Markus Afonso, Devin Kandola
Group 41, Set C
January 9, 2024

Q1: How can you find this (kali) machine's IP?

With the command **ip a : 10.0.2.15**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86269sec preferred_lft 86269sec
    inet6 fe80::865f:a718:2eb0:f021/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Q2: How can you find this (Metasploitable 2) machine's IP?

With the command **ip a : 10.0.2.4**

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:5f:36:bd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe5f:36bd/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 08:00:27:6f:4c:c0 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
```

Q3: How can you find this machine's OS as well as the services and their software versions running on open ports on this machine from your Kali VM?

machine's OS:

Using the -O option, machine OS can be found near the bottom of the screenshot.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 13:34 EST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.00% done; ETC: 13:34 (0:00:01 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.48s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5F:36:BD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds
```

services:

Using the -PS option we can list all the services and their port.

```
┌──(kali㉿kali)-[~]
└─$ nmap -PS 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 13:27 EST
Nmap scan report for 10.0.2.4
Host is up (0.081s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.43 seconds
```

software versions:

Using the -sV option and specifying port 3306 with the option -p3306 we can find the software using port 3306 and it's version.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p3306 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 13:33 EST
Nmap scan report for 10.0.2.4
Host is up (0.0094s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

Q4: What's the use case when we need to use -Pn probing option with nmap?

When a network is blocking ping probes, using the option -Pn can be used to by pass it.

```
┌──(kali㉿kali)-[~]
└─$ nmap scan2.certmike.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 13:36 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn scan2.certmike.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 13:36 EST
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.45% done; ETC: 13:37 (0:00:22 remaining)
Nmap scan report for scan2.certmike.com (18.213.123.154)
Host is up (0.14s latency).
rDNS record for 18.213.123.154: ec2-18-213-123-154.compute-1.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 92.28 seconds
```