Start Nmap

Nmap is usually used through a command-line interface. To verify if Nmap is already installed in Linux, run the **nmap --version** command:

```
root@kali:~# nmap --version

Nmap version 7.01 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2e libpcre-8.38 libpcap-1.7.4 nmap-libdn
et-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

If you don't have Nmap installed, install it using the **sudo apt-get install nmap** command.

The official website, **nmap.org**, offers a machine that can be scanned to help people learn about Nmap. It is available at **scanme.nmap.org**. To scan this machine with default settings, simply run **nmap scanme.nmap.org**:

```
root@kali:~# nmap scanme.nmap.org

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-03 19:41 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.5s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
514/tcp   filtered shell
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 45.55 seconds
```

As you can see from the output above, Nmap provided a report indicating which ports are open on **scanme.nmap.org**. For example, the line **22/tcp open ssh** indicates that the TCP port 22 is open, and that ssh service is probably running on that port.

We can also scan a computer inside our LAN:

```
root@kali:~# nmap 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-03 19:46 CET
Nmap scan report for 192.168.5.102
Host is up (1.0s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
53/tcp    open     domain
80/tcp    open     http
88/tcp    open     kerberos-sec
```

```
111/tcp   open     rpcbind
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
389/tcp   open     ldap
445/tcp   open     microsoft-ds
464/tcp   open     kpasswd5
514/tcp   filtered shell
593/tcp   open     http-rpc-epmap
636/tcp   open     ldapssl
2049/tcp  open     nfs
3260/tcp  open     iscsi
3268/tcp  open     globalcatLDAP
3269/tcp  open     globalcatLDAPssl
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49157/tcp open     unknown
49158/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 100.94 seconds
```

As you can see from the output above, the local machine 192.168.5.102 (it is a Windows Server 2012 instance).

Just like many other Linux commands and applications, Nmap offers a comprehensive **man pages** which can help you if you are in an environment without Internet connection. Simply run **man nmap** to get more information about the program.

Determine service version

You can use Nmap to determine the version of the software the target is running. This is particulary useful when doing vulnerability assessments, since you really want to know, for example, which mail and DNS servers and versions are running, and having an accurate version helps dramatically in determining which exploits a server is vulnerable to.

You can determine a lot of information using service scans, including:

- the service protocol (e.g. FTP, SSH, Telnet, HTTP).
- the application name (e.g. BIND, Apache httpd).
- the version number.
- hostname.
- device type (e.g. printer, router).
- the OS family (e.g. Windows, Linux).

To run a service version scan, use the **-sV** flags:

```
root@kali:~# nmap -sV 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-03 20:07 CET
Nmap scan report for 192.168.5.102
```

```
Host is up (1.0s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          Microsoft ftpd
53/tcp    open     domain       Microsoft DNS
80/tcp    open     http         Microsoft IIS httpd 8.0
88/tcp    open     kerberos-sec Windows 2003 Kerberos (server time: 2016-03-03
19:09:38Z)
111/tcp   open     rpcbind?
135/tcp   open     msrpc        Microsoft Windows RPC
139/tcp   open     netbios-ssn  Microsoft Windows 98 netbios-ssn
389/tcp   open     ldap
445/tcp   open     microsoft-ds (primary domain: MYDOMAIN)
464/tcp   open     kpasswd5?
514/tcp   filtered shell
593/tcp   open     ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open     tcpwrapped
2049/tcp  open     mountd       1-3 (RPC #100005)
3260/tcp  open     tcpwrapped
3268/tcp  open     ldap
3269/tcp  open     tcpwrapped
49152/tcp open     msrpc        Microsoft Windows RPC
49153/tcp open     msrpc        Microsoft Windows RPC
49154/tcp open     msrpc        Microsoft Windows RPC
49155/tcp open     msrpc        Microsoft Windows RPC
49157/tcp open     ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open     msrpc        Microsoft Windows RPC

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.76 seconds
```

Notice how we got more information about a service on the open ports, including the service version. This information is very useful if you are looking for vulnerabilities in certain versions of software.

Specify port ranges

By default, Nmap scans the most common 1,000 ports for each protocol. However, there are 65535 ports that can be used for service, and sometimes you will want to scan very high ports or even individual ports. To do this, the -p flag is used.

Here are a couple of examples. To scan only the port 22, we can use the following command:

```
root@kali:~# nmap -p 22 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 16:23 CET
Nmap scan report for 192.168.5.102
Host is up (0.00034s latency).
PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

To scan a range of ports, use the hyphen to specify the range. For example, to scan ports 50 to 60, we can use the following command:

```
root@kali:~# nmap -p 50-60 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 16:24 CET
Nmap scan report for 192.168.5.102
Host is up (0.74s latency).
PORT   STATE  SERVICE
50/tcp closed re-mail-ck
51/tcp closed la-maint
52/tcp closed xns-time
53/tcp open   domain
54/tcp closed xns-ch
55/tcp closed isi-gl
56/tcp closed xns-auth
57/tcp closed priv-term
58/tcp closed xns-mail
59/tcp closed priv-file
60/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

To exclude certain ports from scanning, use the **--exclude-ports** flag. For example, to exclude ports 1 to 100 from scanning, we would use the following command:

```
root@kali:~# nmap --exclude-ports 1-100 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 16:26 CET
Nmap scan report for 192.168.5.102
Host is up (1.0s latency).
Not shown: 981 closed ports
PORT      STATE    SERVICE
111/tcp   open     rpcbind
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
389/tcp   open     ldap
445/tcp   open     microsoft-ds
464/tcp   open     kpasswd5
514/tcp   filtered shell
593/tcp   open     http-rpc-epmap
636/tcp   open     ldapssl
2049/tcp  open     nfs
3260/tcp  open     iscsi
3268/tcp  open     globalcatLDAP
3269/tcp  open     globalcatLDAPssl
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49157/tcp open     unknown
49158/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 103.70 seconds
```

It is also possible to scan fewer ports than the default 1000. With the **-F** flag, you can reduce the number of scanned ports to 100.

Specify IP address range

Sometimes, you need to scan not a single machine but a whole range of hosts. There are several ways to specify multiple machines:

- specify multiple IP addresses or hostnames - you simply specify IP addresses or hostnames you would like to scan in the command. Here is an example:

```
root@kali:~# nmap -p135 192.168.5.102 192.168.5.11

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 19:40 CET
Nmap scan report for 192.168.5.102
Host is up (0.0012s latency).
PORT    STATE SERVICE
135/tcp open  msrpc

Nmap scan report for 192.168.5.11
Host is up (0.0013s latency).
PORT    STATE SERVICE
135/tcp open  msrpc

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.04 seconds
```

- use CIDR-style addressing - you can use the CIDR notation to specify a range of IP addresses to scan. For example, here is how we would scan the range of IP addresses 192.168.0.0 - 192.168.0.255:

```
root@kali:~# nmap -p135 192.168.5.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 19:43 CET
Nmap scan report for 192.168.5.0
Host is up (0.028s latency).
PORT    STATE    SERVICE
135/tcp filtered msrpc

Nmap scan report for ZyXEL.Home (192.168.5.1)
Host is up (0.15s latency).
PORT    STATE  SERVICE
135/tcp closed msrpc

Nmap scan report for 192.168.5.2
Host is up (0.0051s latency).
PORT    STATE    SERVICE
135/tcp filtered msrpc

Nmap scan report for 192.168.5.3
Host is up (0.0050s latency).
PORT    STATE    SERVICE
135/tcp filtered msrpc
.
.
.
```

- input from list - you can generate a list of machines to scan and pass that filename to Nmap as an argument using the - **iL** option. Entries must be in the format accepted by Nmap on the command line and each entry must be separated by one or more spaces, tabs, or newlines.

Discover if a host is online

Sometimes, you need only to find out whether a host is online and not run a a full port scan. To run a ping scan and disable port scan, the **-sn** flag is used:

```
root@kali:~# nmap -sn 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 16:33 CET
Nmap scan report for 192.168.5.102
Host is up (0.00045s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

Notice how this query took only 0.02 seconds, since no port scans were run.

We can also specify the range of IP addresses that will be checked. One way to do this is by using the CIDR notation. For example, to scan the IP addresses in the range of 192.168.5.0 - 192.168.5.255, we can use the CIDR notation of 192.168.5.0/24.

Sometimes, however, network administrators will make their systems ignore ping requests, which means that you will not be able to discover which hosts are online using the ordinary ping sweep. Nmap does provide some methods to mitigate that, as you will see in the next chapter.

Discover hosts with a TCP SYN ping scan

Many network administrators today block ICMP ping messages, so the ordinary Nmap ping sweep which uses ICMP will not be able to determine if the host is offline or just blocking ICMP messages. However, Nmap also supports a scanning technique called TCP SYN ping scan, which sends a SYN request at a given port on the target host. If the port is open, the target host responds with a TCP SYN/ACK packet indicating that a connection can be established.

The flag **-PS** is used to perform a TCP SYN ping scan. You also need to specify a target port. Here is an example:

```
root@kali:~# nmap -sP -PS21 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 19:16 CET
Nmap scan report for 192.168.5.102
Host is up (0.0014s latency).
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

In the example above we've instructed Nmap to send a TCP SYN packet to the port 21 on the target. The option **-sP** tells Nmap to perform a ping scan only.

Disable ping sweep

When Nmap runs an ordinary scan, it first runs a ping sweep and then follow up with actual port scans (of whatever port ranges specified). If hosts are not responding to a ping, they won't be fully scanned and port scans, version detection, or OS detection will be performed only against the host that are found to be up
You can disable the host discovery process using the **-PN** option. This option forces Nmap to attempt the requested scanning functions against every target IP address specified. Of course, this can significally slow the scanning process, so make sure to list only machines you know are up. Here is an example:

```
root@kali:~# nmap -PN -p 50-90 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 19:25 CET
Nmap scan report for 192.168.5.102
Host is up (1.0s latency).
Not shown: 38 closed ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
88/tcp open  kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
```

In the example above you can see that we've conducted a port scan with the host discovery process disabled.

Determine operating system

Nmap is often used to detect the operating system a host is using. Detecting the operating system of a host is essential to every penetration tester for many reasons - including listing possible security vulnerabilities, determining the available system calls to set the specific exploit payloads, and other OS-dependent tasks. Nmap is known for having the most comprehensive OS fingerprint database and functionality.

Nmap includes a huge a database of the most common operating system fingerprints and can identify hundreds of operating systems based on how they respond to TCP/IP probes. To enable operating system detection, use the **-O** flag. Here is an example:

```
root@kali:~# nmap -O 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 21:16 CET
```

```
Nmap scan report for 192.168.5.102
Host is up (0.30s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
53/tcp    open     domain
80/tcp    open     http
88/tcp    open     kerberos-sec
111/tcp   open     rpcbind
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
389/tcp   open     ldap
445/tcp   open     microsoft-ds
464/tcp   open     kpasswd5
514/tcp   filtered shell
593/tcp   open     http-rpc-epmap
636/tcp   open     ldapssl
2049/tcp  open     nfs
3260/tcp  open     iscsi
3268/tcp  open     globalcatLDAP
3269/tcp  open     globalcatLDAPssl
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49157/tcp open     unknown
49158/tcp open     unknown
Device type: general purpose
Running: Microsoft Windows 7|2012|XP
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.47 seconds
```

In the output above you can see that Nmap has successfully recognized the operating system on the target host (it is indeed Windows Server 2012).

Nmap will even recognize network device (e.g. Cisco devices, Juniper switches):

```
root@kali:~# nmap -O 10.0.0.50

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 21:24 CET
Nmap scan report for 10.0.0.50
Host is up (0.0090s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
```

```
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.64 seconds
```

You can also enable the verbose mode using the **-v** flag to detect additional host information:

```
root@kali:~# nmap -v -O 192.168.5.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 21:26 CET
Initiating Ping Scan at 21:26
Scanning 192.168.5.102 [4 ports]
Completed Ping Scan at 21:26, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:26
Completed Parallel DNS resolution of 1 host. at 21:26, 0.01s elapsed
Initiating SYN Stealth Scan at 21:26
Scanning 192.168.5.102 [1000 ports]
Discovered open port 139/tcp on 192.168.5.102
Discovered open port 111/tcp on 192.168.5.102
Discovered open port 21/tcp on 192.168.5.102
Discovered open port 80/tcp on 192.168.5.102
Discovered open port 3269/tcp on 192.168.5.102
Discovered open port 49158/tcp on 192.168.5.102
Discovered open port 636/tcp on 192.168.5.102
Completed SYN Stealth Scan at 21:29, 135.63s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.5.102
Nmap scan report for 192.168.5.102
Host is up (0.30s latency).
Not shown: 977 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
53/tcp    open     domain
80/tcp    open     http
88/tcp    open     kerberos-sec
111/tcp   open     rpcbind
135/tcp   open     msrpc
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49157/tcp open     unknown
49158/tcp open     unknown
Device type: general purpose
Running: Microsoft Windows 7|2012|XP
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.21 seconds
           Raw packets sent: 1693 (76.130KB) | Rcvd: 1032 (41.650KB)
```