Expt\_09\_D15B Internet Security Lab Roll No: 37



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.

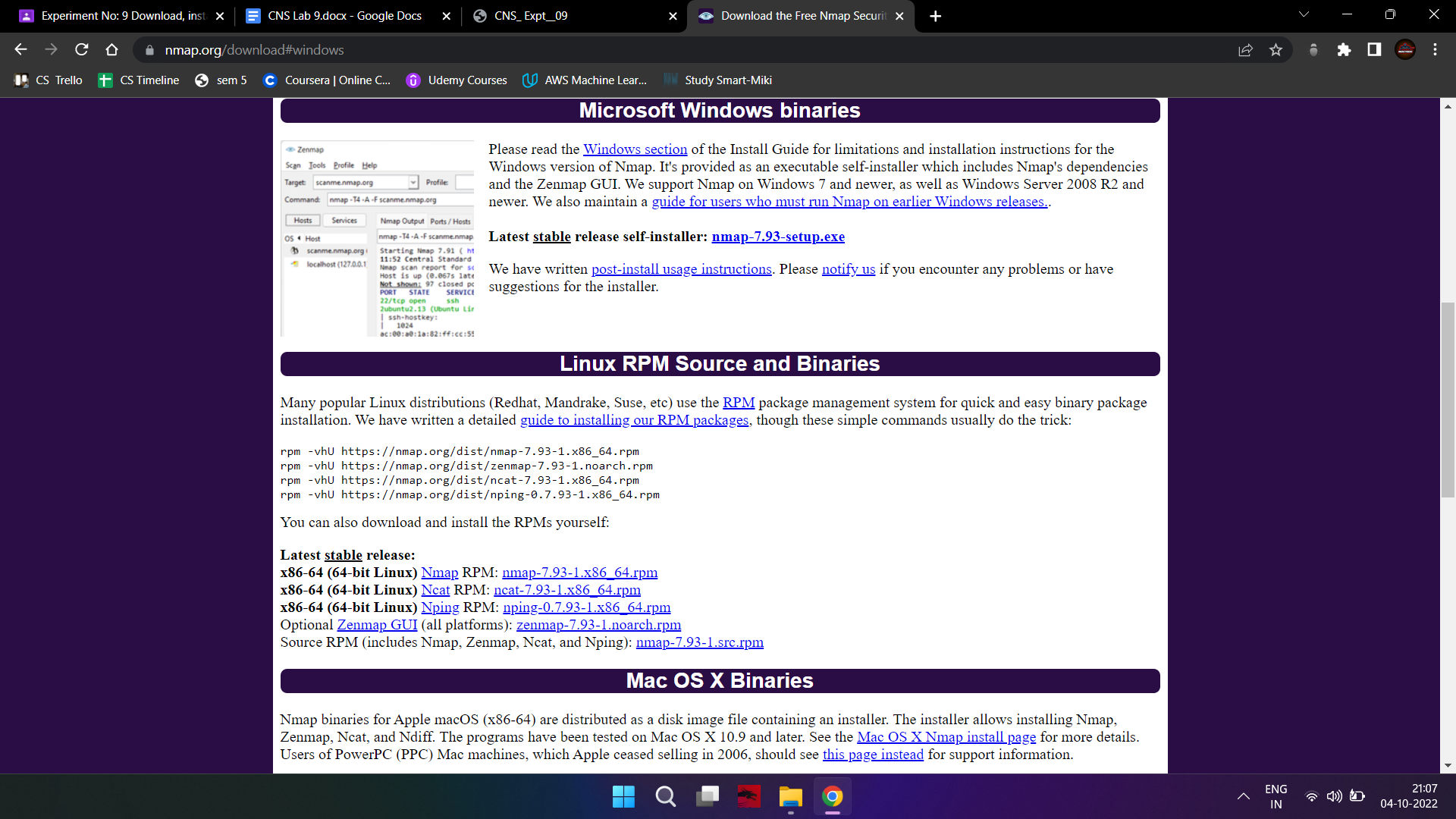
Other features of Nmap include-

* 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

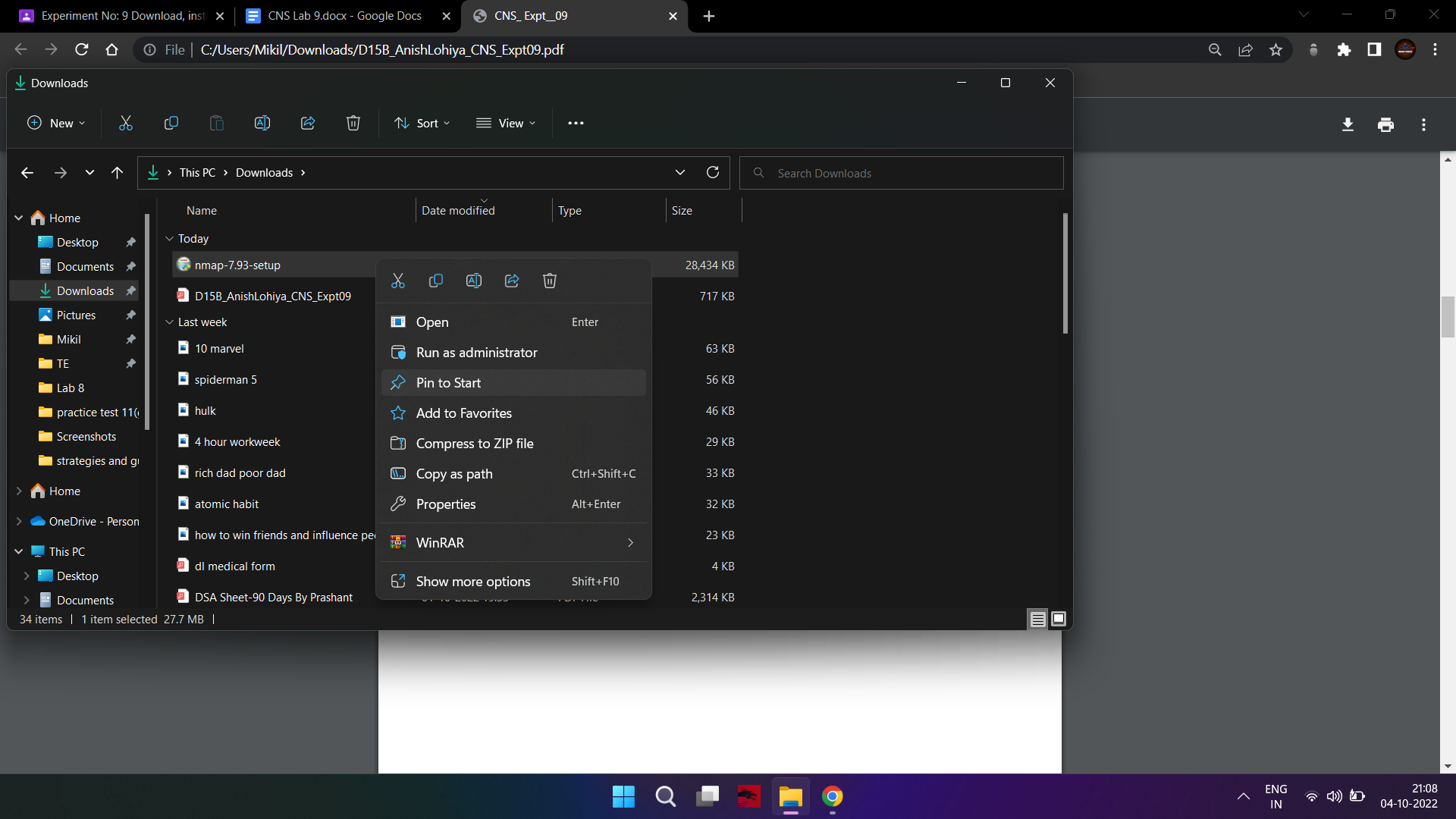
1. Go to the Nmap download page (https://nmap.org/download.html) and

download the latest stable version.

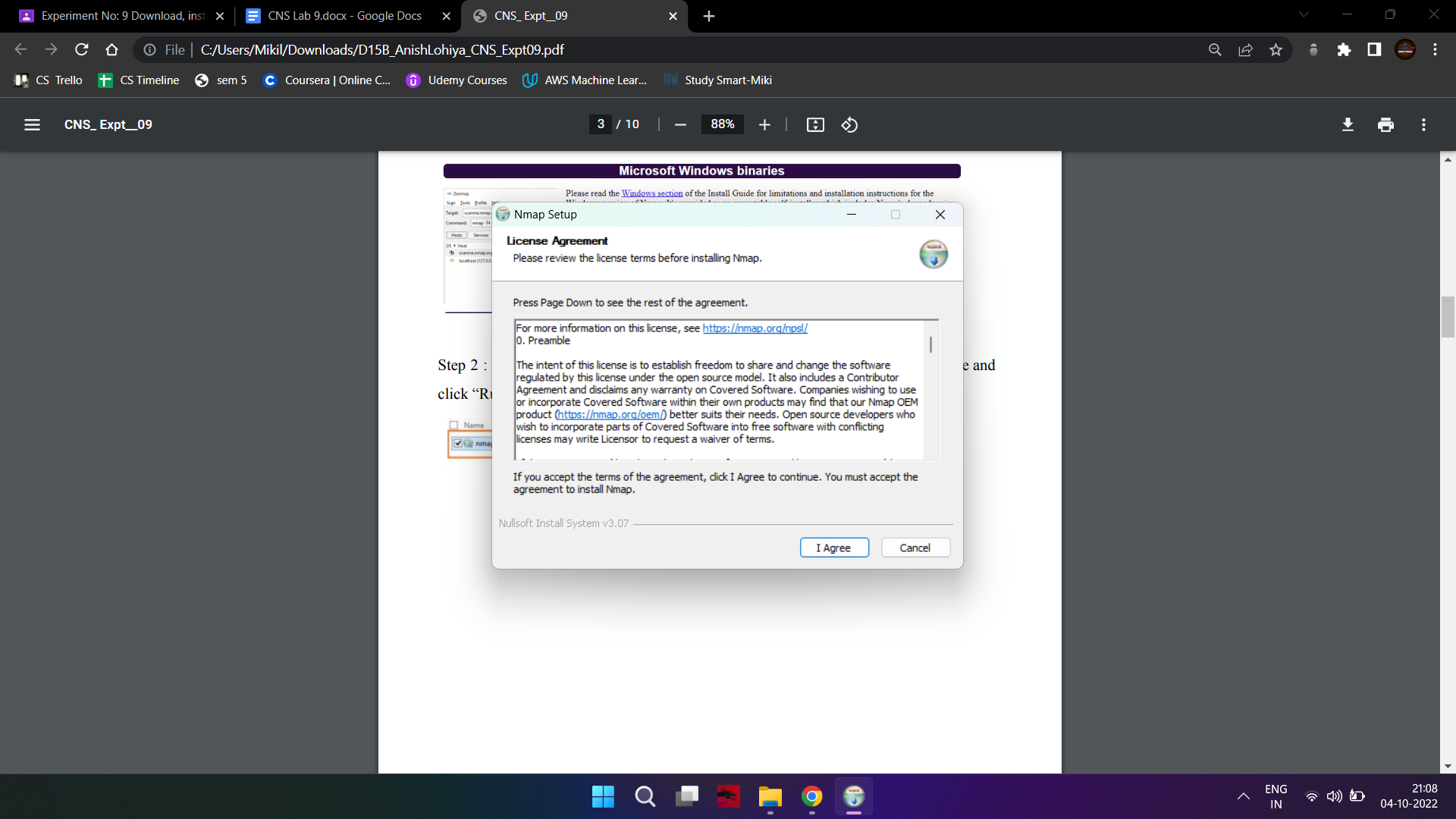


1. Go to the location where the file is downloaded. Right-click on the EXE file and

click “Run as administrator.”

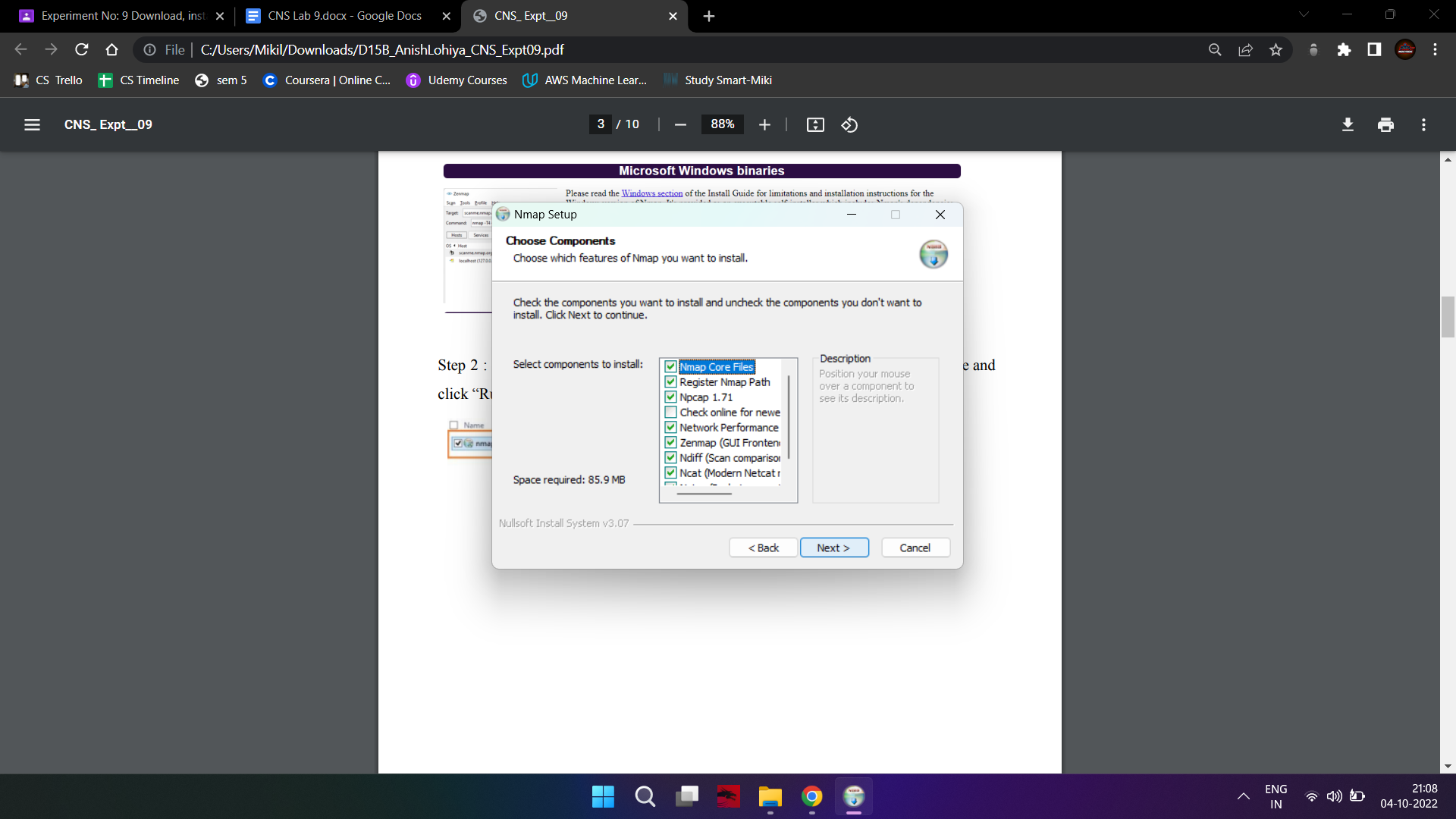


1. It will start the installation process, and accept the license agreement.



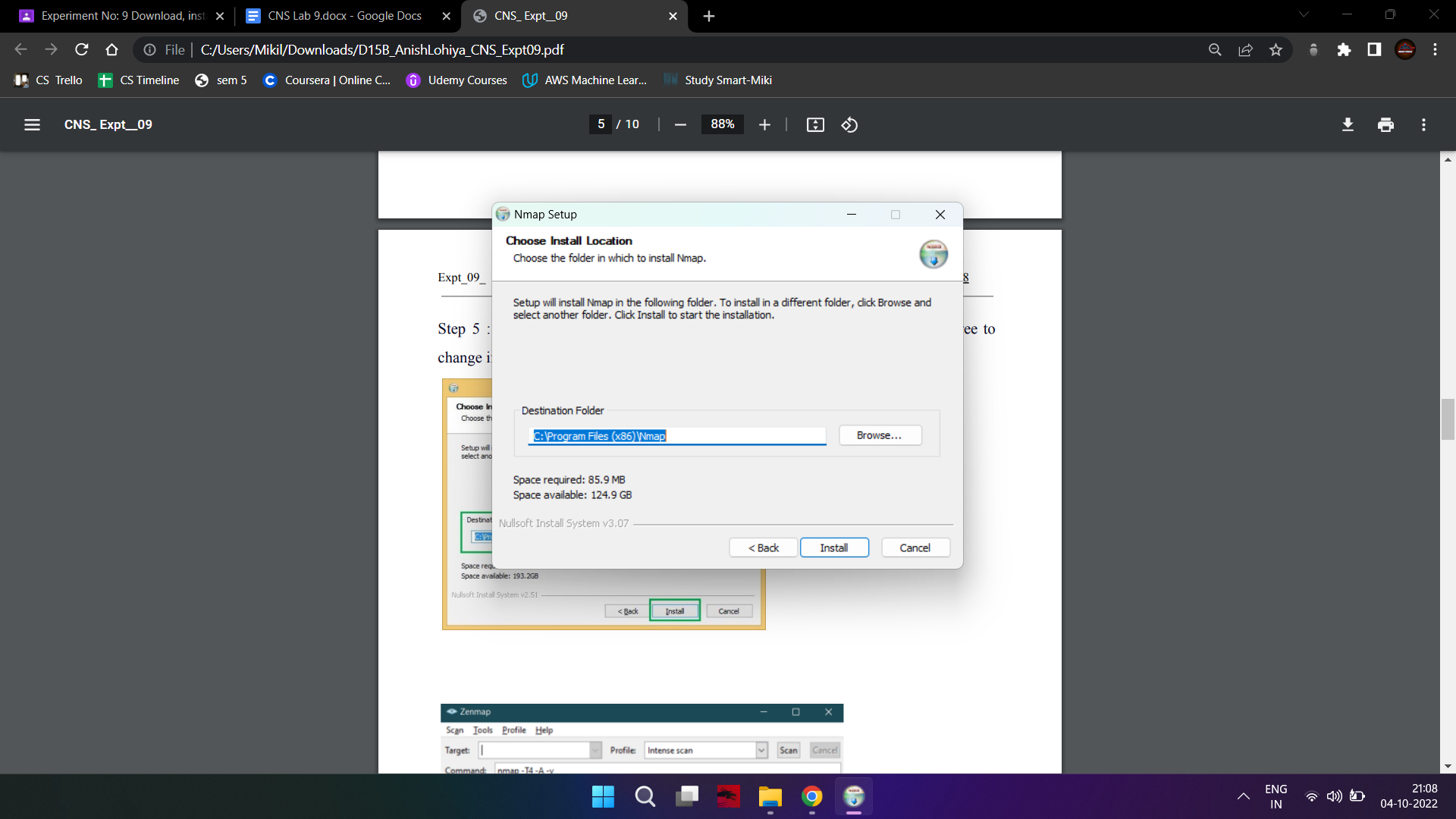
1. You can choose what components to install, but it would be good to install all of

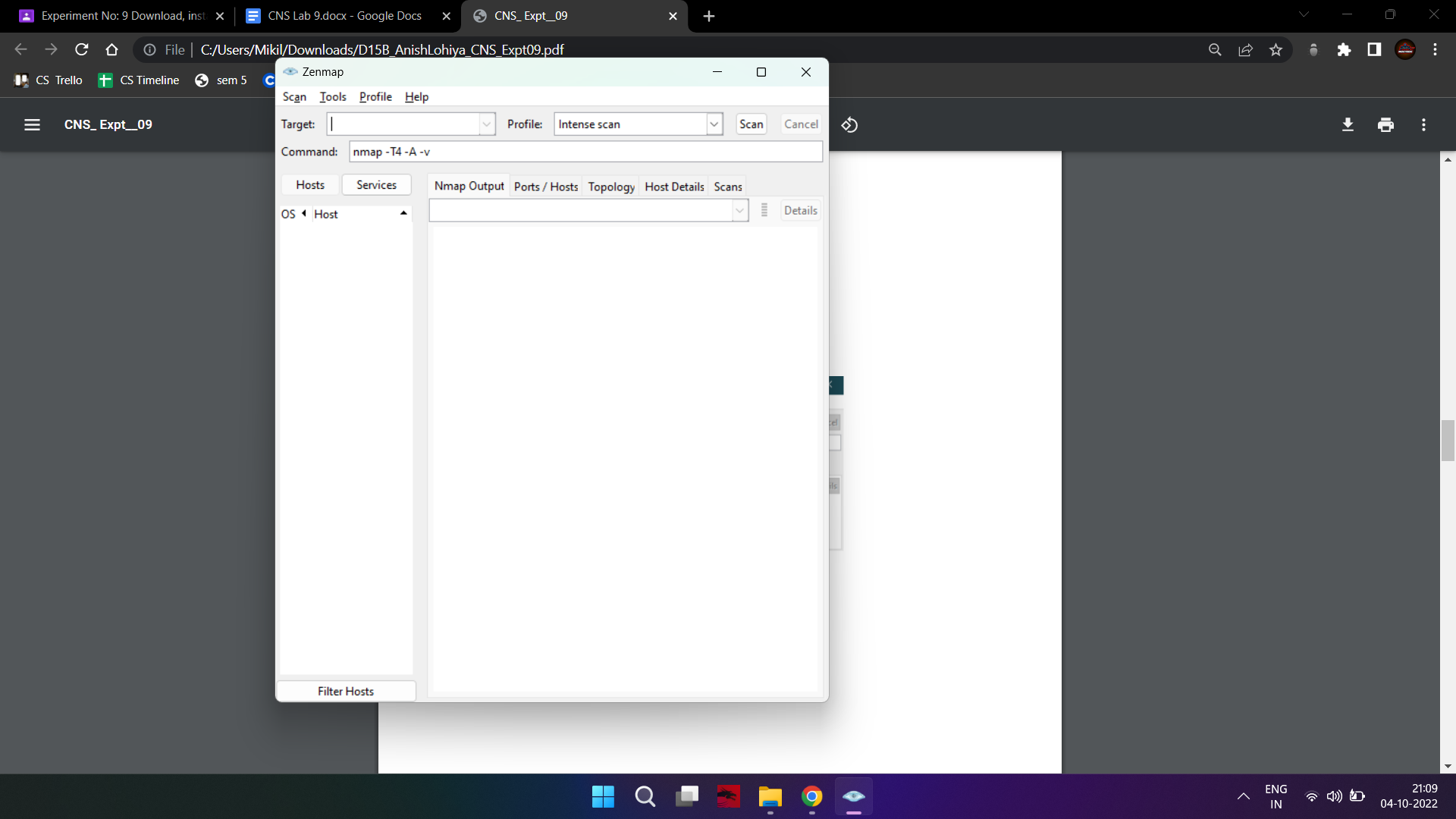
them.



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

change it if needed.



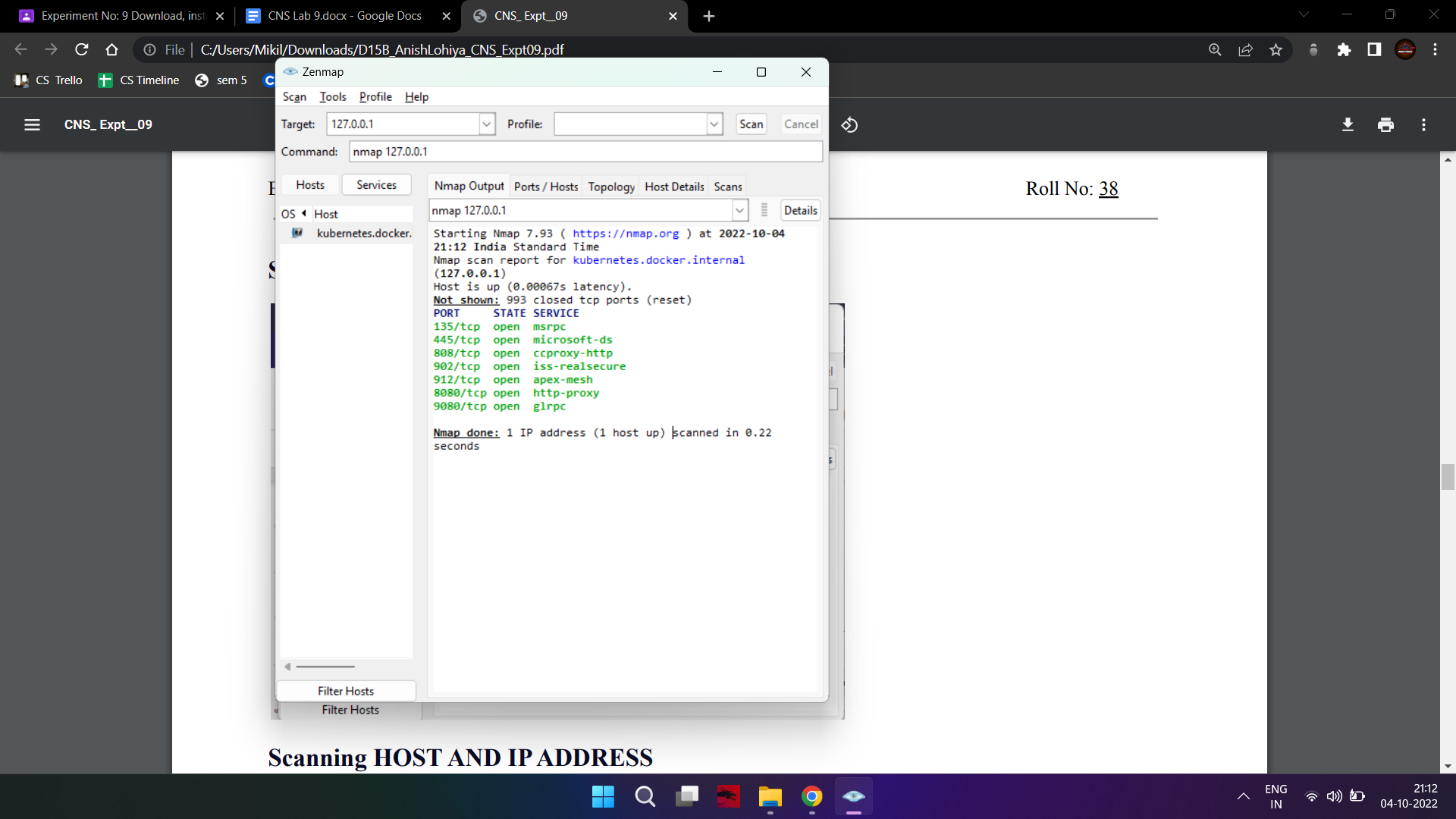


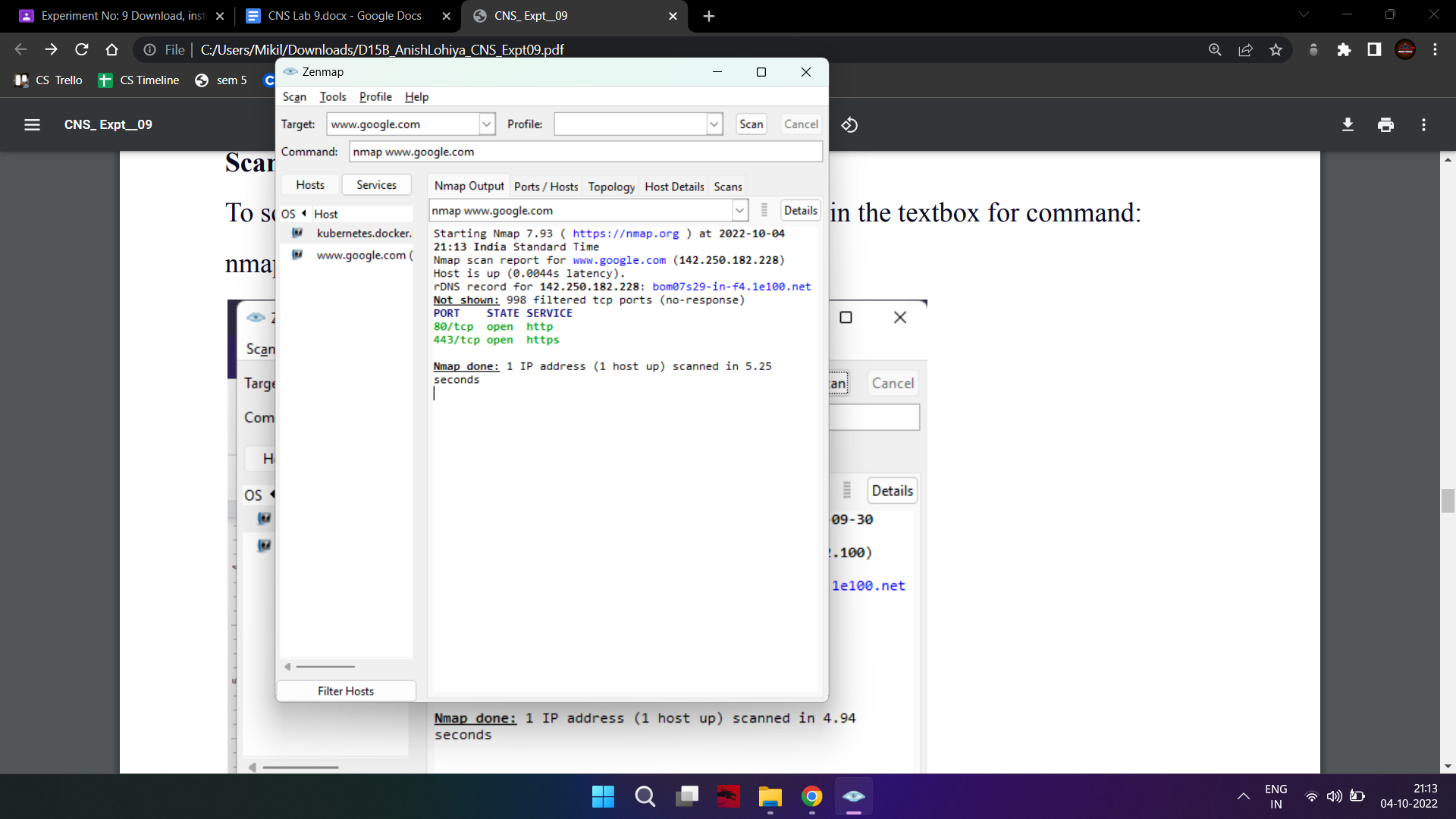
Scanning Ports

Scanning Host and IP Address

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

nmap www.google.com





Performing OS fingerprinting

Determining the operating system of a host is essential to every penetration tester for

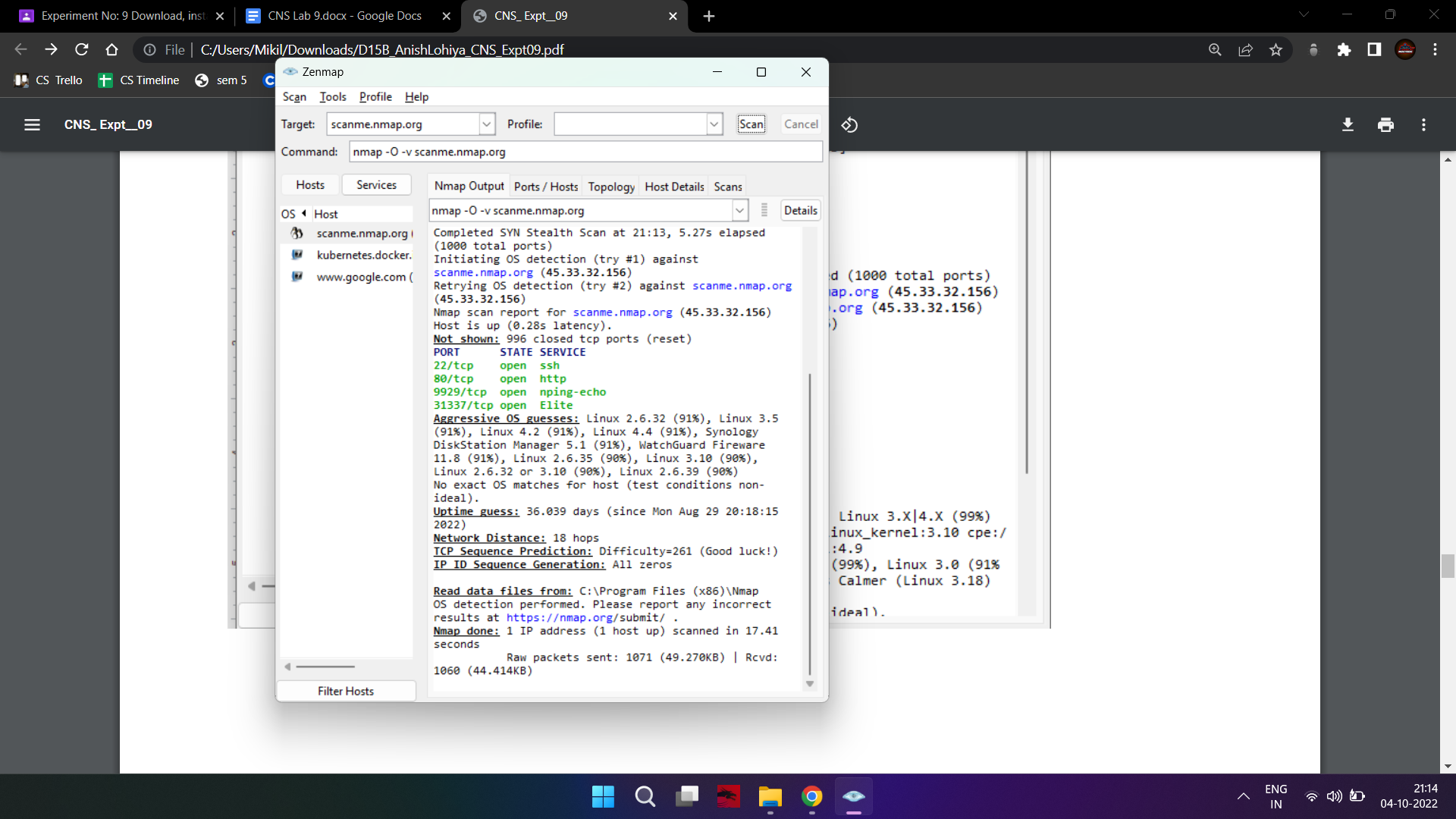
many reasons including listing possible security vulnerabilities, determining the

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



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

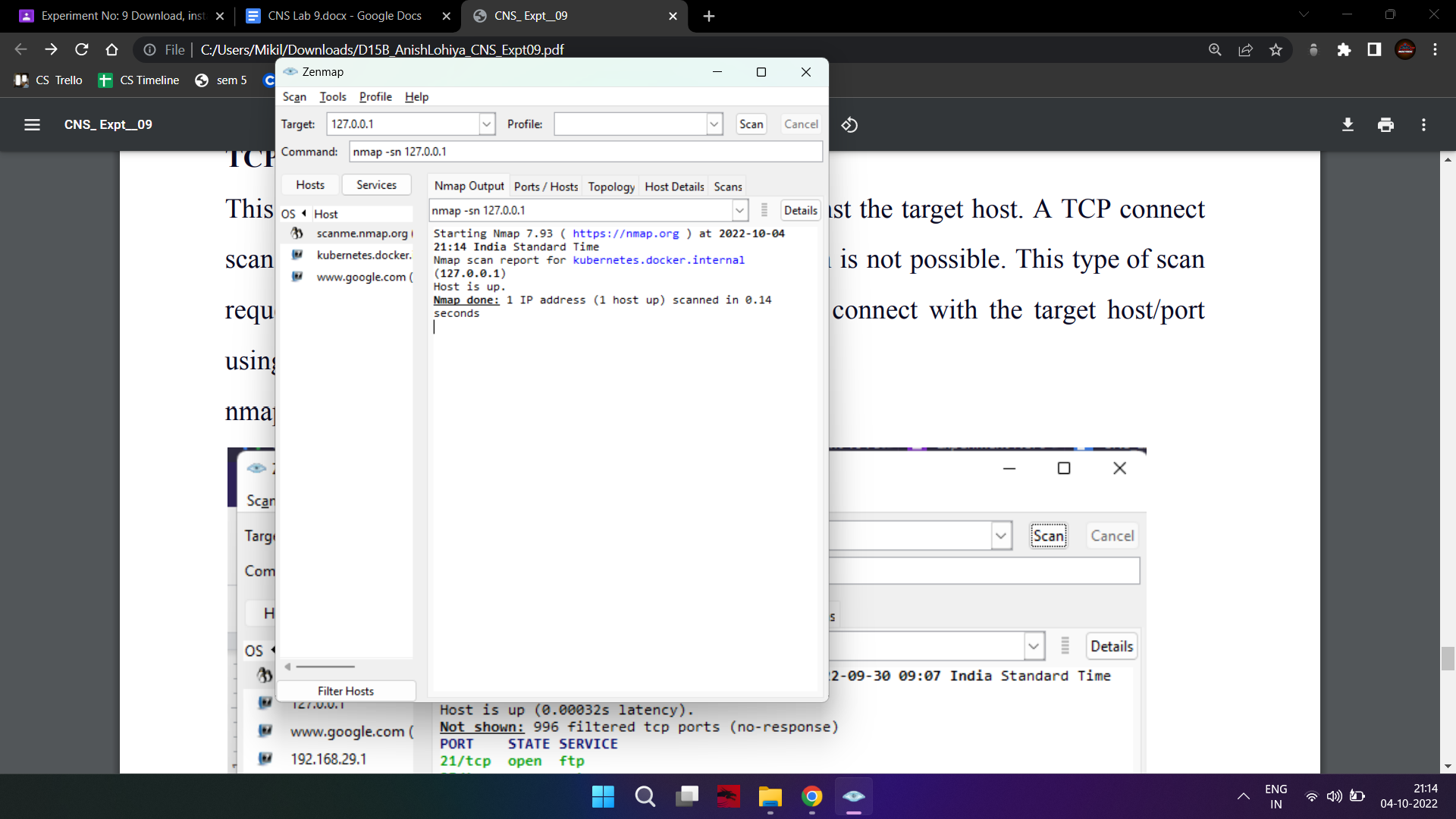
currently online without sending any packers to these hosts. This command then returns

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

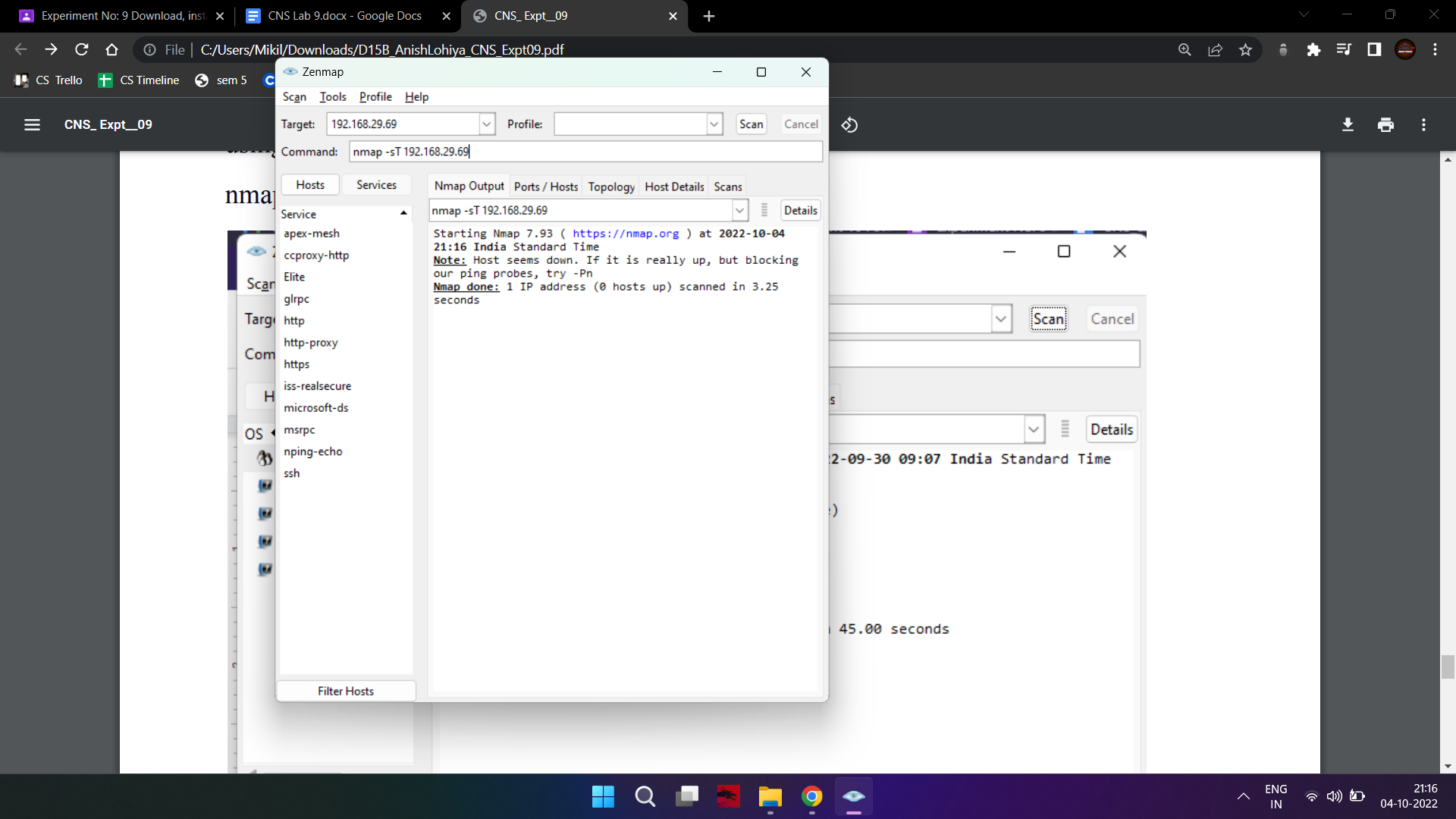
This command will initiate a TCP connect scan against the target host. A TCP connect

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



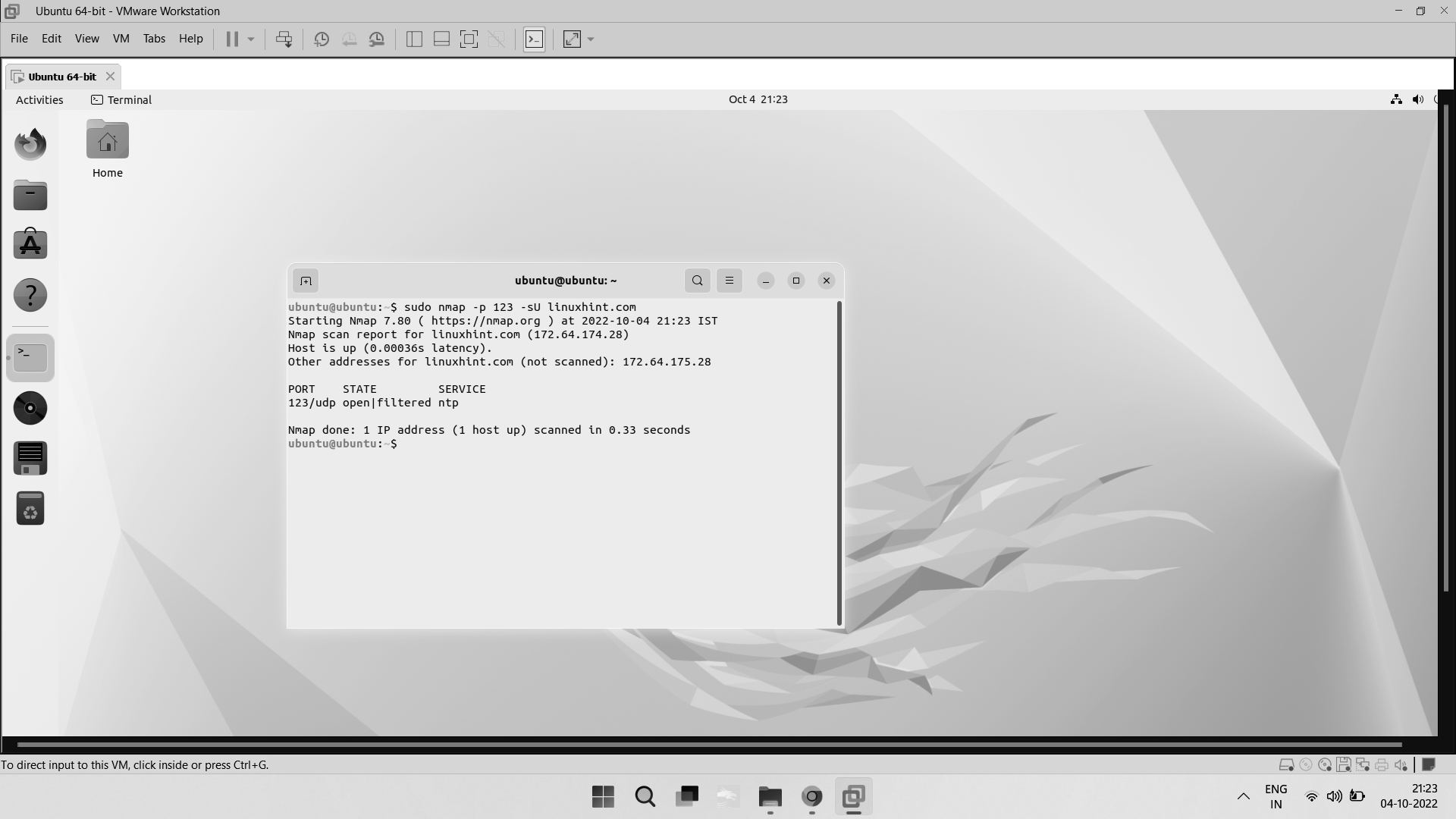
UDP Port Scan

nmap -sU -T4 scanme.nmap.org



Nmap scan specific udp port

nmap -p 123 -sU linuxhint.com



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.