3
Host is up (0.00015s latency).
Not shown: 900 closed ports
PORT    STATE SERVICE
502/tcp open  mbap
MAC Address: 02:42:AC:12:00:03 (Unknown)

Nmap scan report for 172.18.0.10
Host is up (0.00016s latency).
All 901 scanned ports on 172.18.0.10 are closed
MAC Address: 02:42:AC:12:00:0A (Unknown)

Nmap scan report for 172.18.0.1
Host is up (0.000078s latency).
All 901 scanned ports on 172.18.0.1 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.17 seconds
ccre@scadalab:~$
```



```
ccre@scadalab:~$ sudo nmap -sT -p 100-1000 172.19.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:17 CDT
Nmap scan report for 172.19.0.3
Host is up (0.00015s latency).
Not shown: 900 closed ports
PORT    STATE SERVICE
502/tcp open  mbap
MAC Address: 02:42:AC:13:00:03 (Unknown)

Nmap scan report for 172.19.0.10
Host is up (0.00016s latency).
All 901 scanned ports on 172.19.0.10 are closed
MAC Address: 02:42:AC:13:00:0A (Unknown)

Nmap scan report for 172.19.0.1
Host is up (0.000068s latency).
All 901 scanned ports on 172.19.0.1 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.08 seconds
ccre@scadalab:~$
```

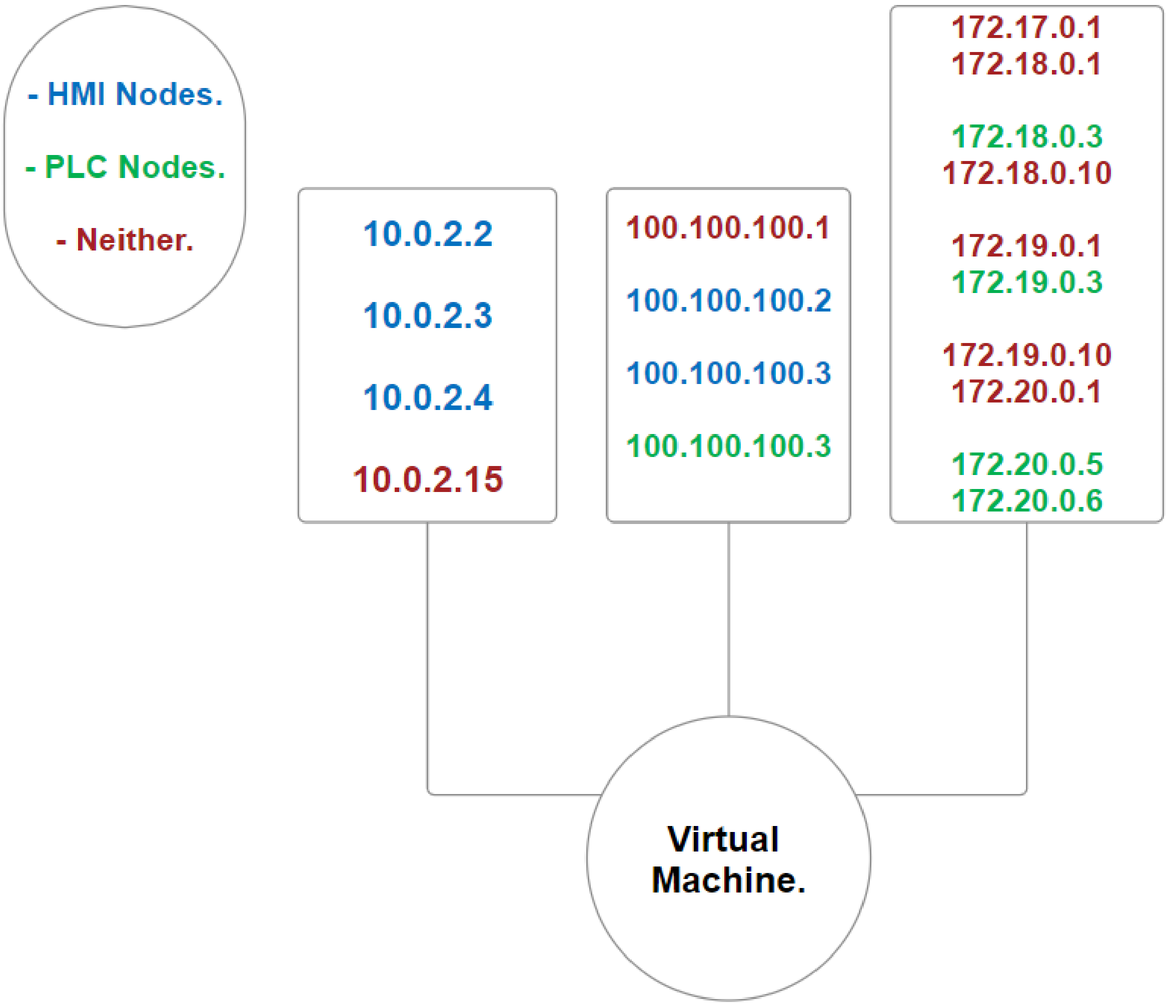


```
ccre@scadalab:~$ sudo nmap -sT -p 100-1000 172.20.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2024-03-26 20:22 CDT
Nmap scan report for 172.20.0.5
Host is up (0.00014s latency).
Not shown: 900 closed ports
PORT    STATE SERVICE
502/tcp open  mbap
MAC Address: 02:42:AC:14:00:05 (Unknown)

Nmap scan report for 172.20.0.6
Host is up (0.00015s latency).
Not shown: 900 closed ports
PORT    STATE SERVICE
502/tcp open  mbap
MAC Address: 02:42:AC:14:00:06 (Unknown)

Nmap scan report for 172.20.0.1
Host is up (0.00013s latency).
All 901 scanned ports on 172.20.0.1 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.45 seconds
ccre@scadalab:~$ 
```

4. Determine what nodes are PLCs, what nodes are HMIs, and what nodes - if any - are neither.
   - **PLC Nodes:**
     - **100.100.100.3**
     - **172.18.0.3**
     - **172.19.0.3**
     - **172.20.0.5**
     - **172.20.0.6**
   - **HMI Nodes:**
     - **10.0.2.2**
     - **10.0.2.3**
     - **10.0.2.4**
     - **100.100.100.2**
     - **100.100.100.3**
   - **Neither:**
     - **10.0.2.15**
     - **100.100.100.1**
     - **172.17.0.1**
     - **172.18.0.1**
     - **172.18.0.10**
     - **172.19.0.1**
     - **172.19.0.10**
     - **172.20.0.1**

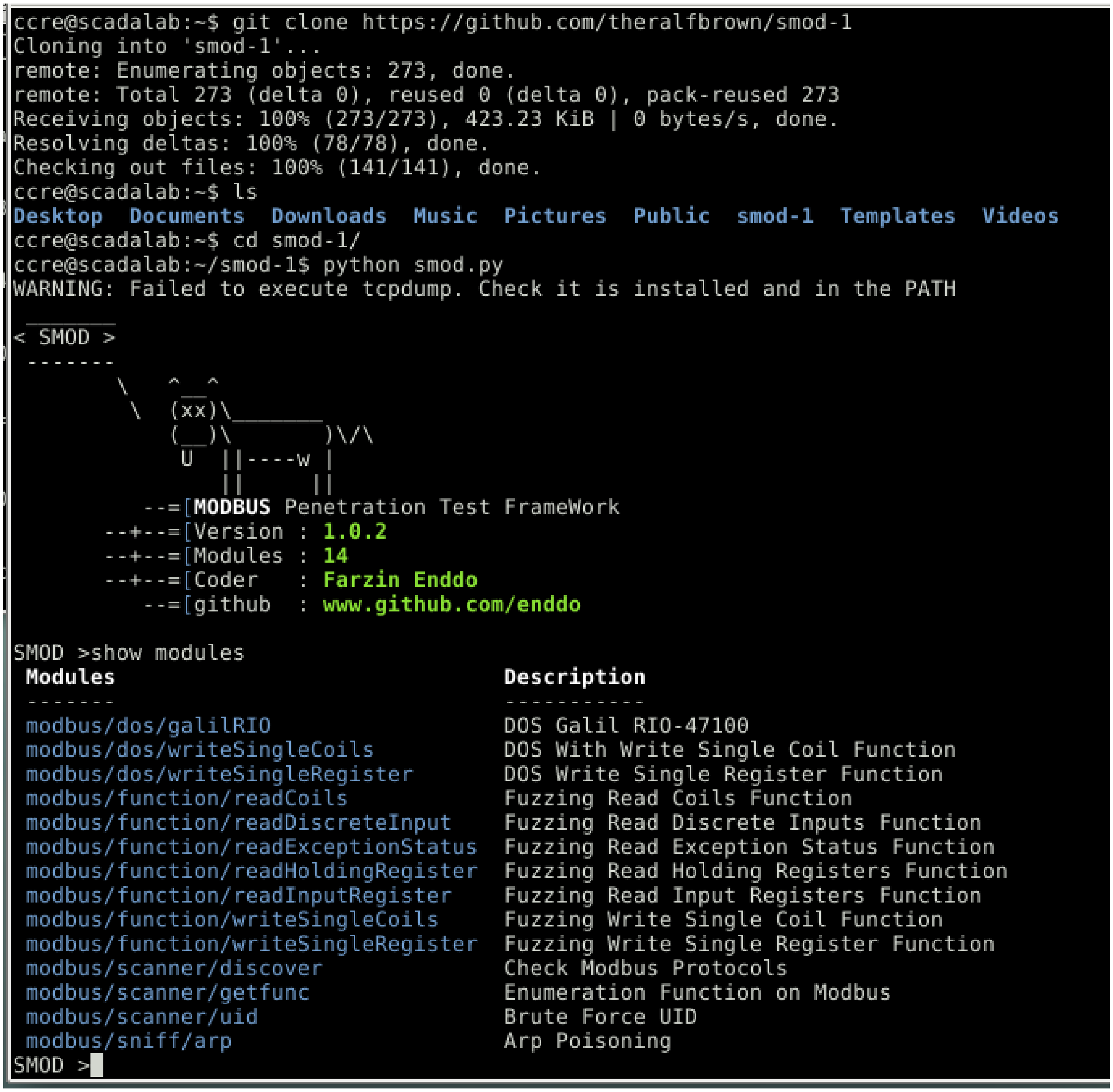
Dan Otieno
CPE 459
Spring 2024.

5. Draw (or digitally create) a picture of the network topology that you determined. Clearly denote the IPs, different network interfaces, and presumed roles of active nodes.



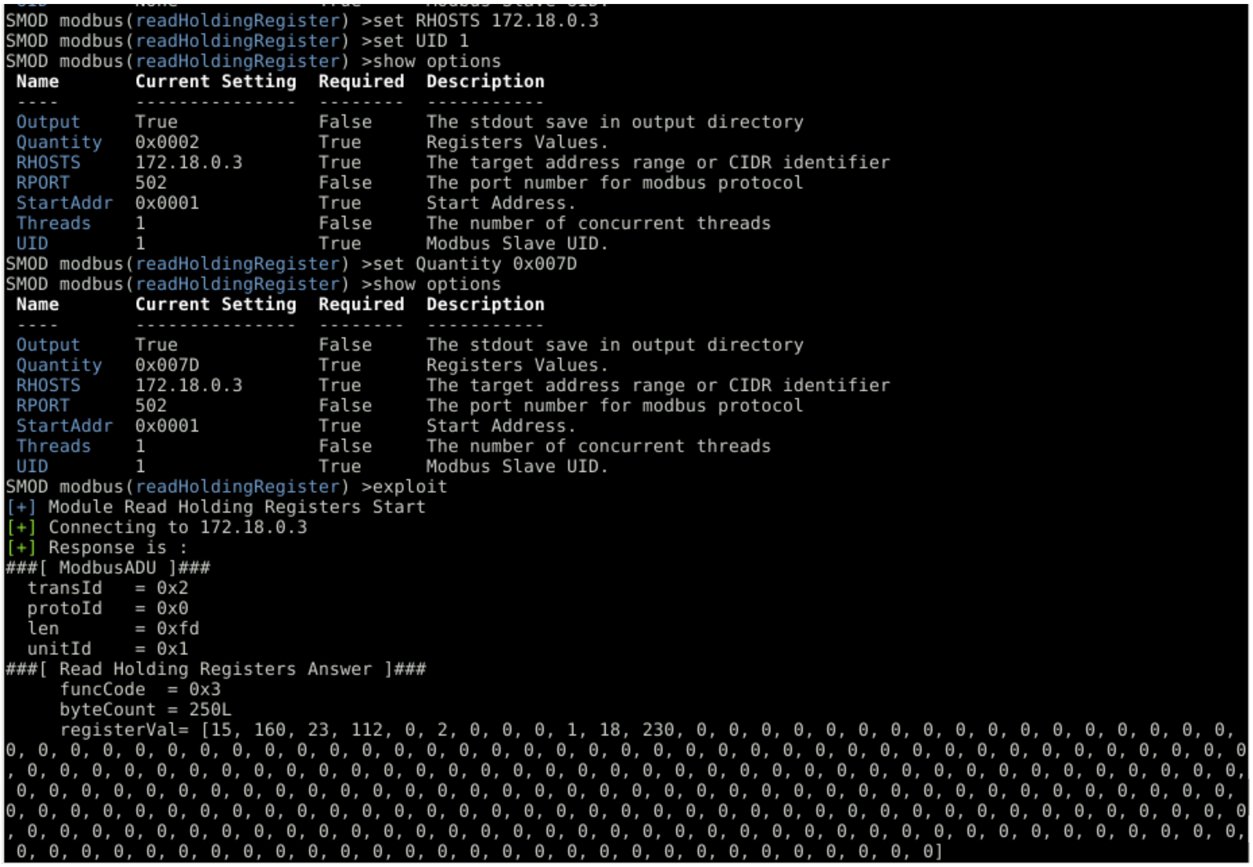
6. Once you've correctly identified the network(s) and their connected nodes, determine all nonzero holding registers on each PLC node using S-MOD, Pymodbus or any other tool you would like.

Dan Otieno
CPE 459
Spring 2024.

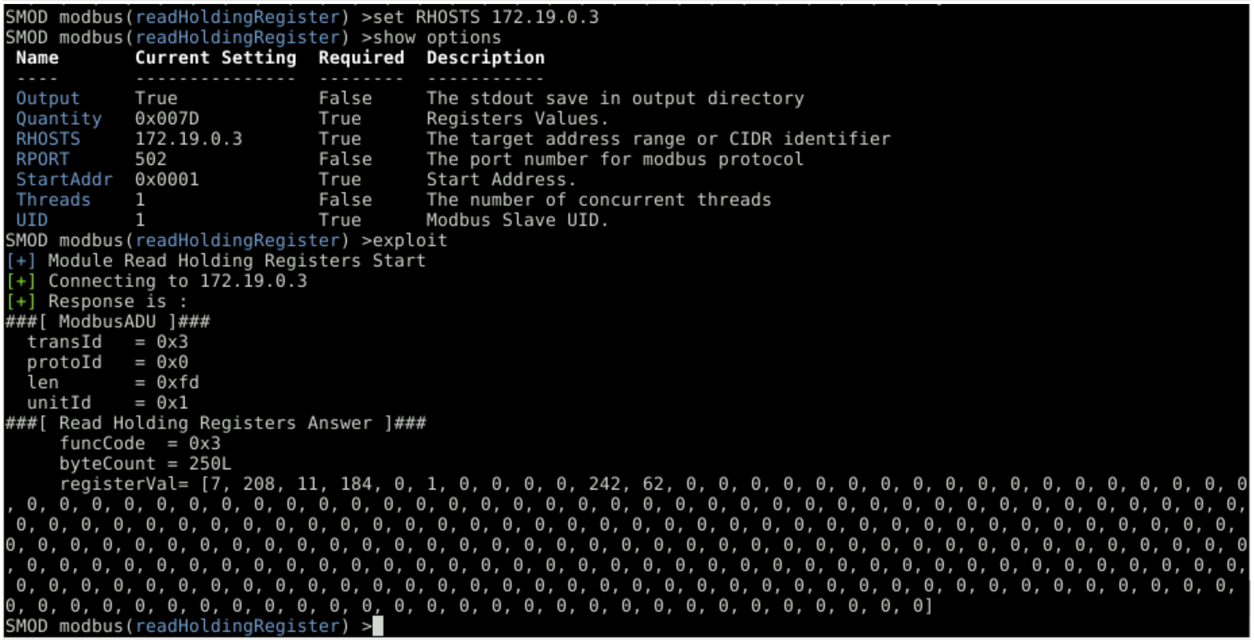


```
ccre@scadalab:~$ git clone https://github.com/theralfbrown/smod-1
Cloning into 'smod-1'...
remote: Enumerating objects: 273, done.
remote: Total 273 (delta 0), reused 0 (delta 0), pack-reused 273
Receiving objects: 100% (273/273), 423.23 KiB | 0 bytes/s, done.
Resolving deltas: 100% (78/78), done.
Checking out files: 100% (141/141), done.
ccre@scadalab:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  smod-1  Templates  Videos
ccre@scadalab:~$ cd smod-1/
ccre@scadalab:~/smod-1$ python smod.py
WARNING: Failed to execute tcpdump. Check it is installed and in the PATH

 _______
< SMOD >
 -------
        \   ^__^
         \  (xx)\_______
            (__)\       )\/\
             U  ||----w |
                ||     ||
          --=[MODBUS Penetration Test FrameWork
       --+--=[Version : 1.0.2
       --+--=[Modules : 14
       --+--=[Coder   : Farzin Enddo
          --=[github  : www.github.com/enddo

SMOD >show modules
 Modules                              Description
 -------                              -----------
 modbus/dos/galilRIO                  DOS Galil RIO-47100
 modbus/dos/writeSingleCoils          DOS With Write Single Coil Function
 modbus/dos/writeSingleRegister       DOS Write Single Register Function
 modbus/function/readCoils            Fuzzing Read Coils Function
 modbus/function/readDiscreteInput    Fuzzing Read Discrete Inputs Function
 modbus/function/readExceptionStatus  Fuzzing Read Exception Status Function
 modbus/function/readHoldingRegister  Fuzzing Read Holding Registers Function
 modbus/function/readInputRegister    Fuzzing Read Input Registers Function
 modbus/function/writeSingleCoils     Fuzzing Write Single Coil Function
 modbus/function/writeSingleRegister  Fuzzing Write Single Register Function
 modbus/scanner/discover              Check Modbus Protocols
 modbus/scanner/getfunc               Enumeration Function on Modbus
 modbus/scanner/uid                   Brute Force UID
 modbus/sniff/arp                     Arp Poisoning
SMOD >
```

Dan Otieno
CPE 459
Spring 2024.

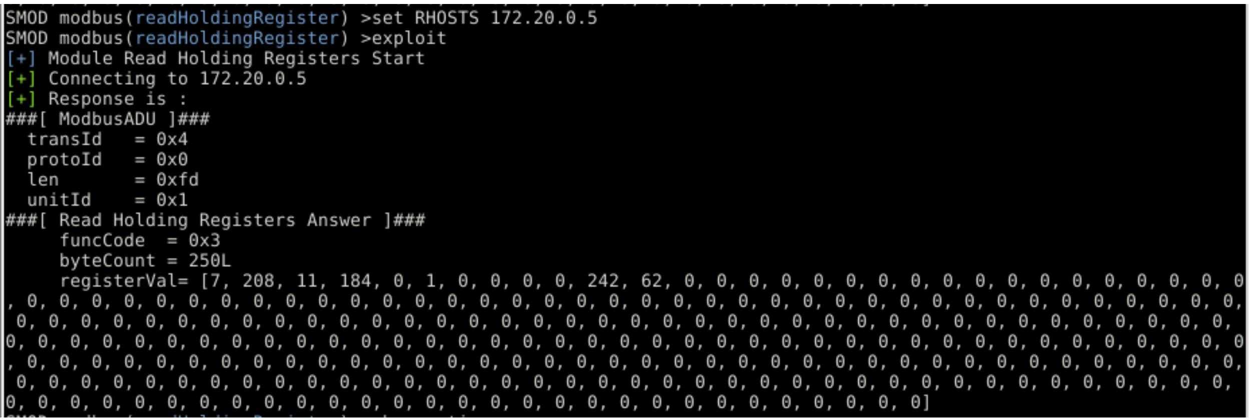


```
SMOD modbus(readHoldingRegister) >set RHOSTS 172.18.0.3
SMOD modbus(readHoldingRegister) >set UID 1
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x0002           True      Registers Values.
 RHOSTS      172.18.0.3       True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >set Quantity 0x007D
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x007D           True      Registers Values.
 RHOSTS      172.18.0.3       True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >exploit
[+] Module Read Holding Registers Start
[+] Connecting to 172.18.0.3
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x2
  protoId   = 0x0
  len       = 0xfd
  unitId    = 0x1
###[ Read Holding Registers Answer ]###
     funcCode  = 0x3
     byteCount = 250L
     registerVal= [15, 160, 23, 112, 0, 2, 0, 0, 0, 1, 18, 230, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

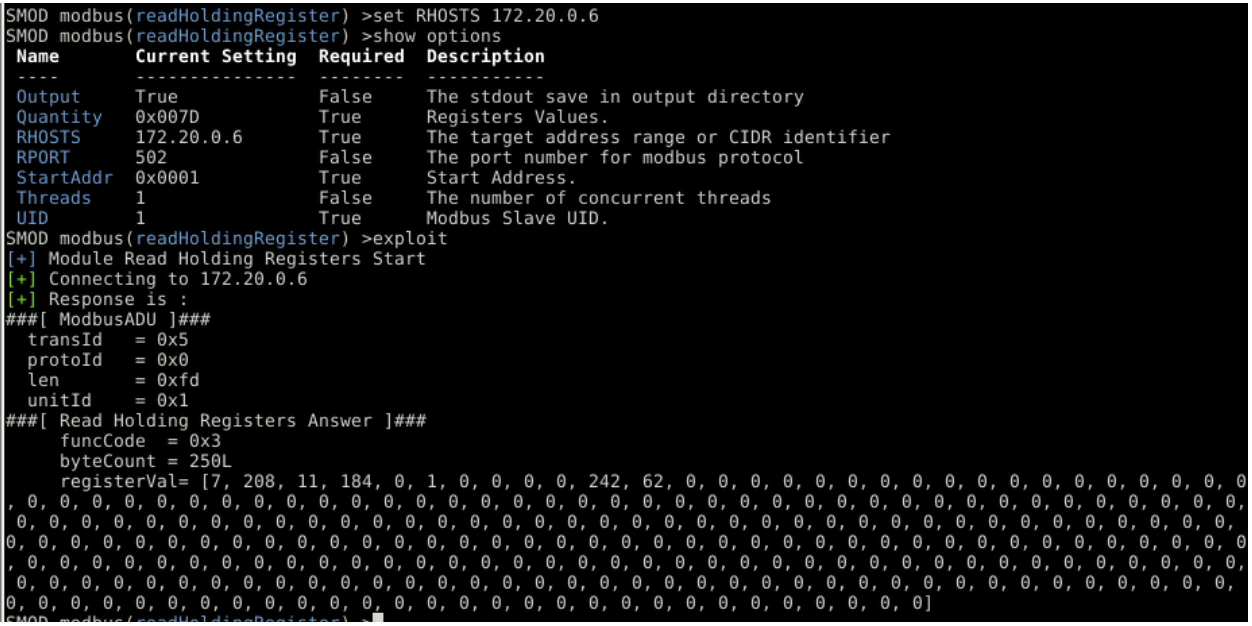


```
SMOD modbus(readHoldingRegister) >set RHOSTS 172.19.0.3
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x007D           True      Registers Values.
 RHOSTS      172.19.0.3       True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >exploit
[+] Module Read Holding Registers Start
[+] Connecting to 172.19.0.3
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x3
  protoId   = 0x0
  len       = 0xfd
  unitId    = 0x1
###[ Read Holding Registers Answer ]###
     funcCode  = 0x3
     byteCount = 250L
     registerVal= [7, 208, 11, 184, 0, 1, 0, 0, 0, 0, 242, 62, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
SMOD modbus(readHoldingRegister) >
```

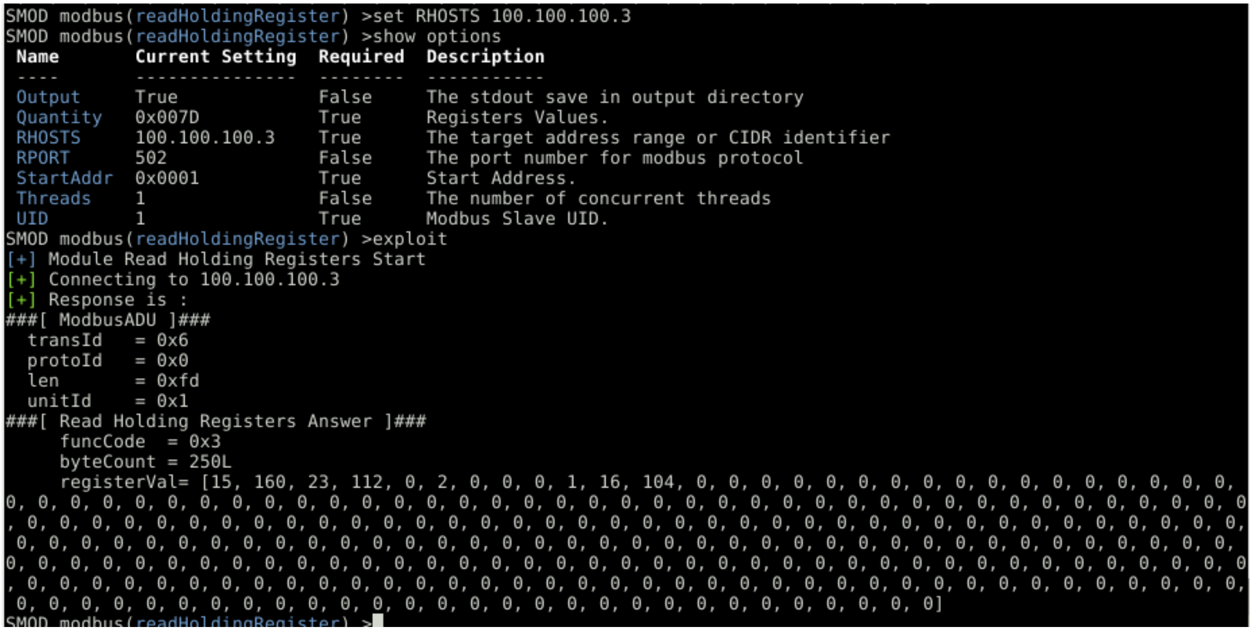
Dan Otieno
CPE 459
Spring 2024.



```
SMOD modbus(readHoldingRegister) >set RHOSTS 172.20.0.5
SMOD modbus(readHoldingRegister) >exploit
[+] Module Read Holding Registers Start
[+] Connecting to 172.20.0.5
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x4
  protoId   = 0x0
  len       = 0xfd
  unitId    = 0x1
###[ Read Holding Registers Answer ]###
     funcCode  = 0x3
     byteCount = 250L
     registerVal= [7, 208, 11, 184, 0, 1, 0, 0, 0, 0, 242, 62, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```



```
SMOD modbus(readHoldingRegister) >set RHOSTS 172.20.0.6
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x007D           True      Registers Values.
 RHOSTS      172.20.0.6       True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >exploit
[+] Module Read Holding Registers Start
[+] Connecting to 172.20.0.6
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x5
  protoId   = 0x0
  len       = 0xfd
  unitId    = 0x1
###[ Read Holding Registers Answer ]###
     funcCode  = 0x3
     byteCount = 250L
     registerVal= [7, 208, 11, 184, 0, 1, 0, 0, 0, 0, 242, 62, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
SMOD modbus(readHoldingRegister) >
```



```
SMOD modbus(readHoldingRegister) >set RHOSTS 100.100.100.3
SMOD modbus(readHoldingRegister) >show options
 Name        Current Setting  Required  Description
 ----        ---------------  --------  -----------
 Output      True             False     The stdout save in output directory
 Quantity    0x007D           True      Registers Values.
 RHOSTS      100.100.100.3    True      The target address range or CIDR identifier
 RPORT       502              False     The port number for modbus protocol
 StartAddr   0x0001           True      Start Address.
 Threads     1                False     The number of concurrent threads
 UID         1                True      Modbus Slave UID.
SMOD modbus(readHoldingRegister) >exploit
[+] Module Read Holding Registers Start
[+] Connecting to 100.100.100.3
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x6
  protoId   = 0x0
  len       = 0xfd
  unitId    = 0x1
###[ Read Holding Registers Answer ]###
     funcCode  = 0x3
     byteCount = 250L
     registerVal= [15, 160, 23, 112, 0, 2, 0, 0, 0, 1, 16, 104, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
SMOD modbus(readHoldingRegister) >
```

Dan Otieno
CPE 459
Spring 2024.