# Security Lab
# Lab Assignment No. 10

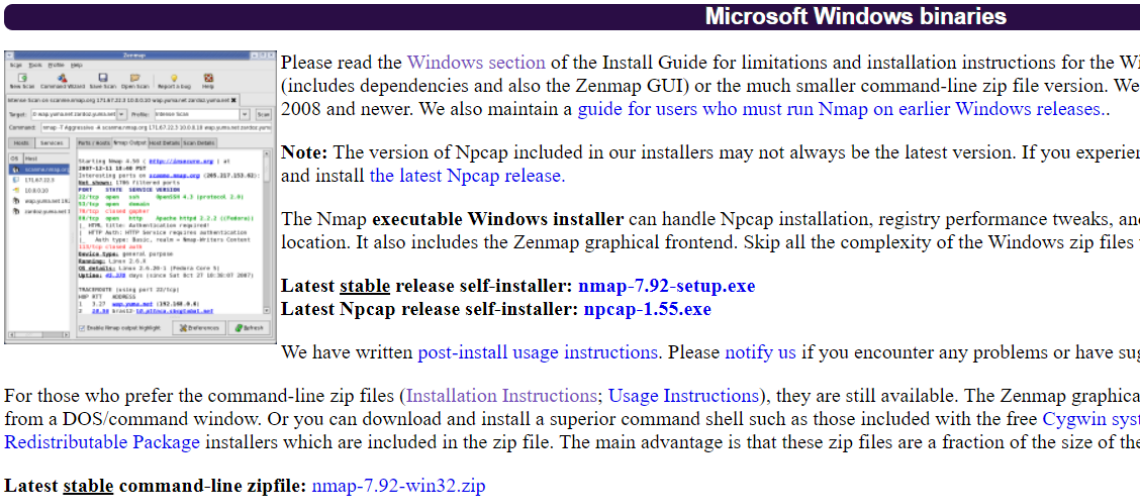
**Aim**: Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

Nmap (network mapper) is the leading security scanning tool used by testers (penetration testers/ethical hackers). Nmap is a port listener. It can listen for responses in the process. It can determine whether a port is open or closed or filtered in one way or another by the firewall (a system designed to deny unauthorized users access to or from a private network).
It's a flexible and versatile tool, meaning it can adapt/change to different activities and functions.
Uses of Nmap tool:

1. Network administrator(s) can identify all devices that are running/accessing their systems.
2. An administrator can identify all the hosts, computers connected to their network, including the services that they offer.
3. An administrator can scan all the open ports (communication endpoint), giving security a priority, that is, security threat detections.
4. An administrator can scan/monitor a single host (a computer connected to the organization network) or thousands of devices connected.

## 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**

Please read the Windows section of the Install Guide for limitations and installation instructions for the Wi
(includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We
2008 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

**Note:** The version of Npcap included in our installers may not always be the latest version. If you experier
and install the latest Npcap release.

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, an
location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files

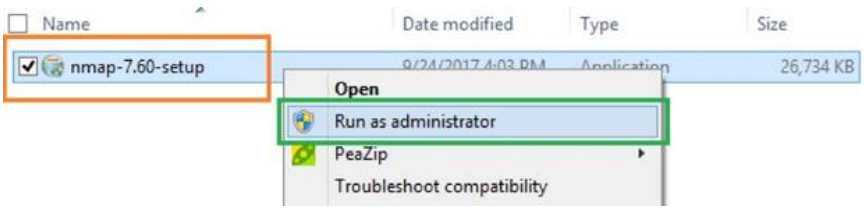
**Latest stable release self-installer: nmap-7.92-setup.exe**
**Latest Npcap release self-installer: npcap-1.55.exe**

We have written post-install usage instructions. Please notify us if you encounter any problems or have su

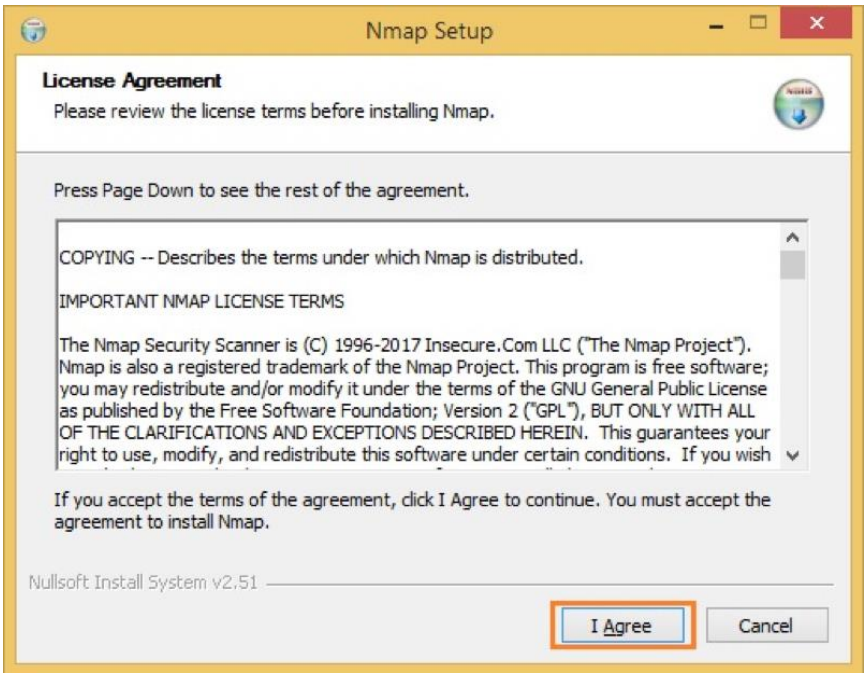
For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), they are still available. The Zenmap graphica
from a DOS/command window. Or you can download and install a superior command shell such as those included with the free Cygwin syst
Redistributable Package installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the

**Latest stable command-line zipfile:** nmap-7.92-win32.zip

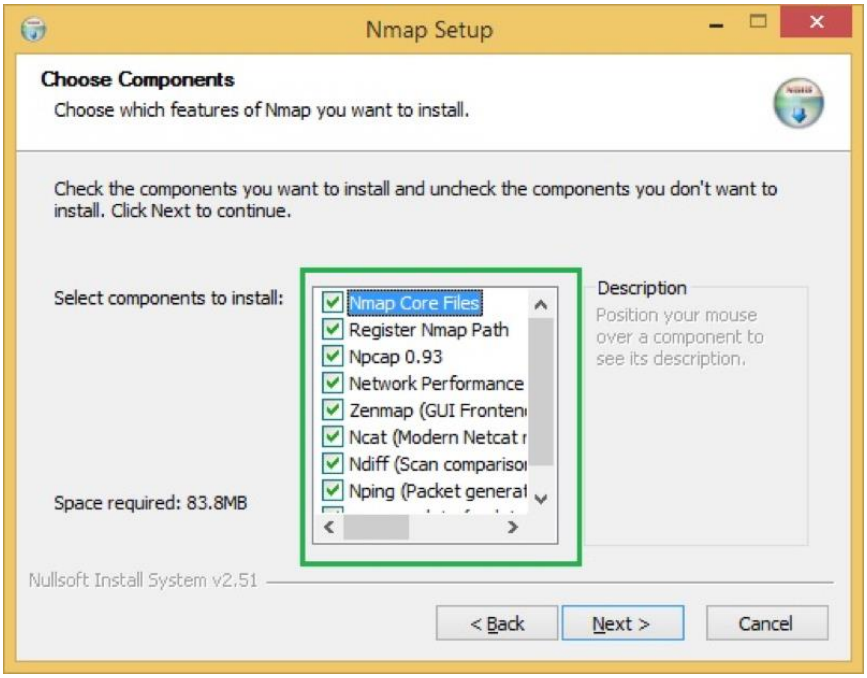
2. Go to the location where the file is downloaded. Right-click on the EXE file and click "Run as administrator."



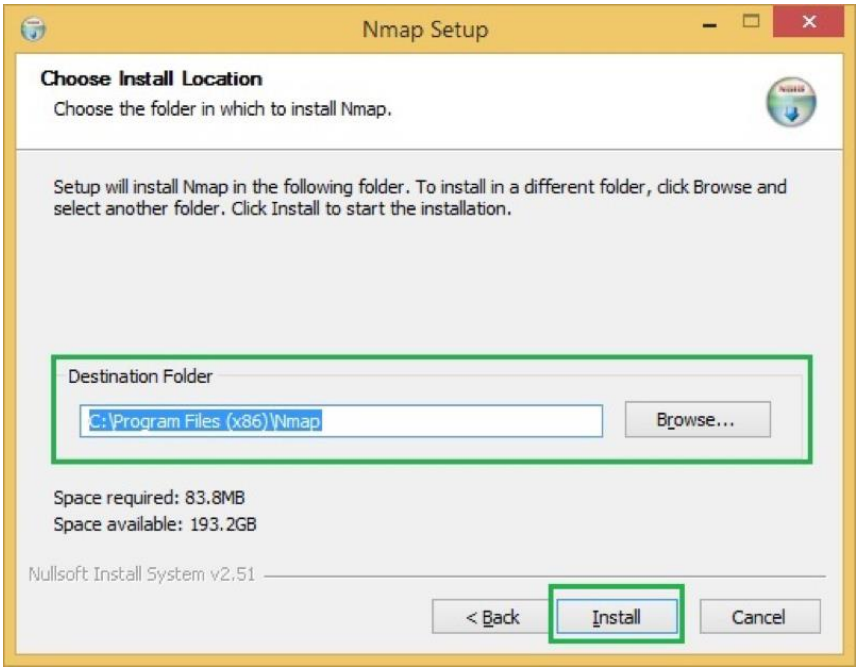

3. It will start the installation process, and accept the license agreement.



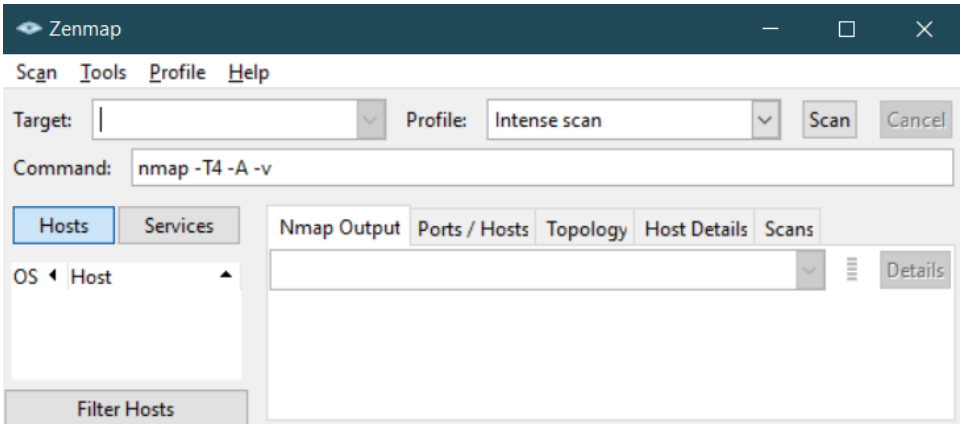

4. You can choose what components to install, but it would be good to install all of them.




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

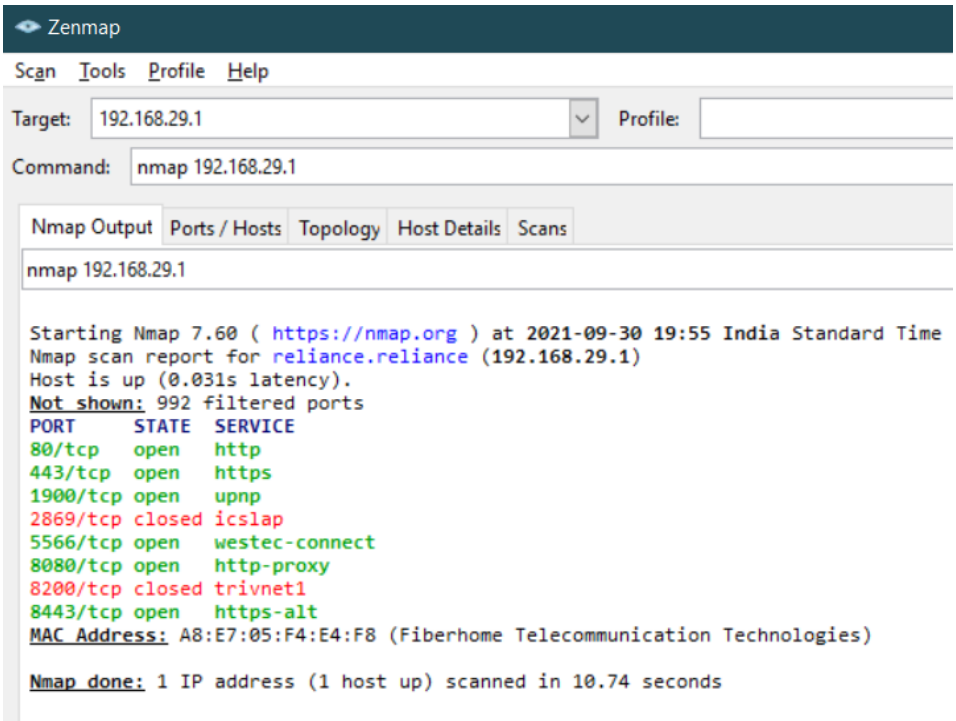



6. It will start installing NMAP and once done; you will get confirmation. NMAP is successfully installed.



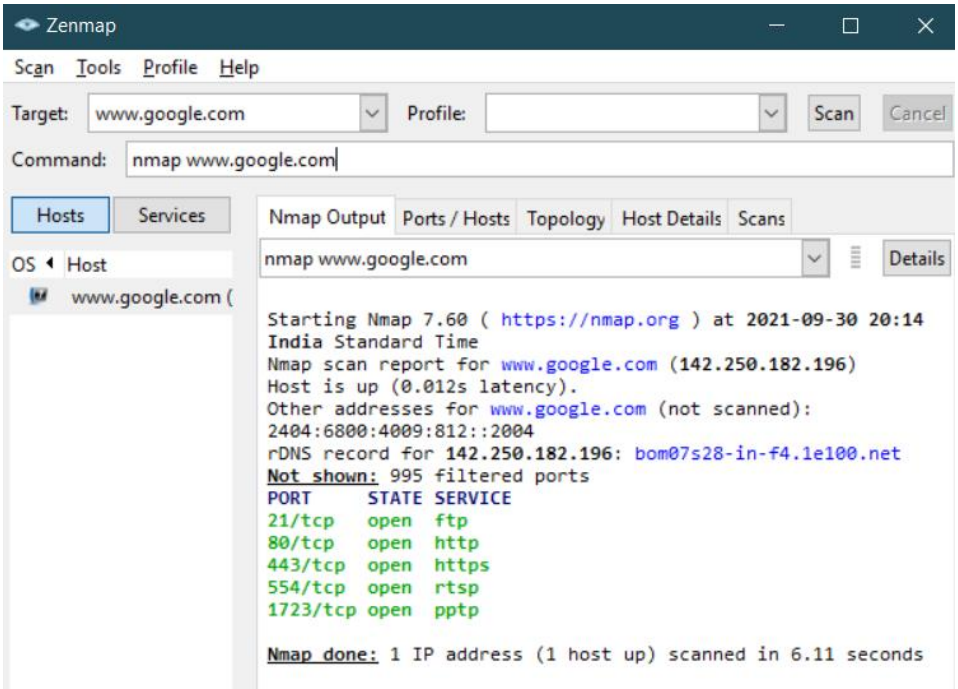

**Scanning open ports**

To scan Nmap ports on a remote system, enter the following in the textbox for command:
***nmap 192.168.29.1***




**Scanning HOST AND IP ADDRESS**

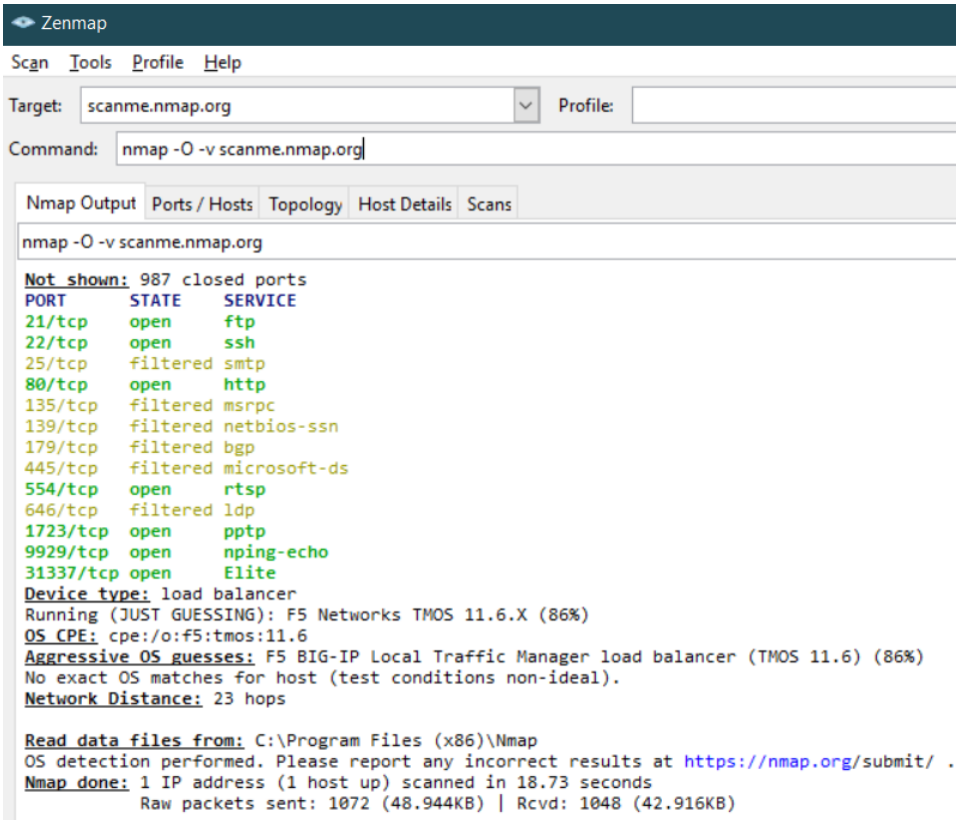
To scan hosts or their ip addresses, enter the following in the textbox for command:
***nmap www.google.com***




**Performing OS fingerprinting of a host**

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***

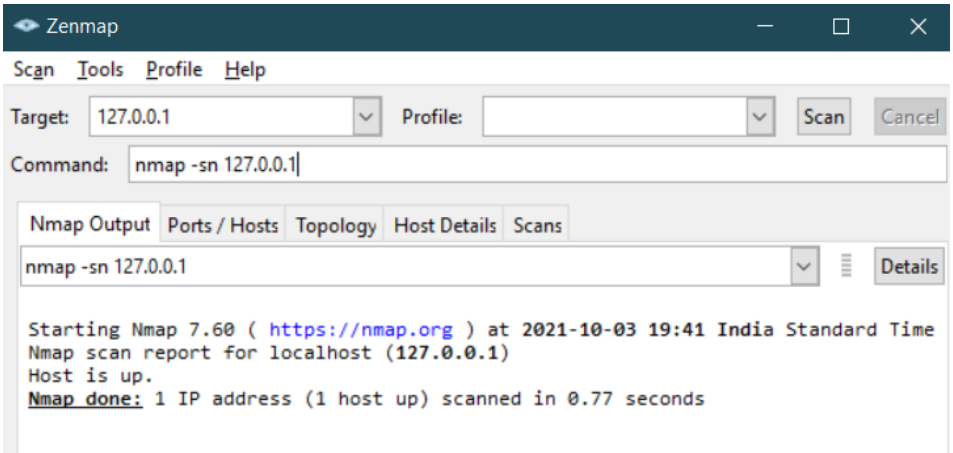



**Ping Scan**

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.

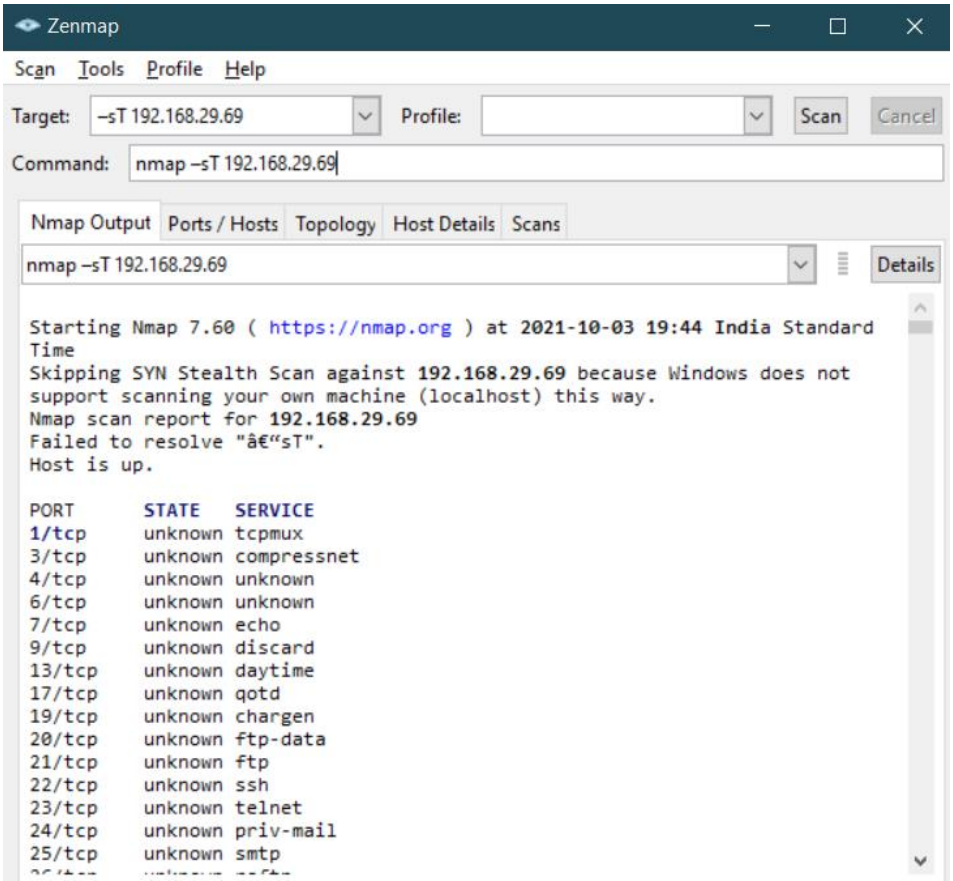
***nmap -sn 127.0.0.1***



**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.

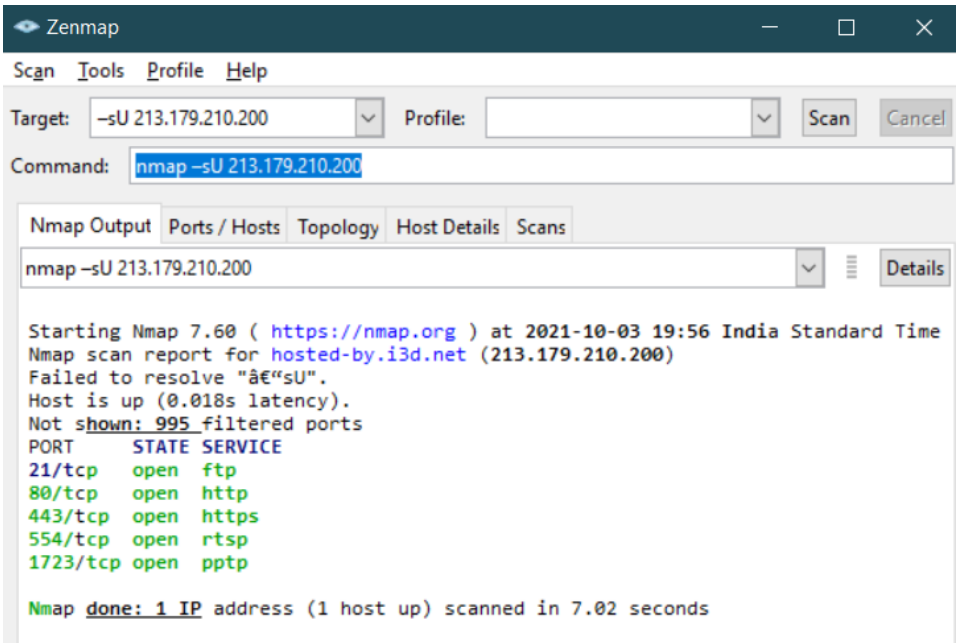
***nmap –sT 192.168.29.69***




**UDP Port Scan**

This command will initiate a UDP port scan against the target host. A UDP scan sends a UDP packet to the target port(s). If a response is received, the port is classified as Open. If no response is received after multiple transmissions, the port is classified as open/filtered.

***nmap –sU 213.179.210.200***




**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.