

# Nmap Lab Form

Name: [ ]

Date: [ ]

1. How many systems were found when performing the default scan in part 2? How long did the scan take?

[ ]

The default scan should find 6 active hosts.

The default scan took 11.17 seconds on my system. It should be more than the time shown in the next question.

```
student@kali: ~  
File Actions Edit View Help  
(student@kali)-[~]  
$ sudo nmap 10.0.255.1-255  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-29 15:45 EDT  
Nmap scan report for ICS-SA.home.arpa (10.0.255.1)  
Host is up (0.00029s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
MAC Address: 08:00:27:30:62:8C (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.255.100  
Host is up (0.00024s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1036/tcp  open  nsstp  
1037/tcp  open  ams  
MAC Address: 08:00:27:F0:AD:D9 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.255.101  
Host is up (0.00027s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1040/tcp  open  netsaint  
MAC Address: 08:00:27:41:54:E6 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.255.102  
Host is up (0.00023s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
23/tcp    open  telnet  
MAC Address: 08:00:27:D8:90:2B (Oracle VirtualBox virtual NIC)
```

2. How many systems were found when performing the ping scan in part 3? How long did the scan take?

The ping scan should find 6 active hosts.

The ping scan took 6.68 seconds on my system. It should be less than the time shown in the next question.

```
student@kali: ~  
File Actions Edit View Help  
  
(student@kali)-[~]  
$ sudo nmap -sn 10.0.255.1-255  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-29 15:51 EDT  
Nmap scan report for ICS-SA.home.arpa (10.0.255.1)  
Host is up (0.00033s latency).  
MAC Address: 08:00:27:30:62:8C (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.255.100  
Host is up (0.00020s latency).  
MAC Address: 08:00:27:F0:AD:D9 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.255.101  
Host is up (0.00019s latency).  
MAC Address: 08:00:27:41:54:E6 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.255.102  
Host is up (0.00019s latency).  
MAC Address: 08:00:27:D8:90:2B (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.255.103  
Host is up (0.00023s latency).  
MAC Address: 08:00:27:CC:D4:FE (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.255.108  
Host is up.  
Nmap done: 255 IP addresses (6 hosts up) scanned in 6.37 seconds  
  
(student@kali)-[~]  
$
```

3. How many systems were found when performing the fast scan in part 3? How long did the scan take?

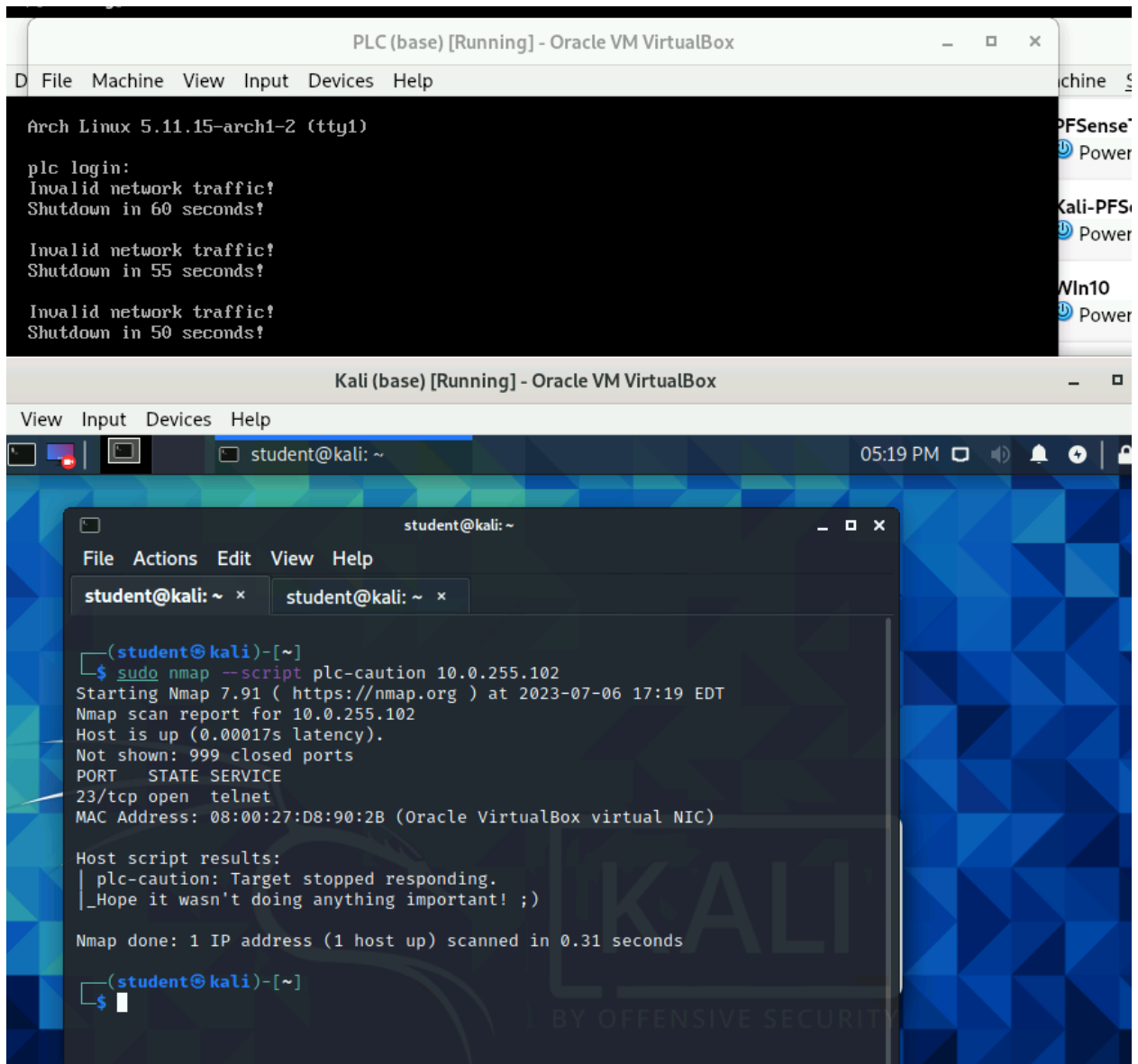
The fast scan should find 6 active hosts.

The fast scan took 7.73 seconds on my system. The time should probably be in between the time taken for the default scan and the ping scan.

```
student@kali: ~  
File Actions Edit View Help  
  
(student@kali)-[~]  
$ sudo nmap -T5 10.0.255.1-255  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-29 15:52 EDT  
Nmap scan report for ICS-SA.home.arpa (10.0.255.1)  
Host is up (0.00025s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
MAC Address: 08:00:27:30:62:8C (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.255.100  
Host is up (0.00029s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1036/tcp  open  nsstp  
1037/tcp  open  ams  
MAC Address: 08:00:27:F0:AD:D9 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.255.101  
Host is up (0.00016s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1040/tcp  open  netsaint  
MAC Address: 08:00:27:41:54:E6 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.255.102  
Host is up (0.00012s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
23/tcp    open  telnet
```

4. What happened to the PLC system when you ran the intrusive plc-caution script?

The plc-caution script causes the PLC system to reboot.



5. What is the IP address of the system that has the NetBIOS computer name OPC\x00?

`sudo nmap -A 10.0.255.1-254`

The OPC\x00 system's IP address is 10.0.255.100

```
student@kali: ~  
File Actions Edit View Help  
(student@kali)-[~]  
$ nmap -A 10.0.255.100  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-07-08 12:10 EDT  
Nmap scan report for 10.0.255.100  
Host is up (0.60s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds Windows XP microsoft-ds  
1035/tcp   open  msrpc        Microsoft Windows RPC  
1036/tcp   open  msrpc        Microsoft Windows RPC  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Host script results:  
_clock-skew: mean: 1h59m59s, deviation: 2h49m42s, median: 0s  
_nbstat: NetBIOS name: OPC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:87:cc:cf (Oracle VirtualBox virtual NIC)  
smb-os-discovery:  
  OS: Windows XP (Windows 2000 LAN Manager)  
  OS CPE: cpe:/o:microsoft:windows_xp::-  
  Computer name: opc  
  NetBIOS computer name: OPC\x00  
  Workgroup: WORKGROUP\x00  
  System time: 2023-07-08T12:11:13-04:00  
smb-security-mode:  
  account_used: <blank>  
  authentication_level: user  
  challenge_response: supported  
_ message_signing: disabled (dangerous, but default)  
_smb2-time: Protocol negotiation failed (SMB2)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 115.28 seconds  
  
(student@kali)-[~]  
$
```

6. What are the IP addresses of the systems running the Modbus protocol?

```
sudo nmap -p 502 10.0.255.1-254  
10.0.255.100, 10.0.255.102
```



```
L$ sudo nmap -p 502 10.0.255.1-254
Starting Nmap 7.91 ( https://nmap.org ) at 2023-07-10 08:45 EDT
Nmap scan report for ICS-SA.home.arpa (10.0.255.1)
Host is up (0.00023s latency).

PORT      STATE      SERVICE
502/tcp    filtered  mbap
MAC Address: 08:00:27:D4:87:C2 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.255.100
Host is up (0.0026s latency).

PORT      STATE      SERVICE
502/tcp    open       mbap
MAC Address: 08:00:27:87:CC:CF (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.255.101
Host is up (0.00029s latency).

PORT      STATE      SERVICE
502/tcp    closed     mbap
MAC Address: 08:00:27:79:57:23 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.255.102
Host is up (0.00027s latency).

PORT      STATE      SERVICE
502/tcp    open       mbap
MAC Address: 08:00:27:0D:C9:89 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.255.103
Host is up (0.00027s latency).

PORT      STATE      SERVICE
502/tcp    closed     mbap
MAC Address: 08:00:27:0E:84:EA (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.255.108
Host is up (0.000025s latency).

PORT      STATE      SERVICE
502/tcp    closed     mbap

Nmap done: 254 IP addresses (6 hosts up) scanned in 4.12 seconds
```