Nmap

Monday, October 28, 2019 9:01 PM

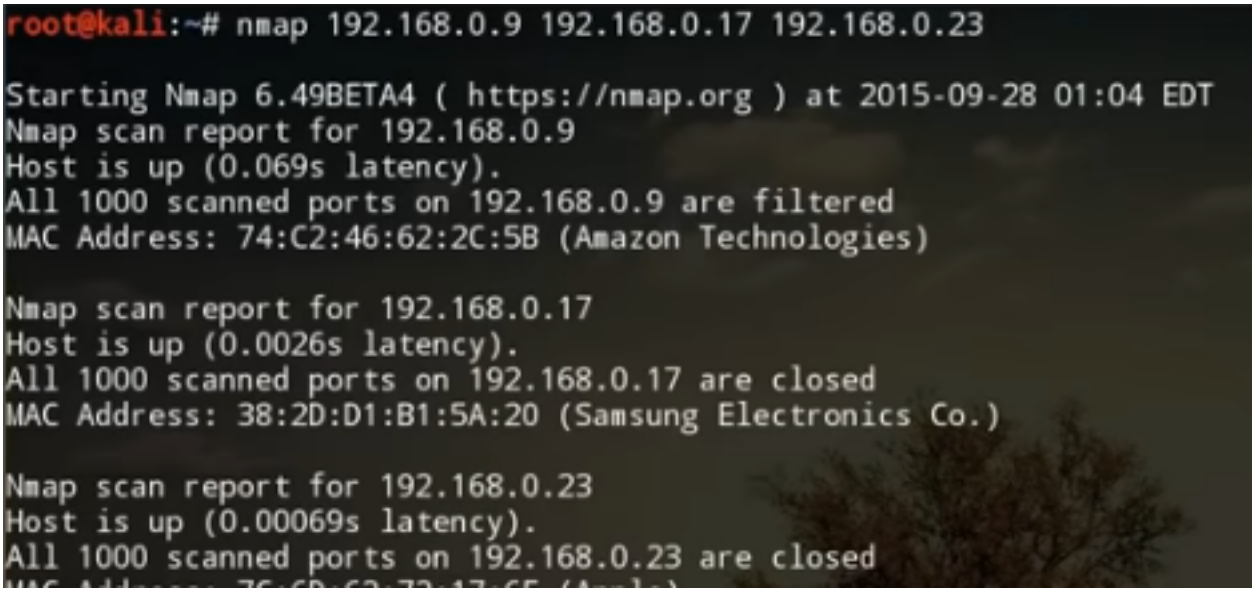
What is Nmap?

Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by Sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

Scanning Multiple Targets:

Doing the tutorial from thenewboston<hyperlink> Nmap tutorial,

We're attempting to scan multiple targets. On the screen below you see Bucky has 3 ip addresses for his nmap scan:



```
Nmap scan report for 192.168.0.23
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.0.23 are closed
MAC Address: 7C:6D:62:72:17:6E (Apple)

Nmap done: 3 IP addresses (3 hosts up) scanned in 230.80 seconds
root@kali:~#
```

Scan the entire range of ip addresses for all of the devices on my network:

```
shinobibughunter@kali:~$ nmap 10.0.2.1-30
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 13:53 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0022s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/tcp open  rpcbind

Nmap scan report for 10.0.2.17
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

Scan the entire subnet:

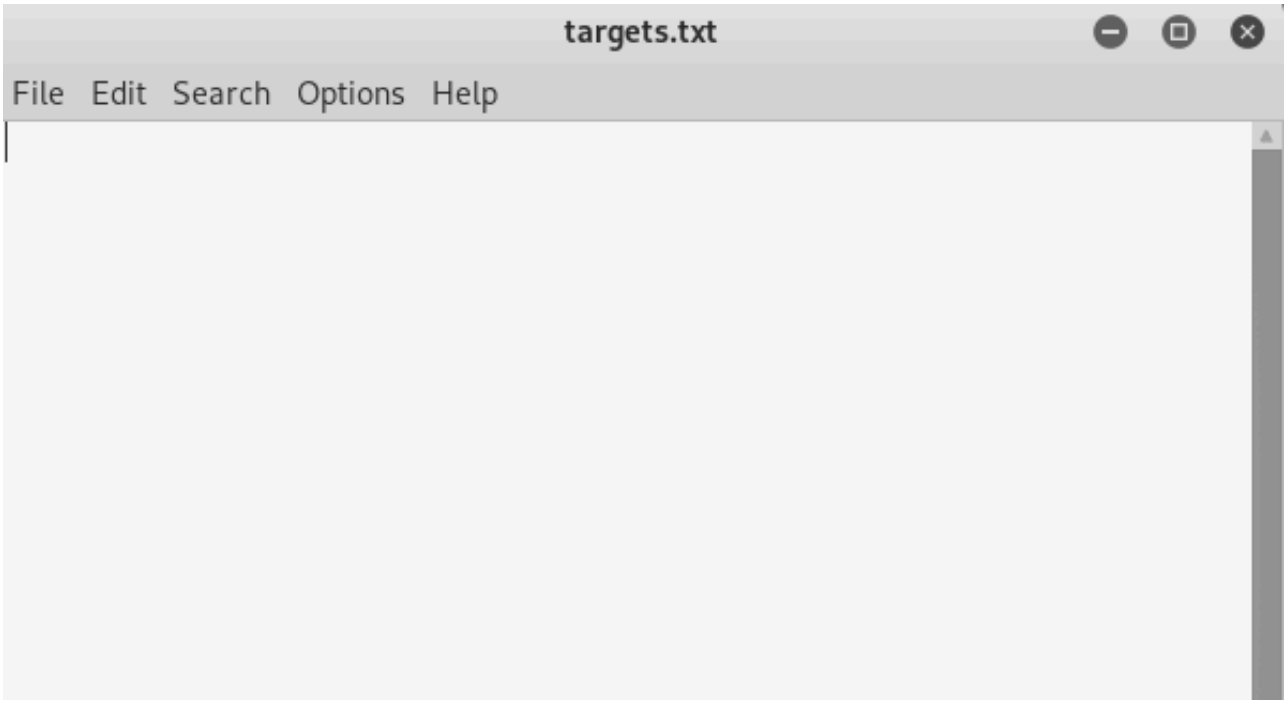
```
shinobibughunter@kali:~$ nmap 10.0.2.0-255
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 13:55 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00082s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/tcp open  rpcbind

Nmap scan report for 10.0.2.17
Host is up (0.00096s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (2 hosts up) scanned in 16.45 seconds
```

Or can write nmap 10.0.2.* should get same result as above

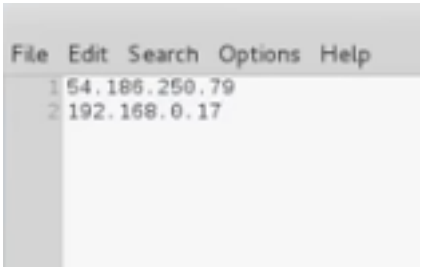
Make a file and have a list of ip address in it:

1. Make a file called "targets.txt":

2. Type leafpad "targets.txt":



3. Type in some Ip address examples:
   (I'm using the image that Bucky used since I don't have many resources avaliable at the moment)



4. Choose the -iL command: which means input lists:

```
root@kali:~/Desktop# nmap -iL targets.txt
```

You would get the same results as before

Aggressive/Detailed Scan:

Nmap -A: which means scan aggressively:

```
shinobibughunter@kali:~$ nmap -A 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 14:58 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.30 seconds
```

Looking at this scan you can see it goes a little further than the previous ones.

You can see what Operating System its running like Linux and it goes much deeper into what the ports show.

Running as Traceroute:

```
root@kali:~# nmap --traceroute 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:04 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00048s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 10.0.2.17
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
root@kali:~#
```

burpsuite

Running for Service:

```
root@kali:~# nmap -O 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:06 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00051s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
```

```
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
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 15.02 seconds
root@kali:~#
```

Running for Service Version:

```
root@kali:~# nmap -sV 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:09 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00021s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.
0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.89 seconds
```

As you can see in the results of the scan, this time we have a Version column appear.

More Port Scanning Options:

Scan Fewer Ports Fast:

```
root@kali:~# nmap -F 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:14 EDT
Nmap scan report for 10.0.2.17
Host is up (0.0037s latency).
Not shown: 97 closed ports
PORT   STATE SERVICE
```

```
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
root@kali:~#
```

Specify Ports:

```
root@kali:~# nmap -p 20-25,80,443 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:17 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00030s latency).

PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed telnet
24/tcp  closed priv-mail
25/tcp  closed smtp
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
root@kali:~#
```

Scan Ports By Name:

```
root@kali:~# nmap -p 20-25,80,443 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:17 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00030s latency).

PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed telnet
24/tcp  closed priv-mail
25/tcp  closed smtp
80/tcp  open   http
```

```
443/tcp closed https
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
root@kali:~#
```

Scan Every Single Port (Best to do for a company):

```
root@kali:~# nmap -p 20-25,80,443 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:17 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00030s latency).

PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed telnet
24/tcp  closed priv-mail
25/tcp  closed smtp
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
root@kali:~#
```

Scan & Display Open ports only:

This will scan the 1000 commonly used ports buts its only going to display the open ports. Because if a port is filtered, its most likely not a huge vulnerability.

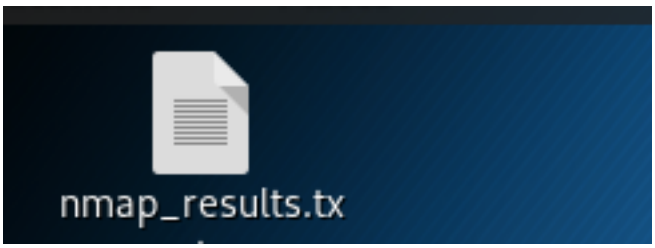
```
root@kali:~# nmap -p http,mysql 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:19 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00042s latency).

PORT     STATE  SERVICE
80/tcp   open   http
```

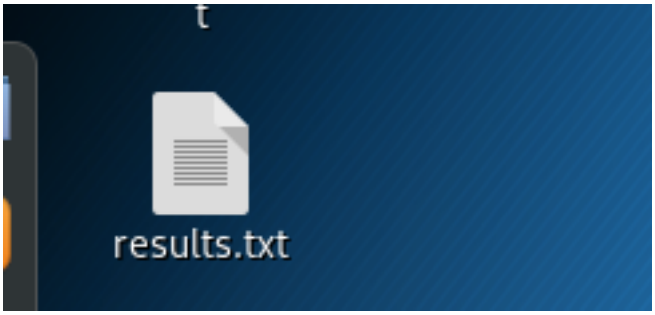
```
3306/tcp closed mysql
8008/tcp closed http
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
root@kali:~#
```

Saving Scan Results:

Typing -oN will save information to a regular text file, while typing -oX will save it to an xml file. Don't forget to write the location of file.

```
root@kali:~# nmap -F -oN Desktop/results.txt 10.0.2.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-02 15:31 EDT
Nmap scan report for 10.0.2.17
Host is up (0.00015s latency).
Not shown: 97 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
root@kali:~#
root@kali:~#
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
nmap_results.txt  results.txt
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
```





nmap_results.txt
~/Desktop

Open Save

```
# Nmap 7.80 scan initiated Sat Nov  2 15:29:58 2019 as: nmap --open -oN Desktop/nmap_results.txt
10.0.2.17
Nmap scan report for 10.0.2.17
Host is up (0.00069s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:69:94:F2 (Oracle VirtualBox virtual NIC)

# Nmap done at Sat Nov  2 15:30:11 2019 -- 1 IP address (1 host up) scanned in 13.30 seconds
```