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.	70
Name	MAYURI SHRIDATTA YERANDE
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

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:

- Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

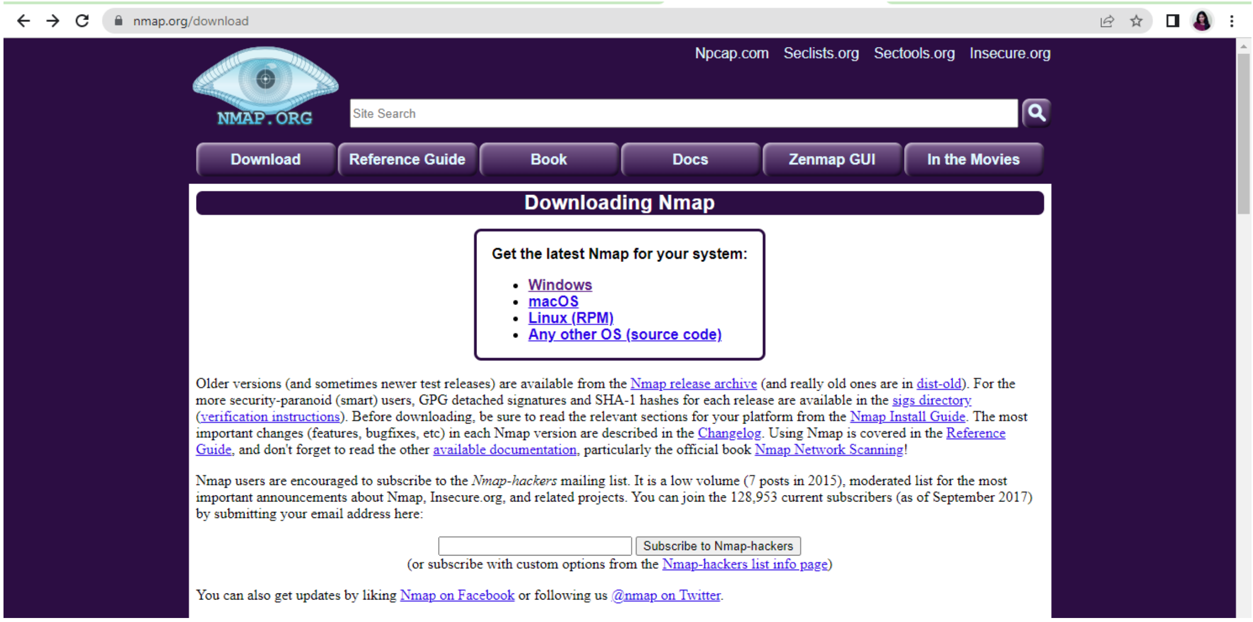
Nmap is:

- **Flexible:** Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.
- **Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable:** Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- **Easy:** While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- **Free:** The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.

Nmap is defined as a tool that can detect or diagnose services that are running on an Internet-connected system by a network administrator in their networked system used to identify potential security flaws. It is used to automate redundant tasks, such as monitoring the service.

Installation:

Download Link for Windows: https://nmap.org/download



Downloading Nmap

Get the latest Nmap for your system:

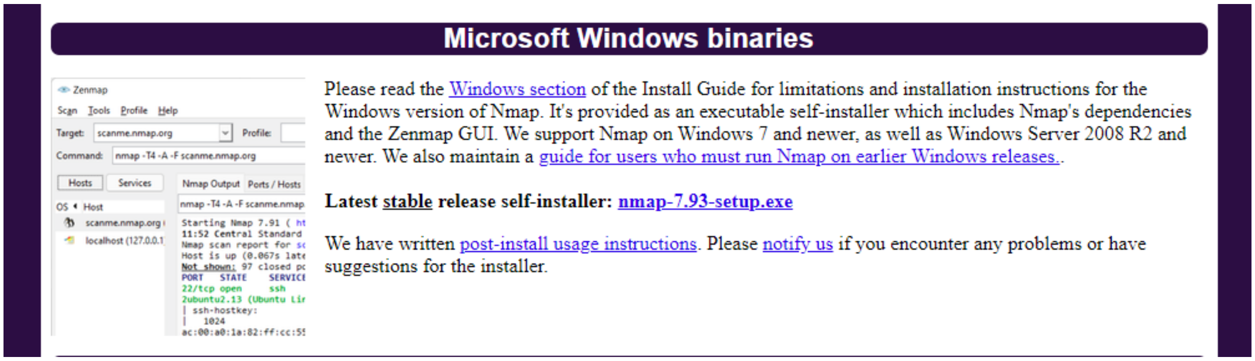
- Windows
- macOS
- Linux (RPM)
- Any other OS (source code)

Older versions (and sometimes newer test releases) are available from the Nmap release archive (and really old ones are in dist-old). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the sigs directory (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the Nmap Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the official book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

(or subscribe with custom options from the Nmap-hackers list info page)

You can also get updates by liking Nmap on Facebook or following us @nmap on Twitter.



Microsoft Windows binaries

Target: scanme.nmap.org

Profile:

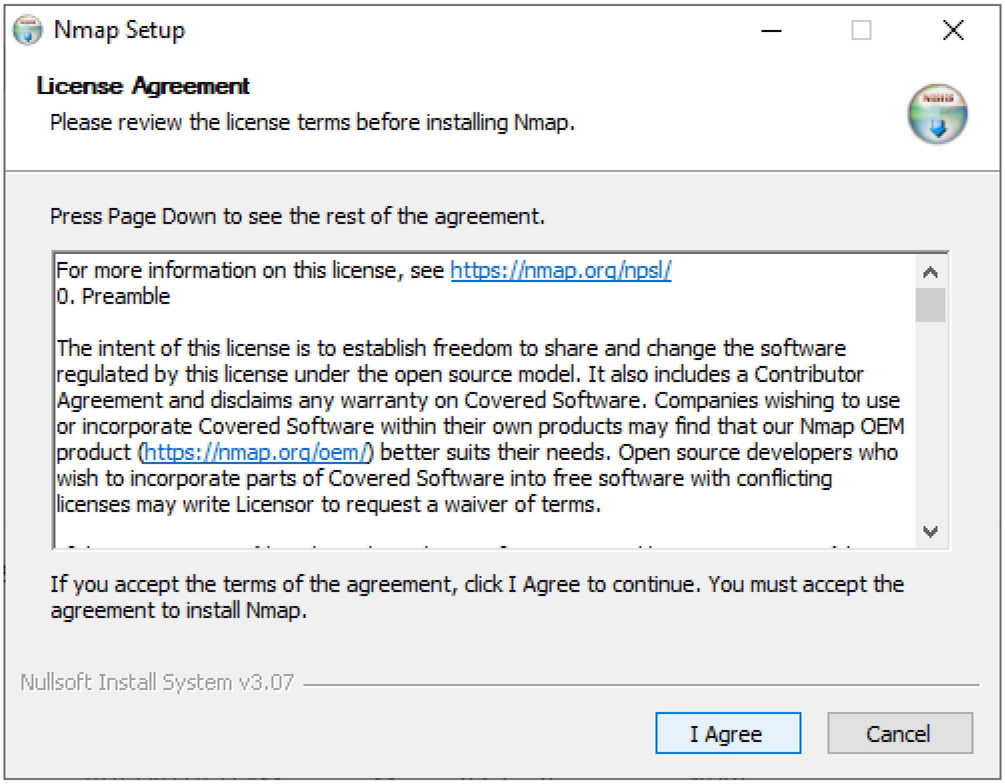
Command: nmap -T4 -A -F scanme.nmap.org

```
nmap -T4 -A -F scanme.nmap
Starting Nmap 7.91 ( ht
11:52 Central Standard
Nmap scan report for sc
Host is up (0.067s late
Not shown: 97 closed pc
PORT     STATE    SERVICE
22/tcp open       ssh
2ubuntu2.13 (Ubuntu Lir
| ssh-hostkey:
|   1024
ac:00:a0:1a:82:ff:cc:55
```

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

Latest stable release self-installer: nmap-7.93-setup.exe

We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.



License Agreement

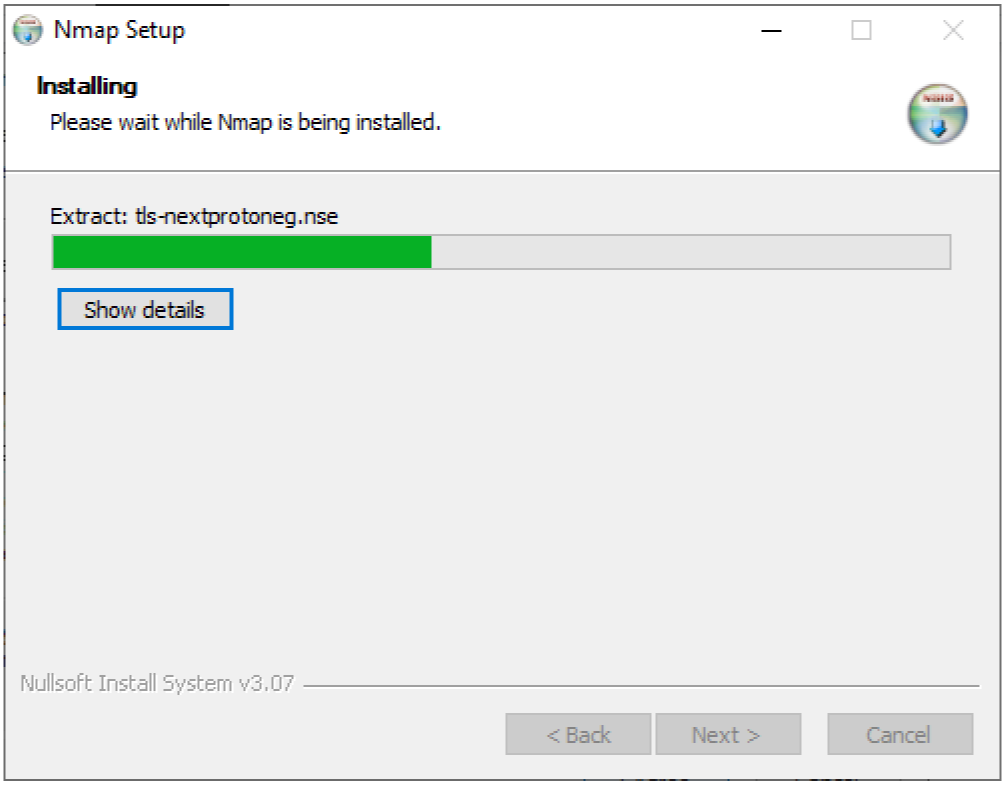
Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

For more information on this license, see https://nmap.org/npsl/
0. Preamble

The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Companies wishing to use or incorporate Covered Software within their own products may find that our Nmap OEM product (https://nmap.org/oem/) better suits their needs. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.

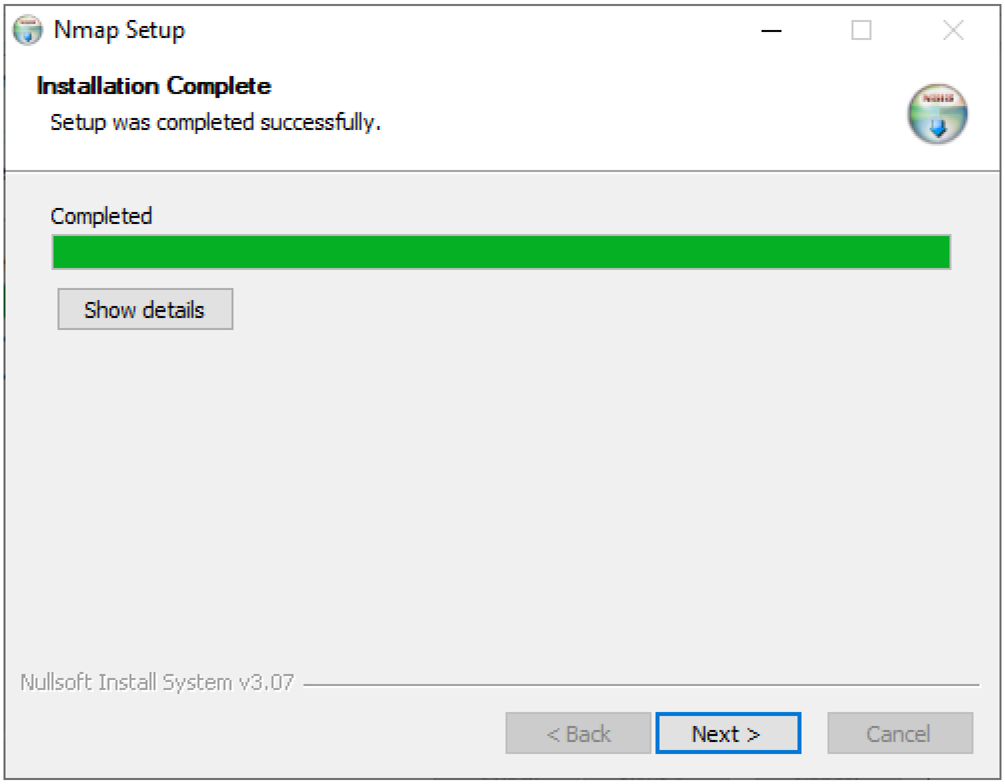
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.



Installing

Please wait while Nmap is being installed.

Extract: tls-nextprotoneg.nse

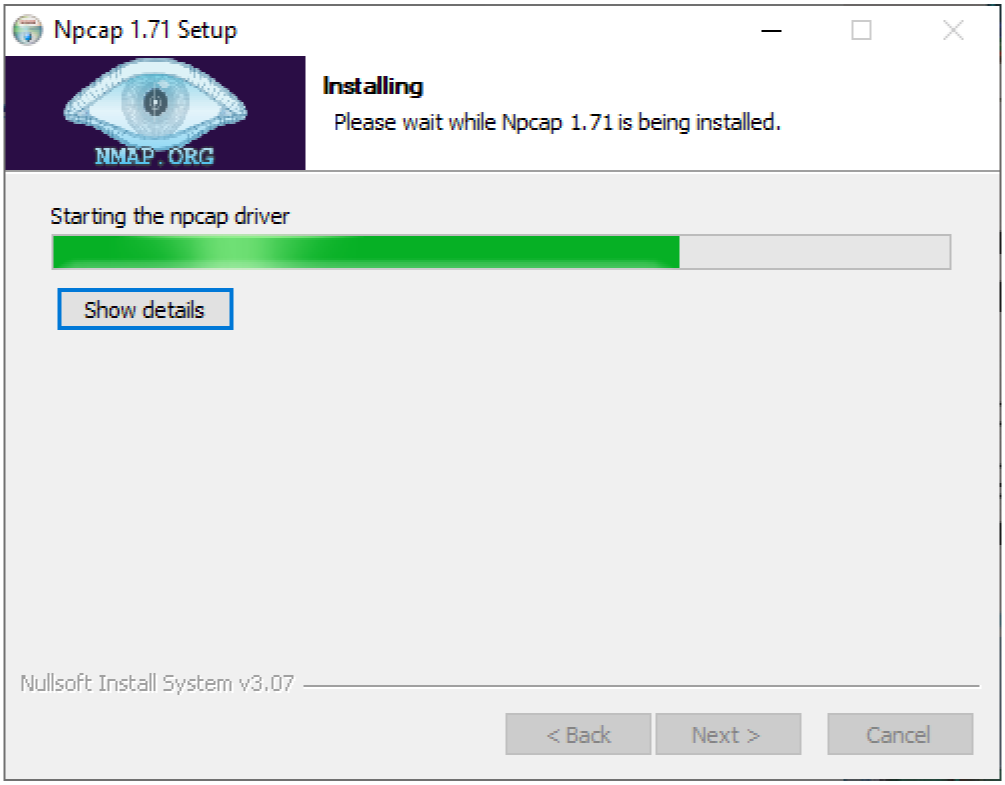


Nmap Setup

Installation Complete

Setup was completed successfully.

Completed

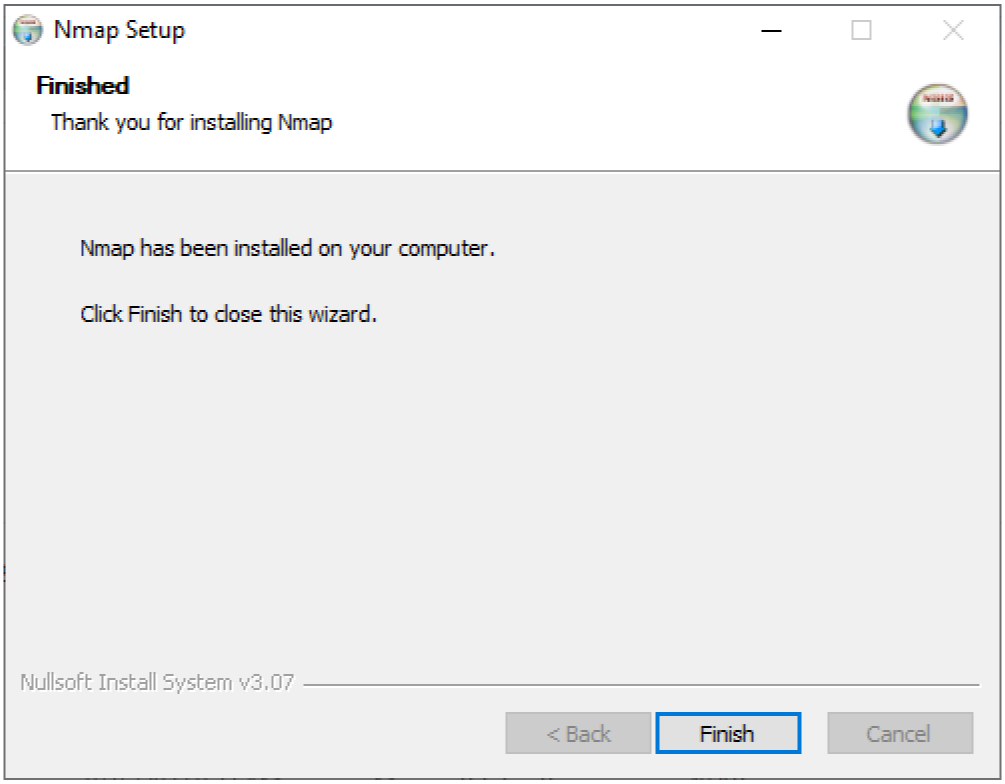


Npcap 1.71 Setup

Installing

Please wait while Npcap 1.71 is being installed.

Starting the npcap driver



Finished

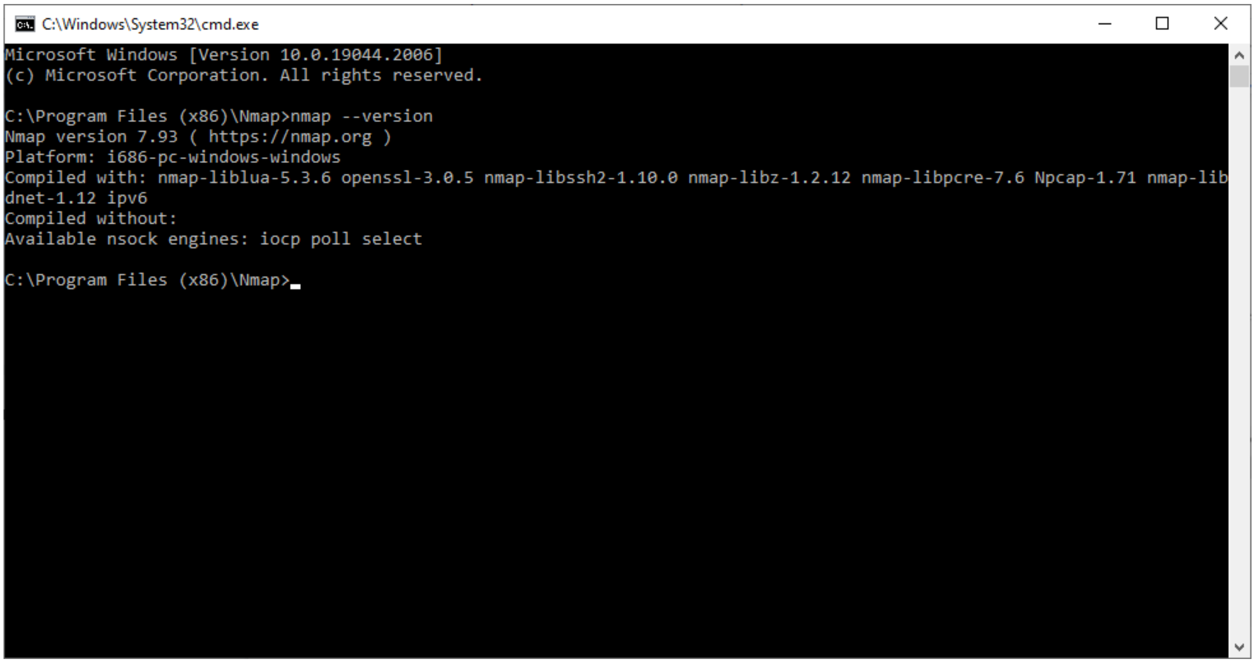
Thank you for installing Nmap

Nmap has been installed on your computer.

Click Finish to close this wizard.

Nmap and Npcap are successfully installed.

- Open command prompt and type the command ‘nmap –version’ to check for the proper installation of the nmap.

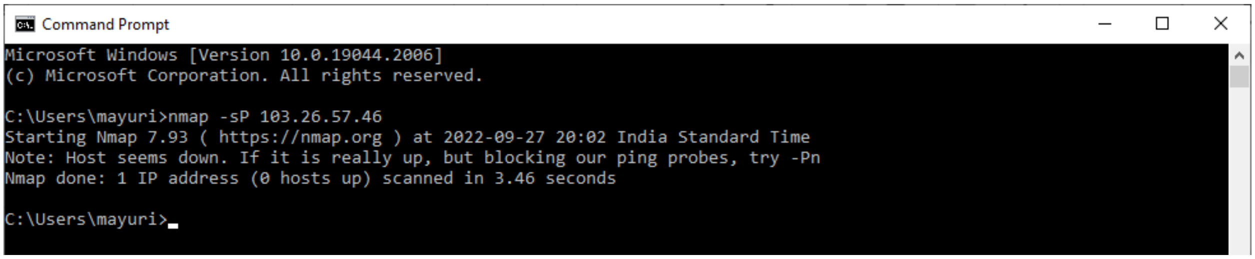


```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Nmap>nmap --version
Nmap version 7.93 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.6 openssl-3.0.5 nmap-libssh2-1.10.0 nmap-libz-1.2.12 nmap-libpcre-7.6 Npcap-1.71 nmap-lib
dnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select

C:\Program Files (x86)\Nmap>
```

Ping scanning: Scans the list of devices up and running on a given subnet.

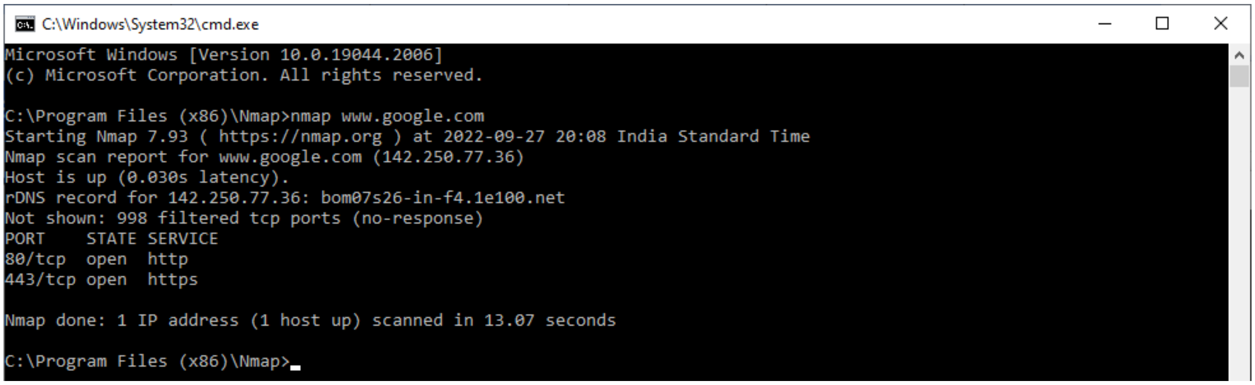


```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mayuri>nmap -sP 103.26.57.46
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:02 India Standard Time
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 3.46 seconds

C:\Users\mayuri>
```

Single Port Scanning: Scans a single host for 1000 well-known ports. These ports are the ones used by popular services like SQL, SNTP, apache, and others.



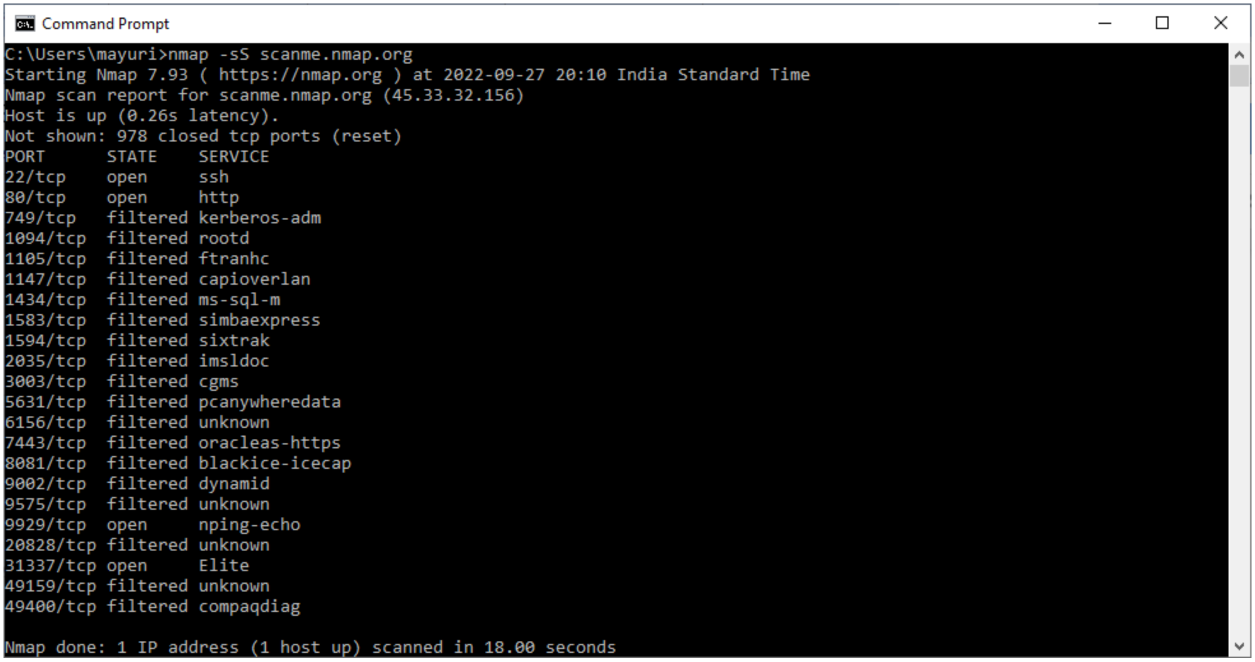
```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Nmap>nmap www.google.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:08 India Standard Time
Nmap scan report for www.google.com (142.250.77.36)
Host is up (0.030s latency).
rDNS record for 142.250.77.36: bom07s26-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 13.07 seconds

C:\Program Files (x86)\Nmap>
```

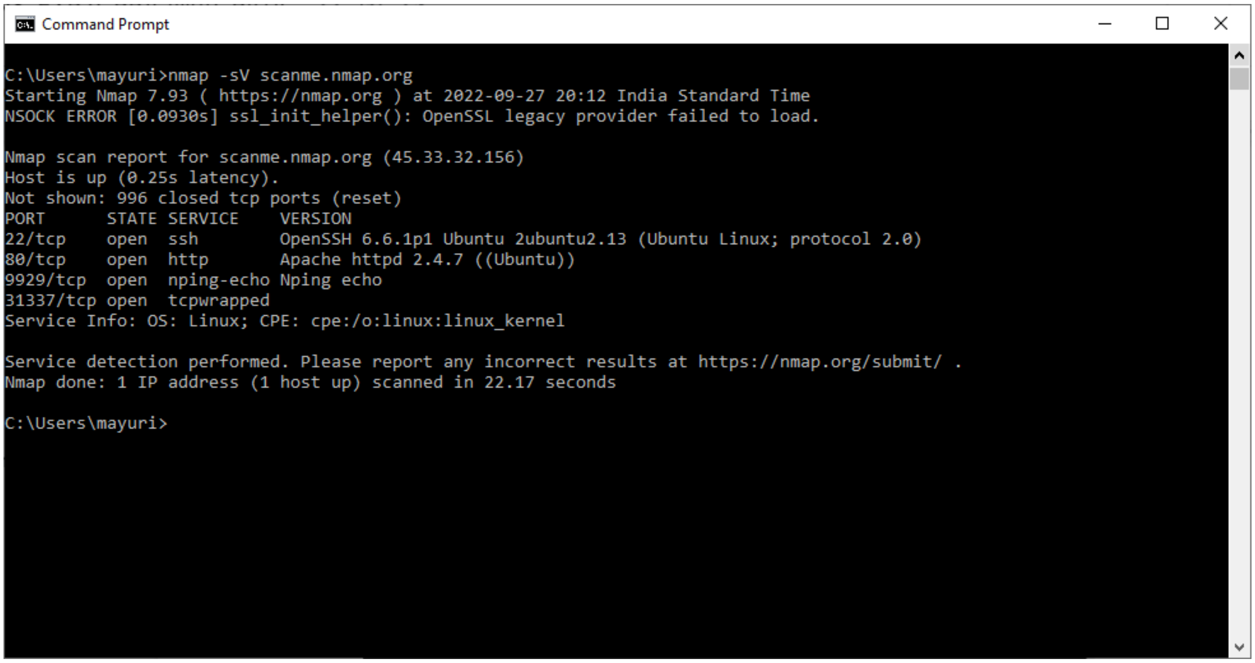
Stealth scan: Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection. However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.



```
C:\Users\mayuri>nmap -sS scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:10 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
749/tcp   filtered kerberos-adm
1094/tcp  filtered rootd
1105/tcp  filtered ftranhc
1147/tcp  filtered capioverlan
1434/tcp  filtered ms-sql-m
1583/tcp  filtered simbaexpress
1594/tcp  filtered sixtrak
2035/tcp  filtered imsldoc
3003/tcp  filtered cgms
5631/tcp  filtered pcanywheredata
6156/tcp  filtered unknown
7443/tcp  filtered oracleas-https
8081/tcp  filtered blackice-icecap
9002/tcp  filtered dynamid
9575/tcp  filtered unknown
9929/tcp  open     nping-echo
20828/tcp filtered unknown
31337/tcp open     Elite
49159/tcp filtered unknown
49400/tcp filtered compaqdiag

Nmap done: 1 IP address (1 host up) scanned in 18.00 seconds
```

Version scanning: Finding application versions is a crucial part in penetration testing. To do a version scan, use the ‘-sV’ command. Nmap will provide a list of services with its versions.



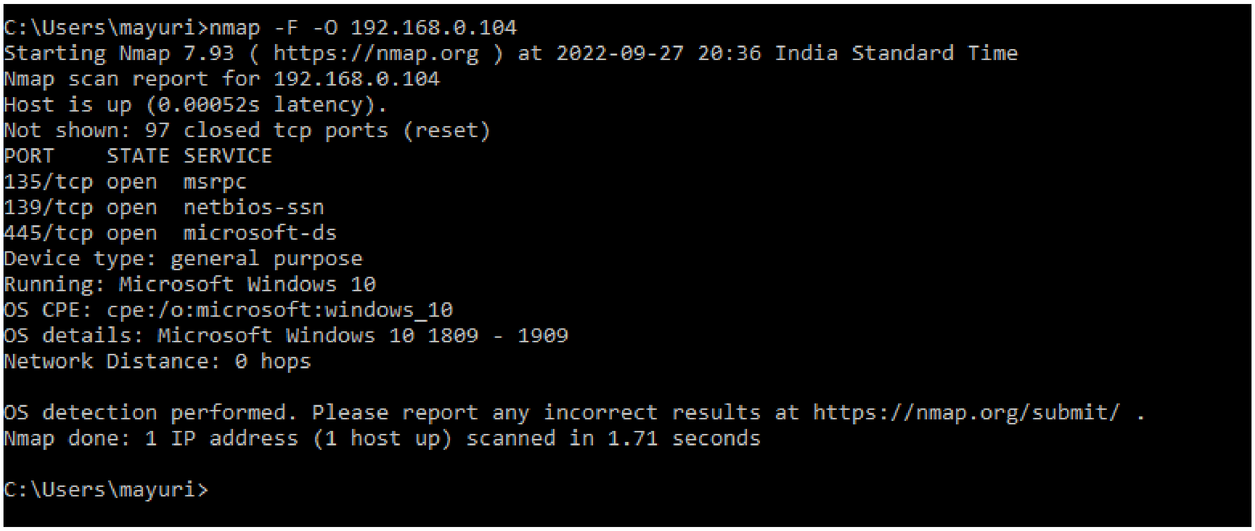
```
C:\Users\mayuri>nmap -sV scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:12 India Standard Time
NSOCK ERROR [0.0930s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: 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 22.17 seconds

C:\Users\mayuri>
```

OS Fingerprinting Scanning: In addition to the services and their versions, Nmap can provide information about the underlying operating system using TCP/IP fingerprinting. Nmap will also try to find the system uptime during an OS scan.

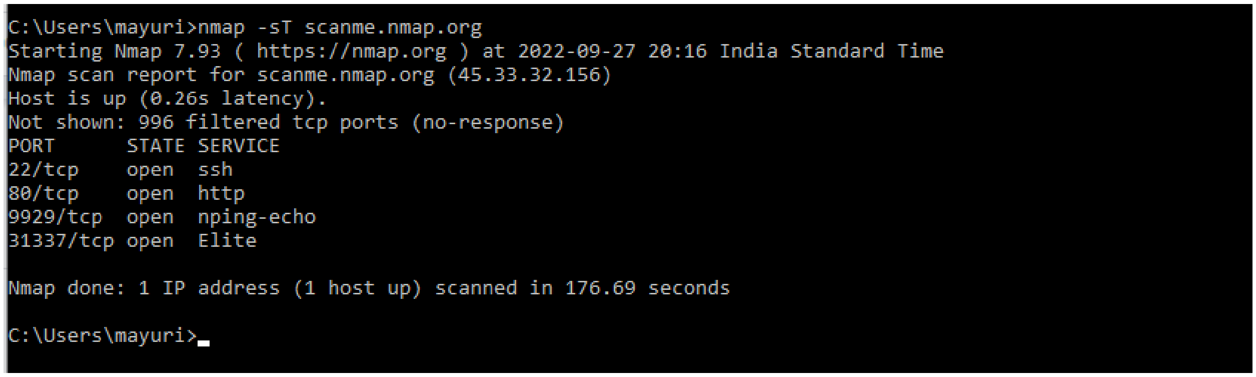


```
C:\Users\mayuri>nmap -F -O 192.168.0.104
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:36 India Standard Time
Nmap scan report for 192.168.0.104
Host is up (0.00052s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds

C:\Users\mayuri>
```

TCP port Scanning: CP scanning is SYN scans. This involves creating a partial connection to the host on the target port by sending a SYN packet and then evaluating the response from the host. If the request packet is not filtered or blocked by a firewall, then the host will reply by sending a SYN/ACK packet if the port is open or a RST packet if the port is closed.

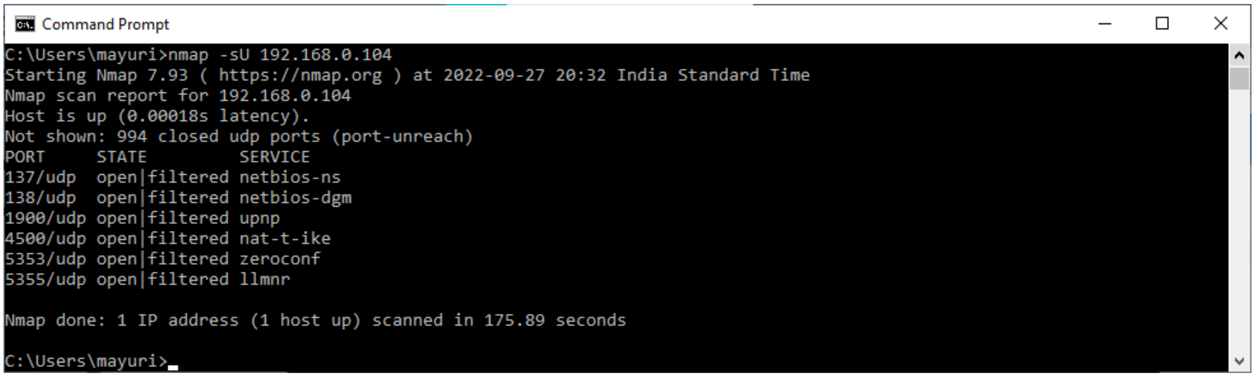


```
C:\Users\mayuri>nmap -sT scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:16 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 176.69 seconds

C:\Users\mayuri>
```

UDP port scanning: UDP scans, like TCP scans, send a UDP packet to various ports on the target host and evaluate the response packets to determine the availability of the service on the host. As with TCP scans, receiving a response packet indicates that the port is open.



```
C:\Users\mayuri>nmap -sU 192.168.0.104
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 20:32 India Standard Time
Nmap scan report for 192.168.0.104
Host is up (0.00018s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 175.89 seconds

C:\Users\mayuri>
```

Conclusion: In this experiment, we have successfully downloaded and installed it in our system. We also have successfully implemented various scans such as scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.