

Experiment 09

Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.

Roll No.	37
Name	Mikil Lalwani
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO4: Use tools like sniffers, port scanners and other related tools for analyzing packets in a network.

Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.

Theory-

What is Nmap?

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and find its open ports and services.

Why use Nmap?

There are a number of reasons why security pros prefer Nmap over other scanning tools. First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

Other features of Nmap include-

- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.
- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

Downloading and Installing NMAP

1. Go to the Nmap download page (<https://nmap.org/download.html>) and download the latest stable version.

Microsoft Windows binaries

```
nmap -T4 -A -F scanner.nmap.org
Starting Nmap 7.01 ( https://nmap.org ) at 2015-07-24 11:52 CEST
Nmap scan report for 127.0.0.1
Host is up (0.007s latency).
Not shown: 998 services closed by port
PORT      STATE    SERVICE
22/tcp    open     ssh
22/tcp    open     ssh-hostkey
| ssh-hostkey:
|   1024
|   ac:00:a0:1a:b2:f#ccc:5f

```

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the [RPM](#) package management system for quick and easy binary package installation. We have written a detailed [guide to installing our RPM packages](#), though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.93-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.93-1.x86_64.rpm
```

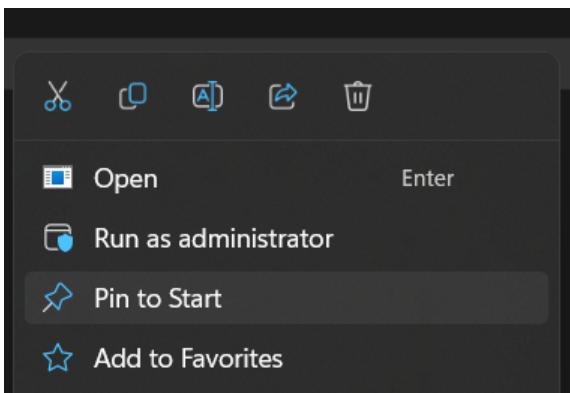
You can also download and install the RPMs yourself:

Latest stable release:
x86-64 (64-bit Linux) [Nmap](#) RPM: [nmap-7.93-1.x86_64.rpm](#)
x86-64 (64-bit Linux) [Ncat](#) RPM: [ncat-7.93-1.x86_64.rpm](#)
x86-64 (64-bit Linux) [Nping](#) RPM: [nping-0.7.93-1.x86_64.rpm](#)
Optional [Zenmap GUI](#) (all platforms): [zenmap-7.93-1.noarch.rpm](#)
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): [nmap-7.93-1.src.rpm](#)

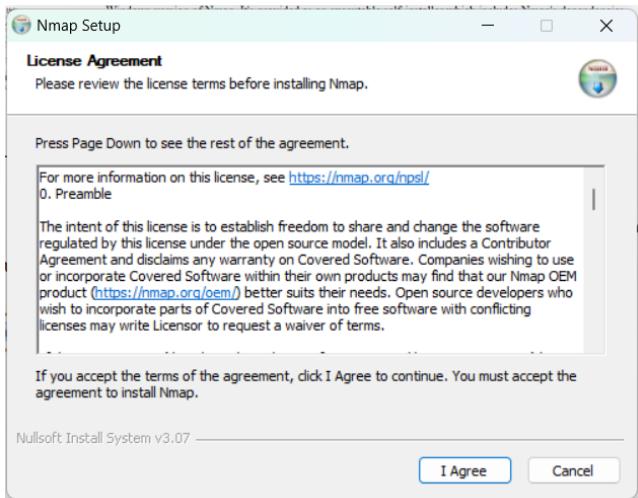
Mac OS X Binaries

Nmap binaries for Apple macOS (x86-64) are distributed as a disk image file containing an installer. The installer allows installing Nmap, Zenmap, Ncat, and Ndifff. The programs have been tested on Mac OS X 10.9 and later. See the [Mac OS X Nmap install page](#) for more details. Users of PowerPC (PPC) Mac machines, which Apple ceased selling in 2006, should see [this page instead](#) for support information.

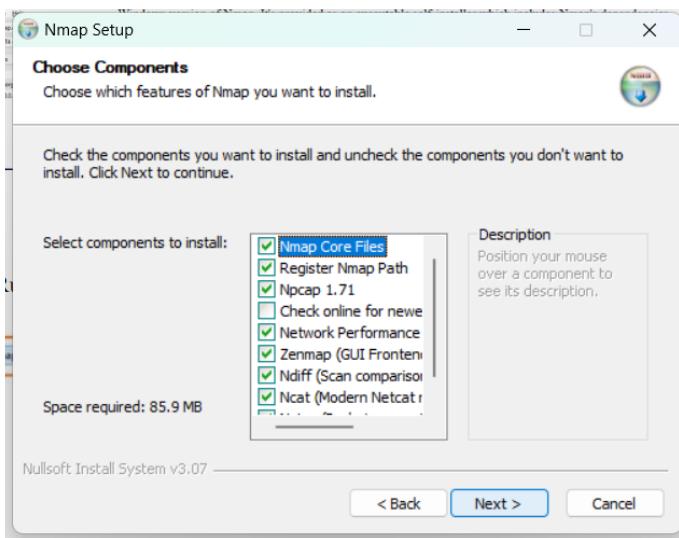
2. Go to the location where the file is downloaded. Right-click on the EXE file and click “Run as administrator.”



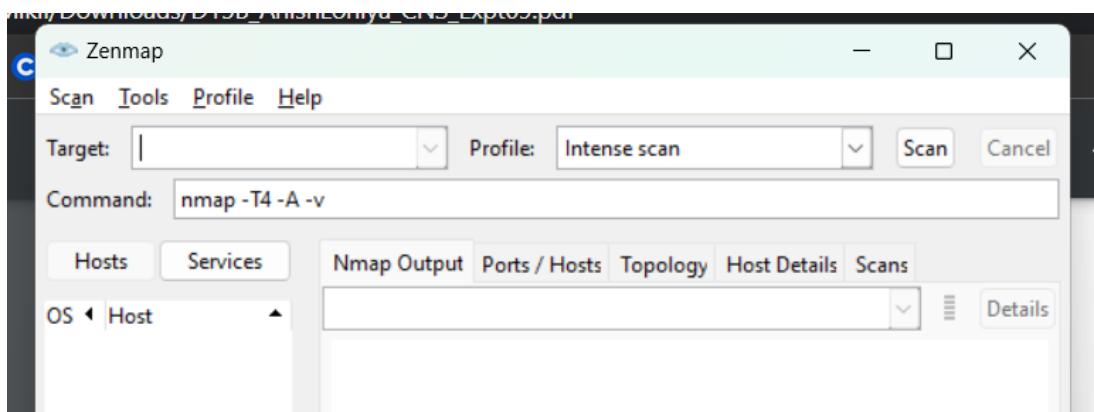
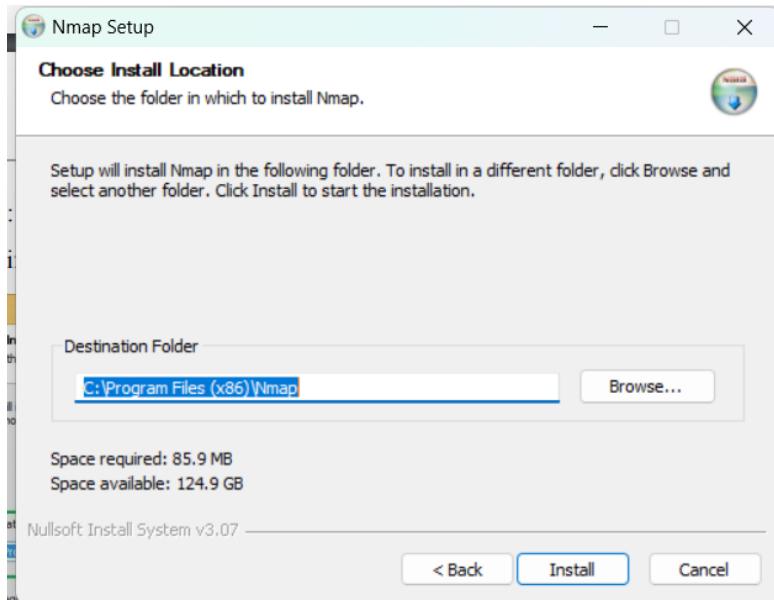
3. It will start the installation process, and accept the license agreement.



4. You can choose what components to install, but it would be good to install all of them.



5. By default, it will install under C:\Program Files (x86)\Nmap but feel free to change it if needed.



Scanning Ports

Scanning Host and IP Address

To scan hosts or their ip addresses, enter the following in the textbox for command:

```
nmap www.google.com
```

Zenmap interface showing the results of a scan on 127.0.0.1. The Nmap Output tab displays the following scan report:

```
nmap 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-04
21:12 India Standard Time
Nmap scan report for kubernetes.docker.internal (127.0.0.1)
Host is up (0.00067s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
808/tcp   open  cproxy-ssh
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
8080/tcp  open  http-proxy
9080/tcp  open  gRPC

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Zenmap interface showing the results of a scan on www.google.com. The Nmap Output tab displays the following scan report:

```
nmap www.google.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-04
21:13 India Standard Time
Nmap scan report for www.google.com (142.250.182.228)
Host is up (0.0044s latency).
rDNS record for 142.250.182.228: bom07s29-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.25 seconds
```

Performing OS fingerprinting

Determining 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 for many other OS-dependent tasks. Nmap is known for having the most comprehensive OS fingerprint database and functionality.

`nmap -O -v scanme.nmap.org`

```

Completed SYN Stealth Scan at 21:13, 5.27s elapsed
(1000 total ports)
Initiating OS detection (try #1) against
scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org
(45.33.32.156)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9292/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Linux 2.6.32 (91%), Linux 3.5
(91%), Linux 4.2 (91%), Linux 4.4 (91%), Synology
DiskStation Manager 5.1 (91%), WatchGuard Fireware
11.8 (91%), Linux 2.6.35 (90%), Linux 3.10 (90%),
Linux 2.6.32 or 3.10 (90%), Linux 2.6.39 (90%)
No exact OS matches for host (test conditions non-
ideal).
Uptime guess: 36.039 days (since Mon Aug 29 20:18:15
2022)
Network Distance: 18 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect
results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 17.41
seconds
Raw packets sent: 1071 (49.270KB) | Rcvd:
1060 (44.414KB)

```

Ping Scan

One of the most basic functions of Nmap is to identify active hosts on your network.

Nmap does this by using a ping scan. This identifies all of the IP addresses that are currently online without sending any packers to these hosts. This command then returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands (see below) to investigate them further.

`nmap -sn 127.0.0.1`

```

Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-04
21:14 India Standard Time
Nmap scan report for kubernetes.docker.internal
(127.0.0.1)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.14
seconds

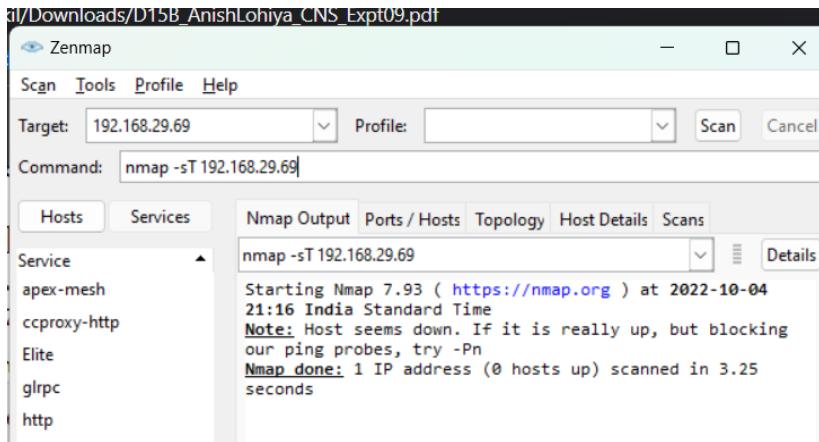
```

TCP Port Scan

This command will initiate a TCP connect scan against the target host. A TCP connect

scan is the default scan performed if a TCP SYN scan is not possible. This type of scan requests that the underlying operating system try to connect with the target host/port using the ‘connect’ system call.

```
nmap -sT 192.168.29.69
```



UDP Port Scan

```
nmap -sU -T4 scanme.nmap.org
```

```
ubuntu@ubuntu:~$ sudo nmap -sU -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-04 21:22 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.024s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
123/udp  open   ntp

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
ubuntu@ubuntu:~$
```

Nmap scan specific udp port

```
nmap -p 123 -sU linuxhint.com
```

```
ubuntu@ubuntu:~$ sudo nmap -p 123 -sU linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-04 21:23 IST
Nmap scan report for linuxhint.com (172.64.174.28)
Host is up (0.00036s latency).
Other addresses for linuxhint.com (not scanned): 172.64.175.28

PORT      STATE      SERVICE
123/udp  open|filtered  ntp

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
ubuntu@ubuntu:~$
```

Conclusion:

Thus we understand how to use Nmap with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.