# Nmap

Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So Nmap is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac. Nmap is a very powerful utility that can be used to:

- Detect the live host on the network (host discovery)
- Detect the open ports on the host (port discovery or enumeration)
- Detect the software and the version to the respective port (service discovery)
- Detect the operating system, hardware address, and the software version
- Detect the vulnerability and security holes (Nmap scripts)

Nmap is a very common tool, and it is available for both the command line interface and the graphical user interface.

## Supported Operating System:-

Windows

Linux

## How to download Nmap?

Download Nmap from www.nmap.org for windows and in Kali Linux Nmap is by default tool.

Git Repository:- https://github.com/nmap/nmap.git

## How to use Nmap

The usage of Nmap depends on the target machine because there is a difference between simple (basic) scanning and advance scanning. We need to use some advanced techniques to bypass the firewall and intrusion detection/preventative software to get the right result. Below are the examples of some basic commands and their usage:

If you want to scan a single system, then you can use a simple command

```
nmap target
```

```
# nmap target.com
```

```
# nmap 192.168.1.1
```

If you want to scan the entire subnet, then the command is

```
nmap target/cdir
```

```
# nmap 192.168.1.1/24
```

It is very easy to scan a multiple targets, all you need to do is to separate each target via space:

```
nmap target target1 target2
```

```
# nmap 192.168.1.1 192.168.1.8
```

Let’s suppose you want to scan a range of IP addresses, but not the entire subnet. In this scenario, use this command:

```
nmap target-100
```

```
# nmap 192.168.1.1-100
```

Let suppose you have a list of a target machines. You can make Nmap scan for the entire list:

```
# nmap -iL target.txt
```

**Make sure to put the file on the same directory**

If you want to see the list of all the hosts that you are scanning, then use the command with an -sL parameter:

```
nmap -sL target/cdir
```

```
# nmap -sL 192.168.1.1/24
```

In some cases we need to scan the entire subnet but not a specific IP addresses because it might be dangerous for us. In this scenario, use the Nmap command with the excluding parameter:

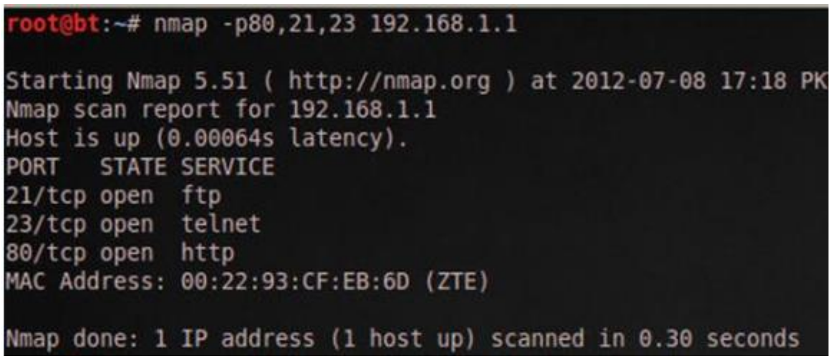
**# nmap 192.168.1.1/24 – -exclude 192.168.1.1**

If you have a file that contains the list of IP addresses that you want to exclude, then you can call the file in the exclude parameter:

**# nmap 192.168.1.1/24 –exclude file target.txt**

If you want to scan a specific port on the target machines (for example, if you want to scan the HTTP, FTP, and Telnet port only on the target computer), then you can use the Nmap command with the relevant parameter:

**# nmap -p80,21,23 192.168.1.1 It scan the target for port number 80,21 and 23.**



```
root@bt:~# nmap -p80,21,23 192.168.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-08 17:18 PK
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:22:93:CF:EB:6D (ZTE)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```