**PRACTICAL: 4**

**AIM:**

Port scanning is a method for determining open ports and services available on a network or a host. It involves connecting with TCP and UDP ports on the system, once you found the IP addresses of a target network or host by the Footprinting technique. You have to map the network of this targeted organization. Nmap (Network Mapper) is a powerful, flexible, open-source, and easy-to-use tool for port scanning available for both Linux and Windows-based operating systems. Study practical approaches to implementing scanning and enumeration techniques using Nmap.

**THEORY:**

**Port scanning:** Finding out which ports are open on a network may be done using a port scan. Port scanning is comparable to knocking on doors to determine whether somebody is home since ports are where information is transferred and received on computers. By doing a port scan on a network or server, you may find out which ports are open and listening (receiving information) as well as whether there are any firewalls or other security measures between the sender and the destination.

The term "fingerprinting" describes this method. In order to determine the current state, it transmits a packet of network data to a port.

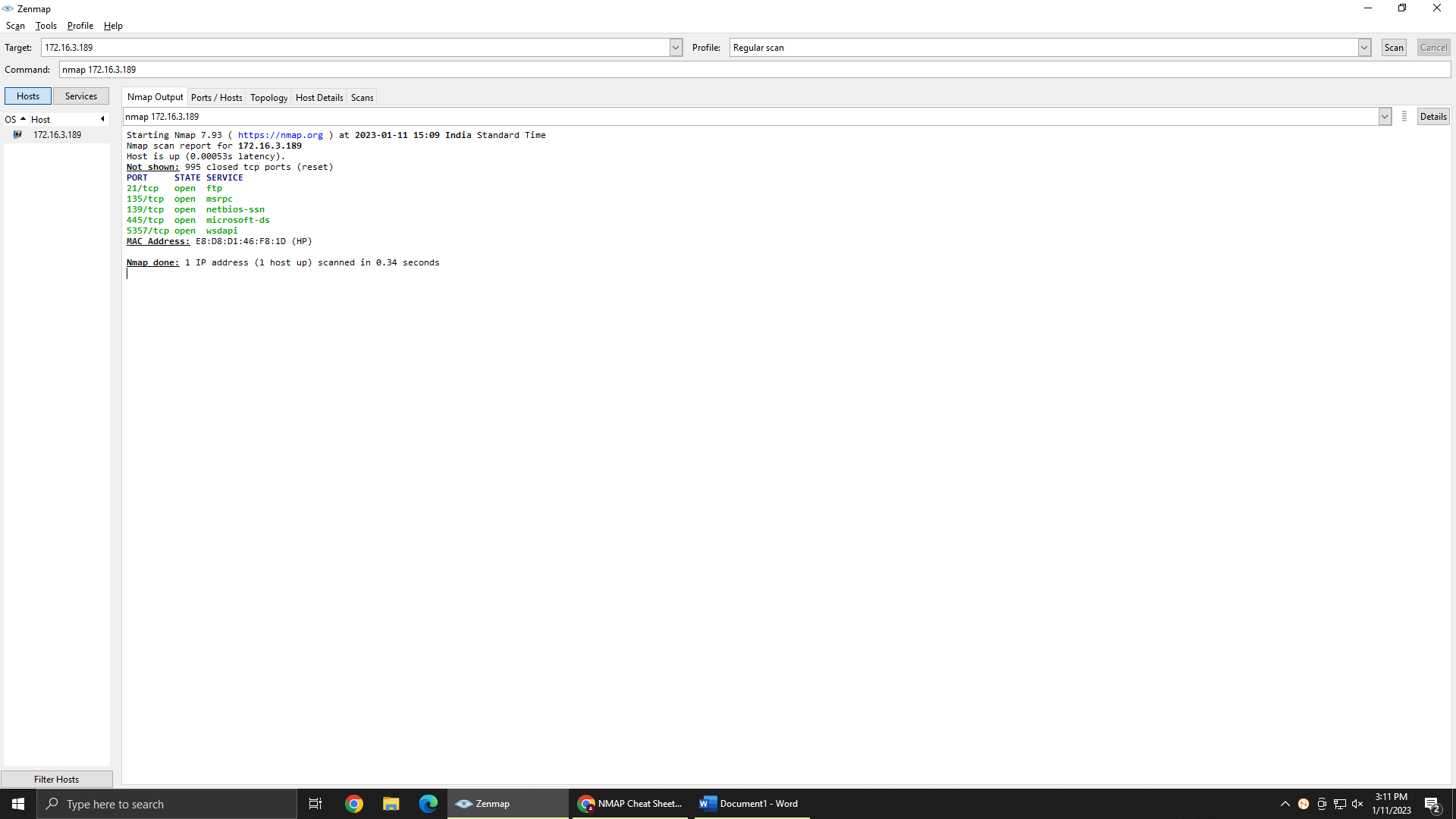
**Nmap:** A free and open source tool for network discovery and security auditing is called Nmap ("Network Mapper"). It is helpful for duties like managing service update schedules, network inventory, and host or service uptime, according to several systems and network managers.

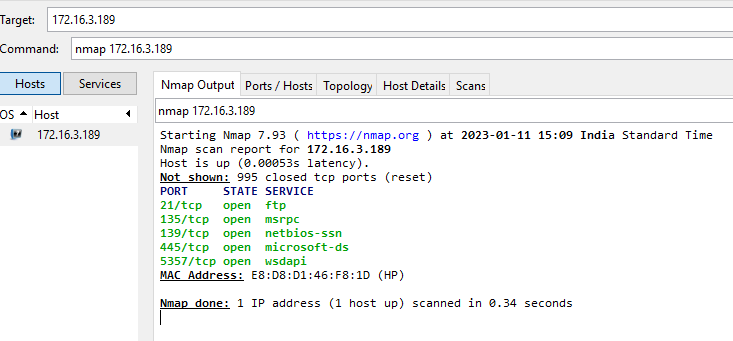
* The ability to instantly identify any device on a single or numerous networks, including servers, routers, switches, mobile devices, etc.
* Using pre-existing scripts from the Nmap Scripting Engine, you may attack systems using Nmap during security audits and vulnerability assessment.
* Zenmap is the name of Nmap's graphical user interface. It aids in the creation of network visual maps for enhanced use and reporting.

**Advantages and Disadvantages**

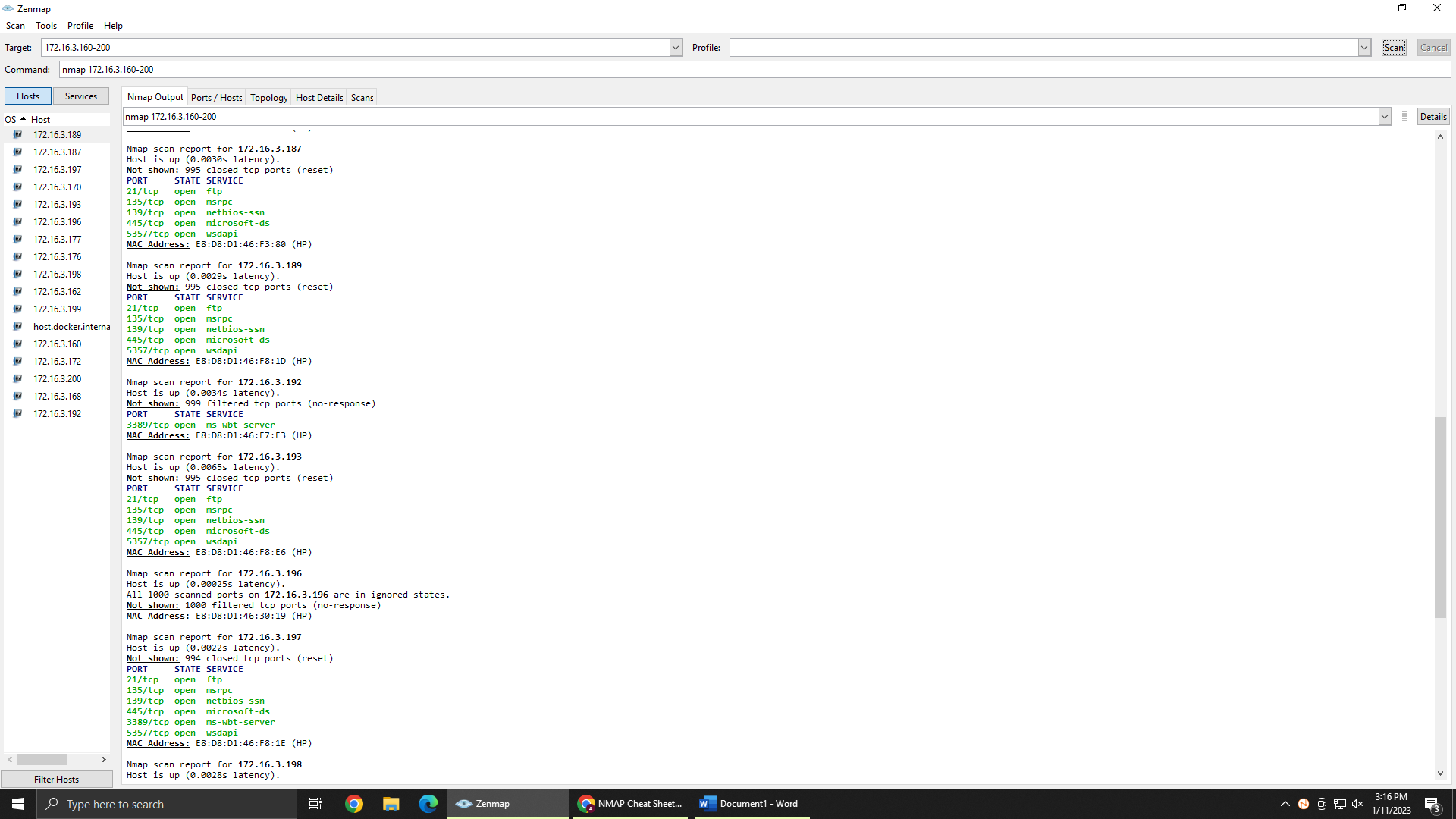
|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| Only for beginner | Not all the configuration which we need |
| OS Detection, Checking Firewall  rules and unique process of  fingerprinting applications/devices. | You cannot use this tool if there is no  Network. |

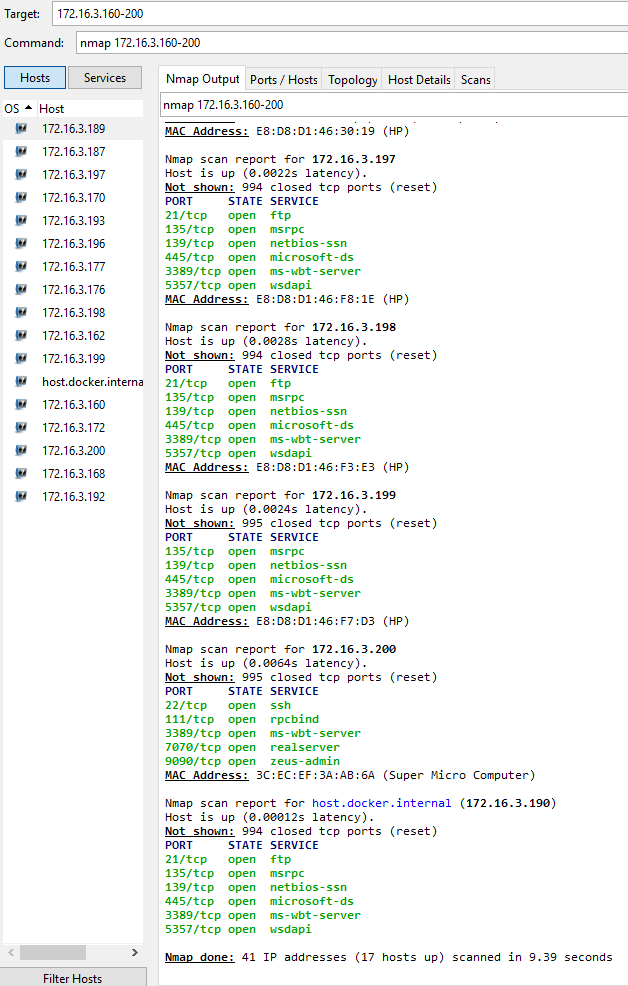
**OUTPUT:**



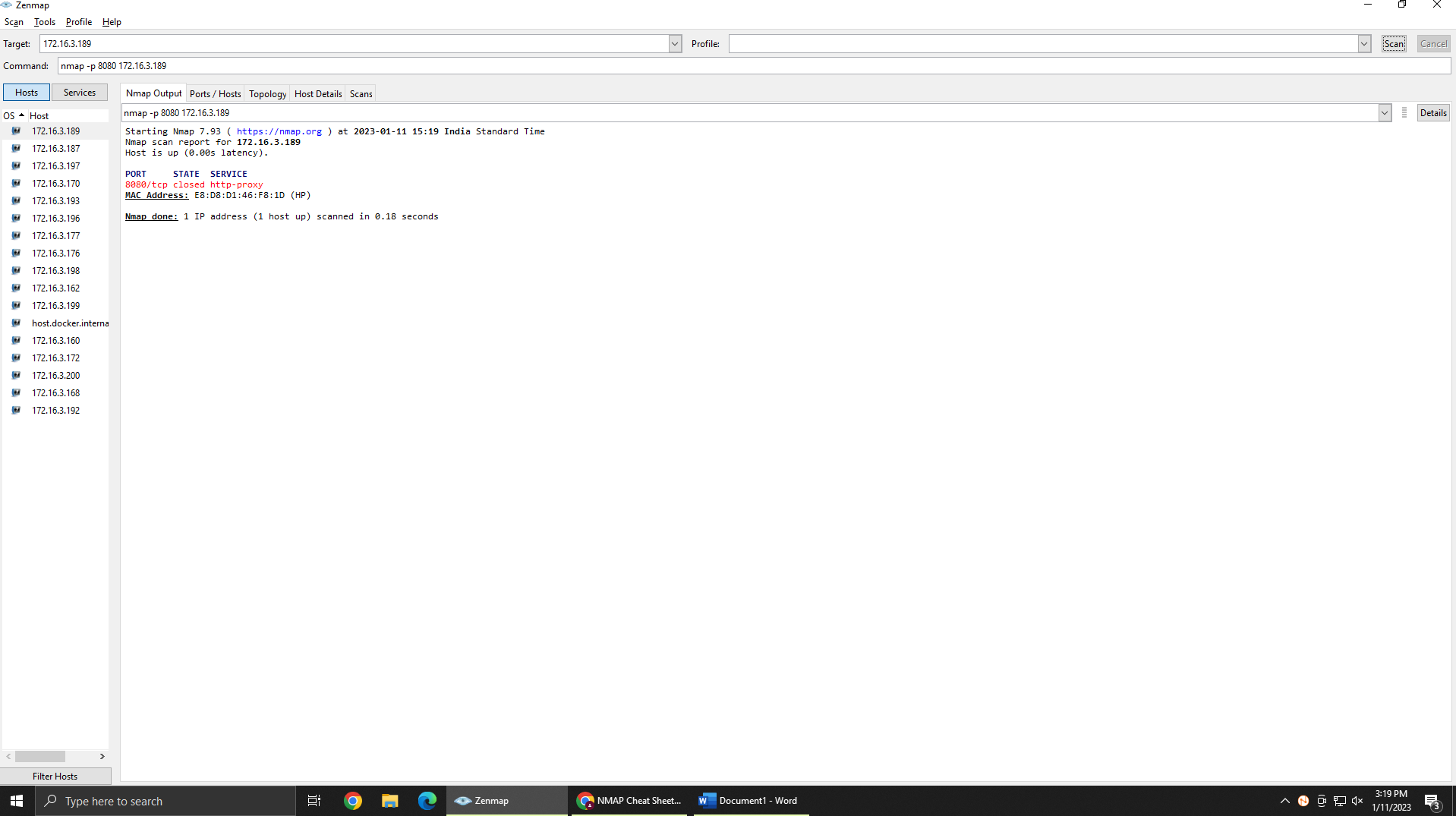


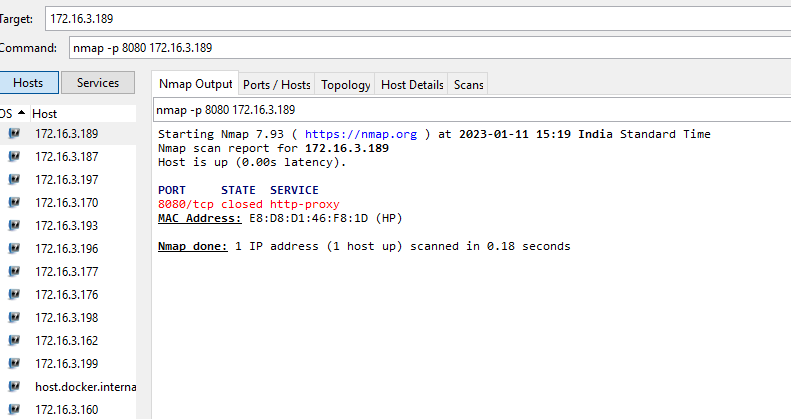
Scanning a single target- nmap172.16.3.189



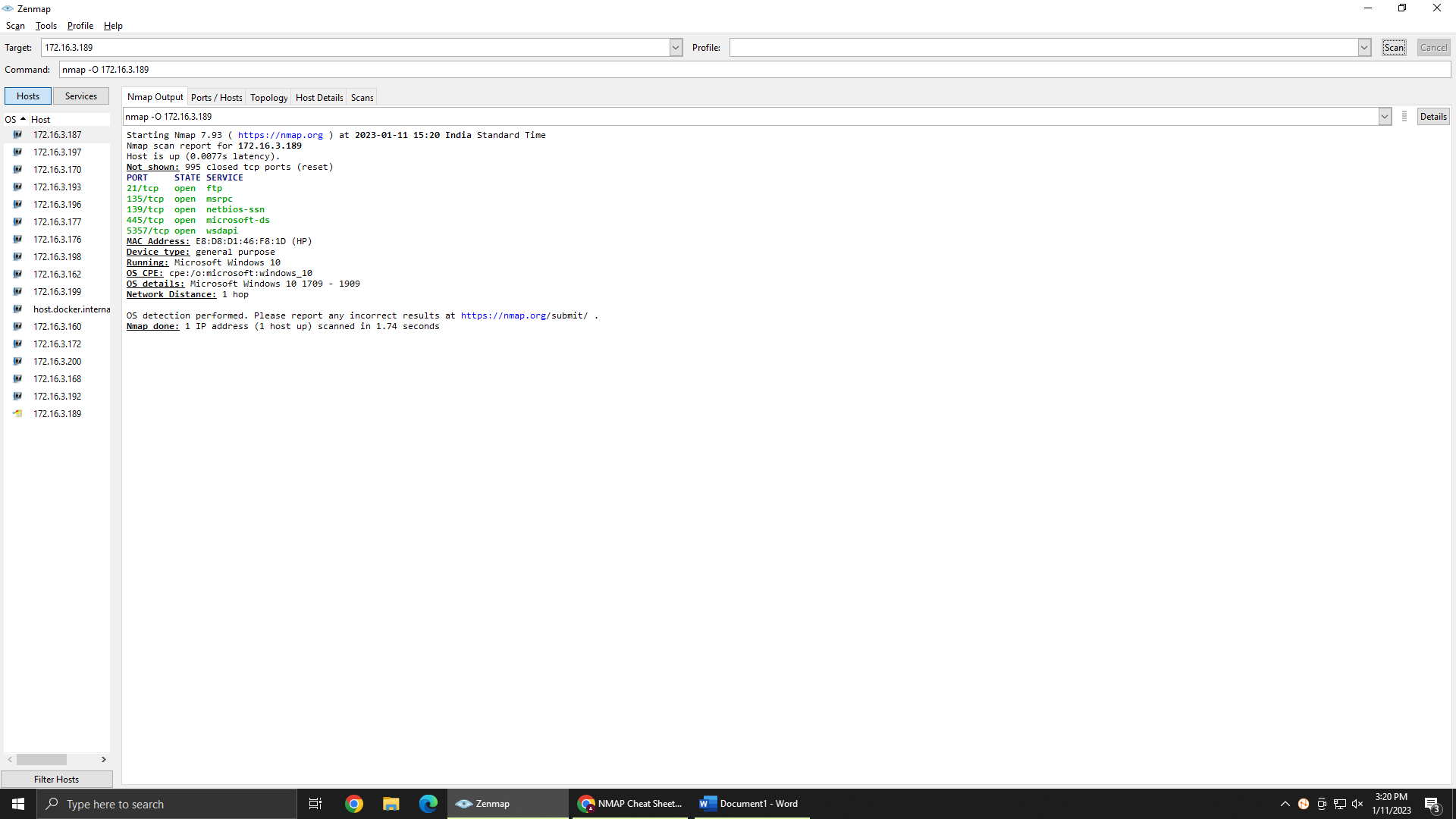


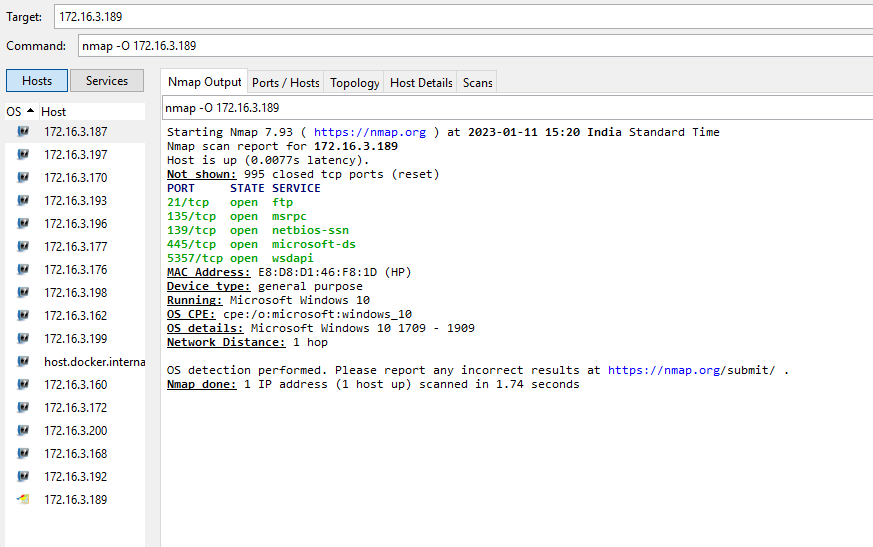
Scanning a range of hosts nmap 172.16.3.160-200



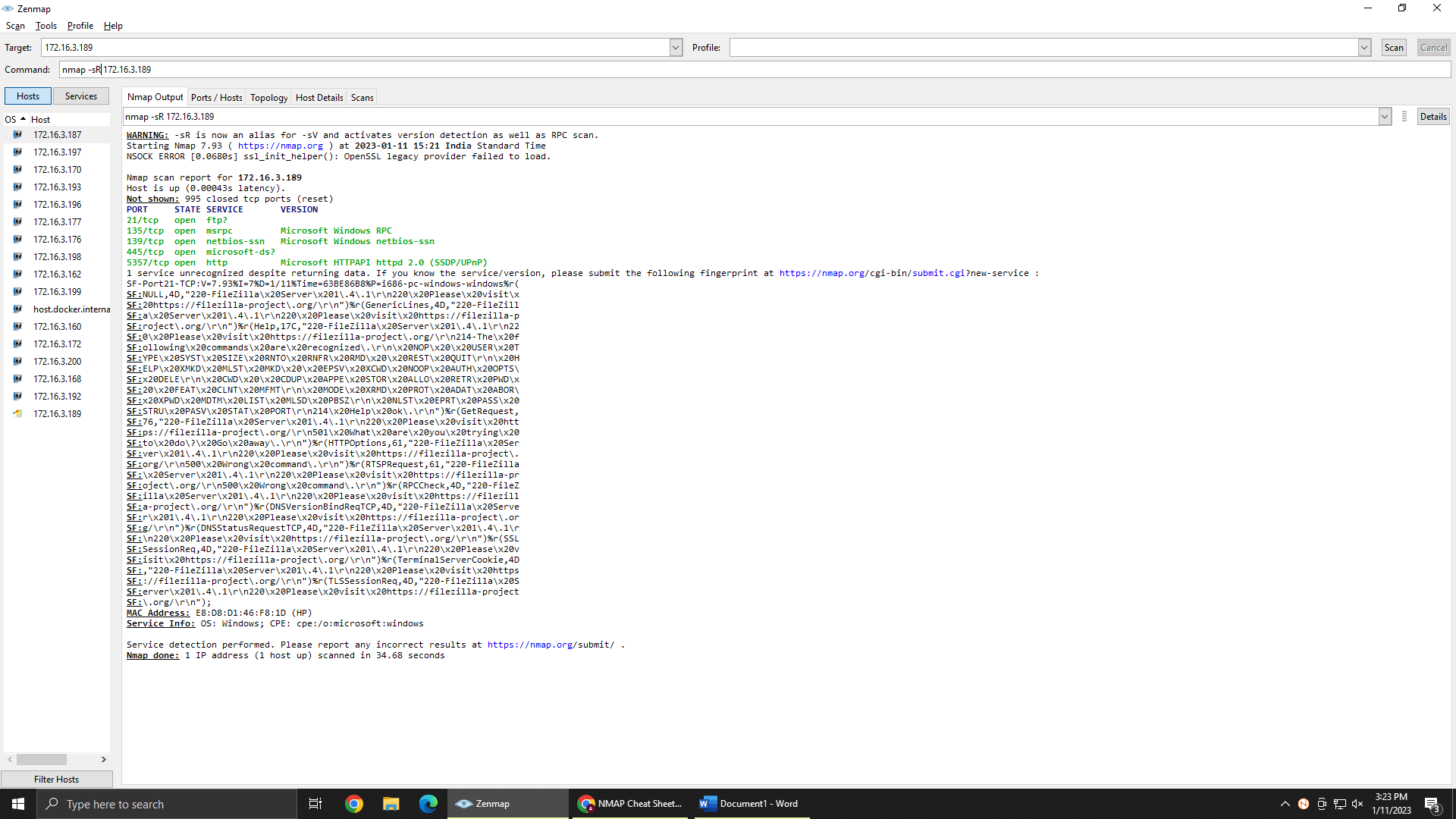


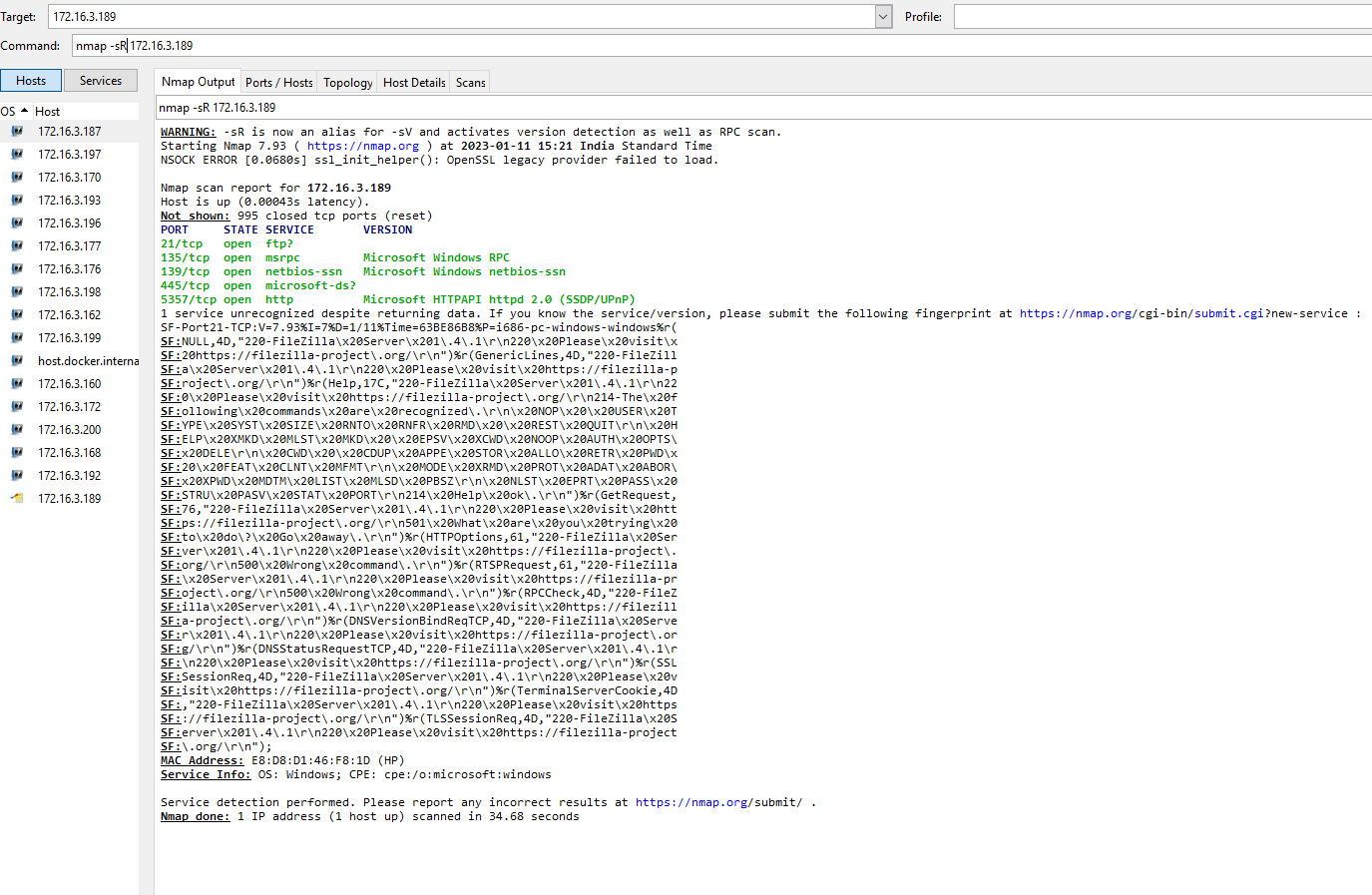
Scan specific port – nmap -p 8080 172.16.3.189





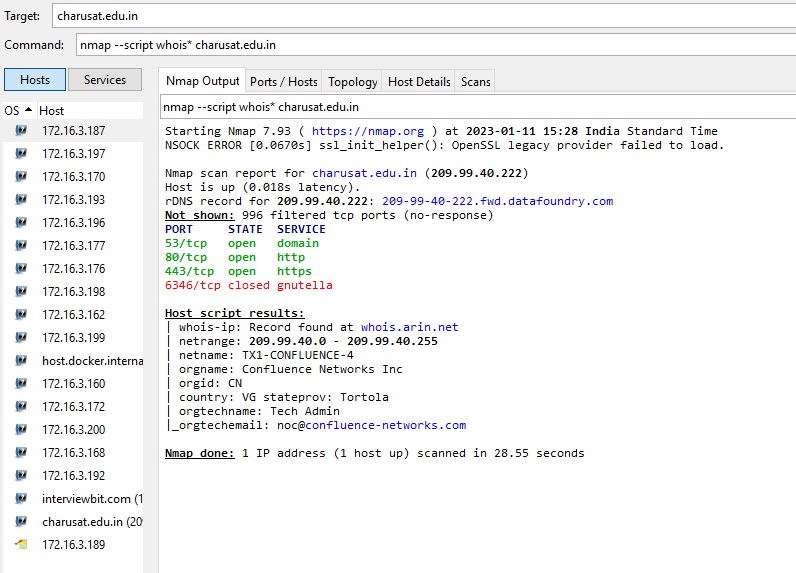
Operating system detection – nmap -O 172.16.3.189



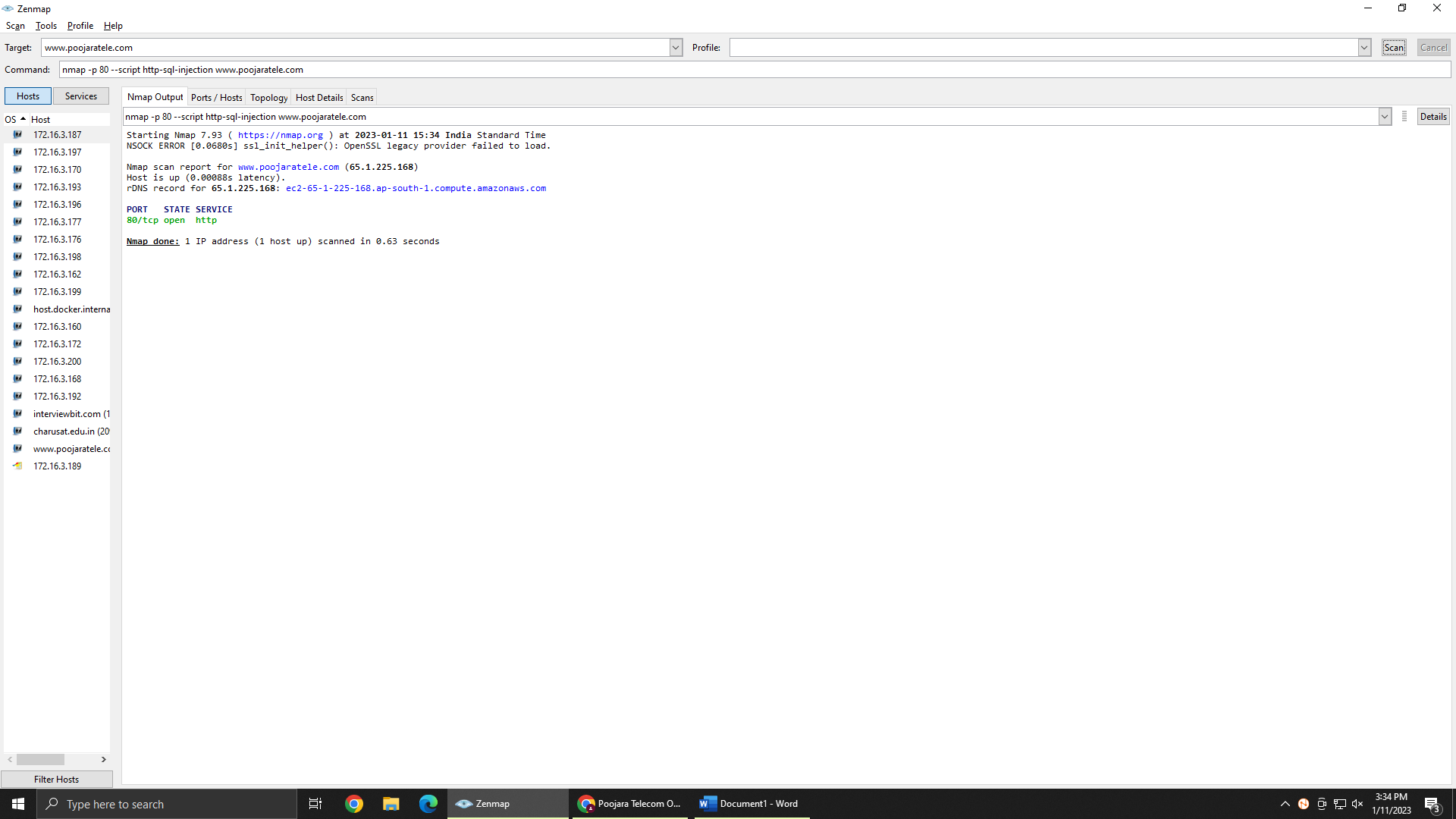


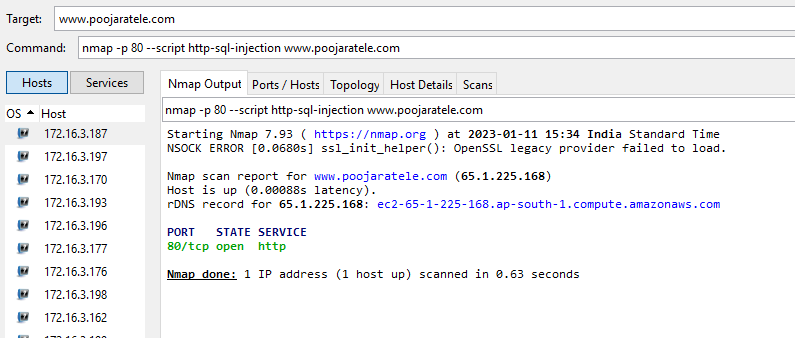
Perform a RPC scan – nmap -sR 172.16.3.189





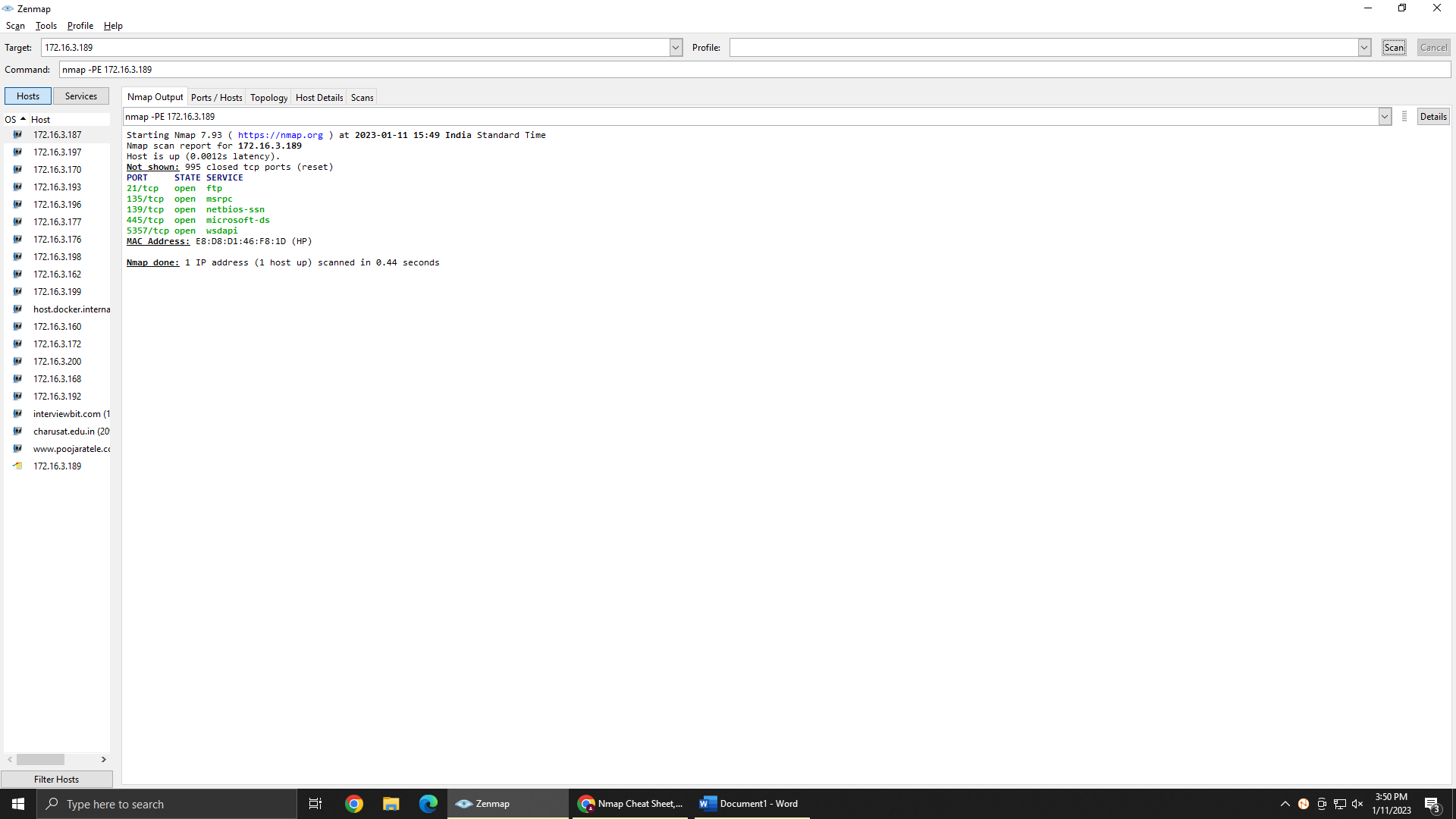
Query for who is - nmap –script whois\* charusat.edu.in

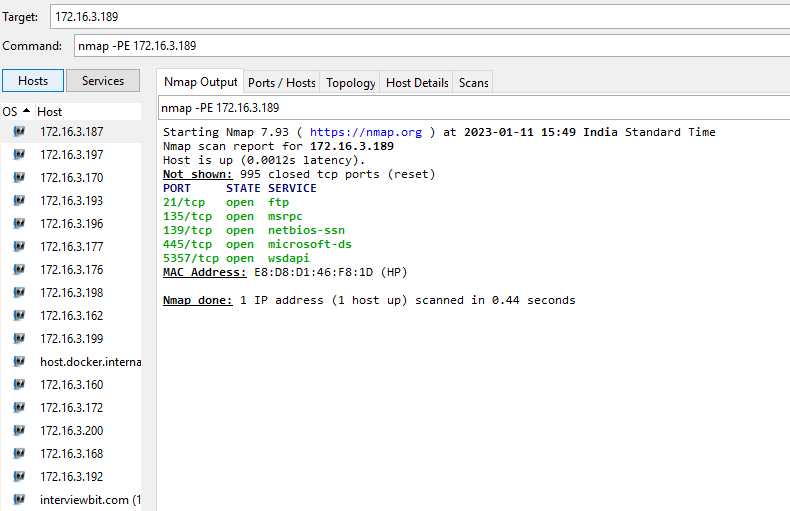




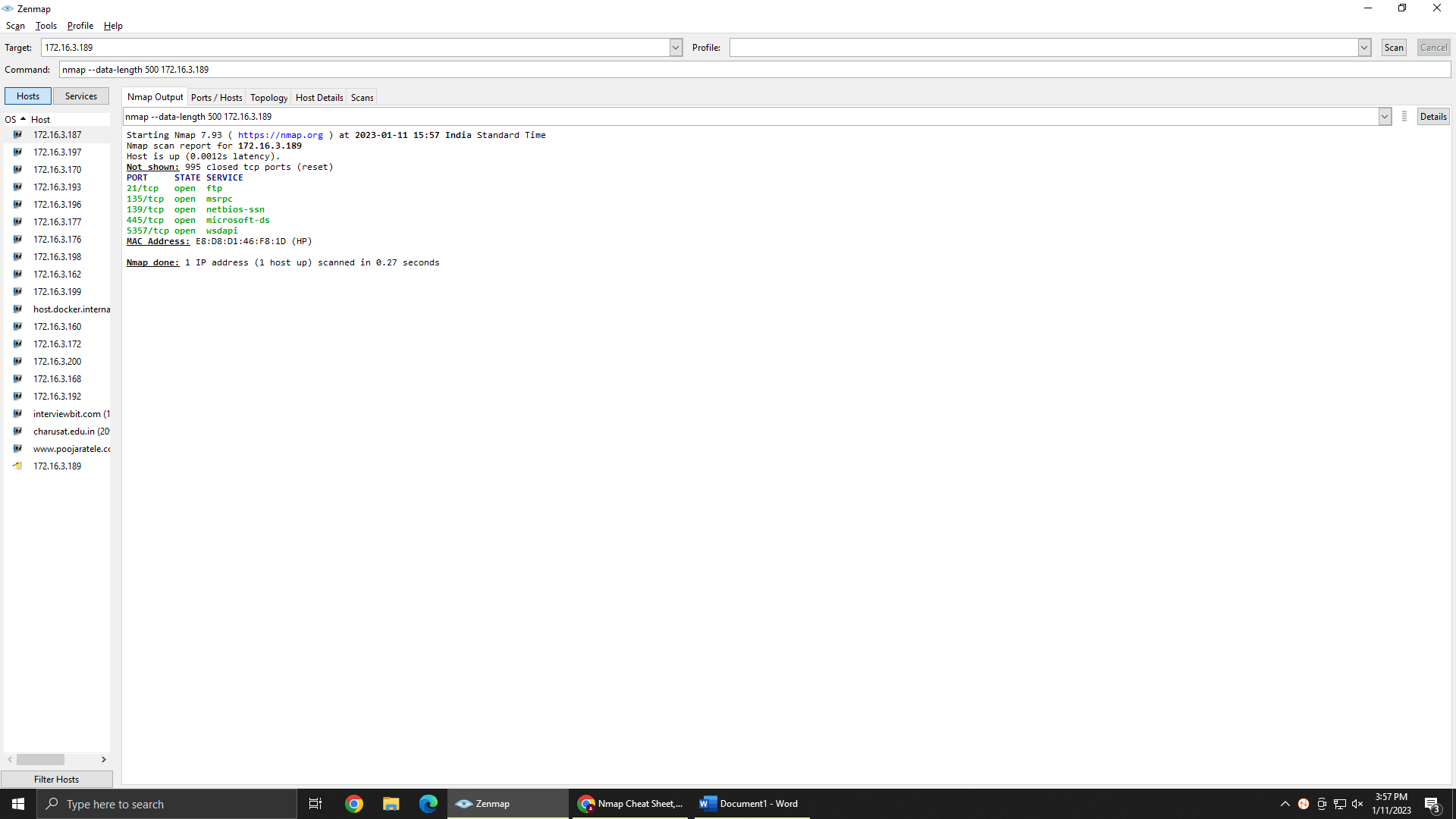
SQL injection detection

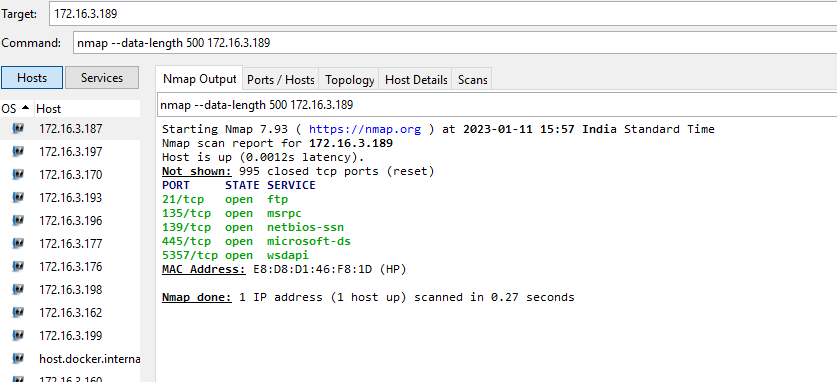
Nmap -p 80 –script http-sql-injection [www.poojaratele.com](http://www.poojaratele.com)



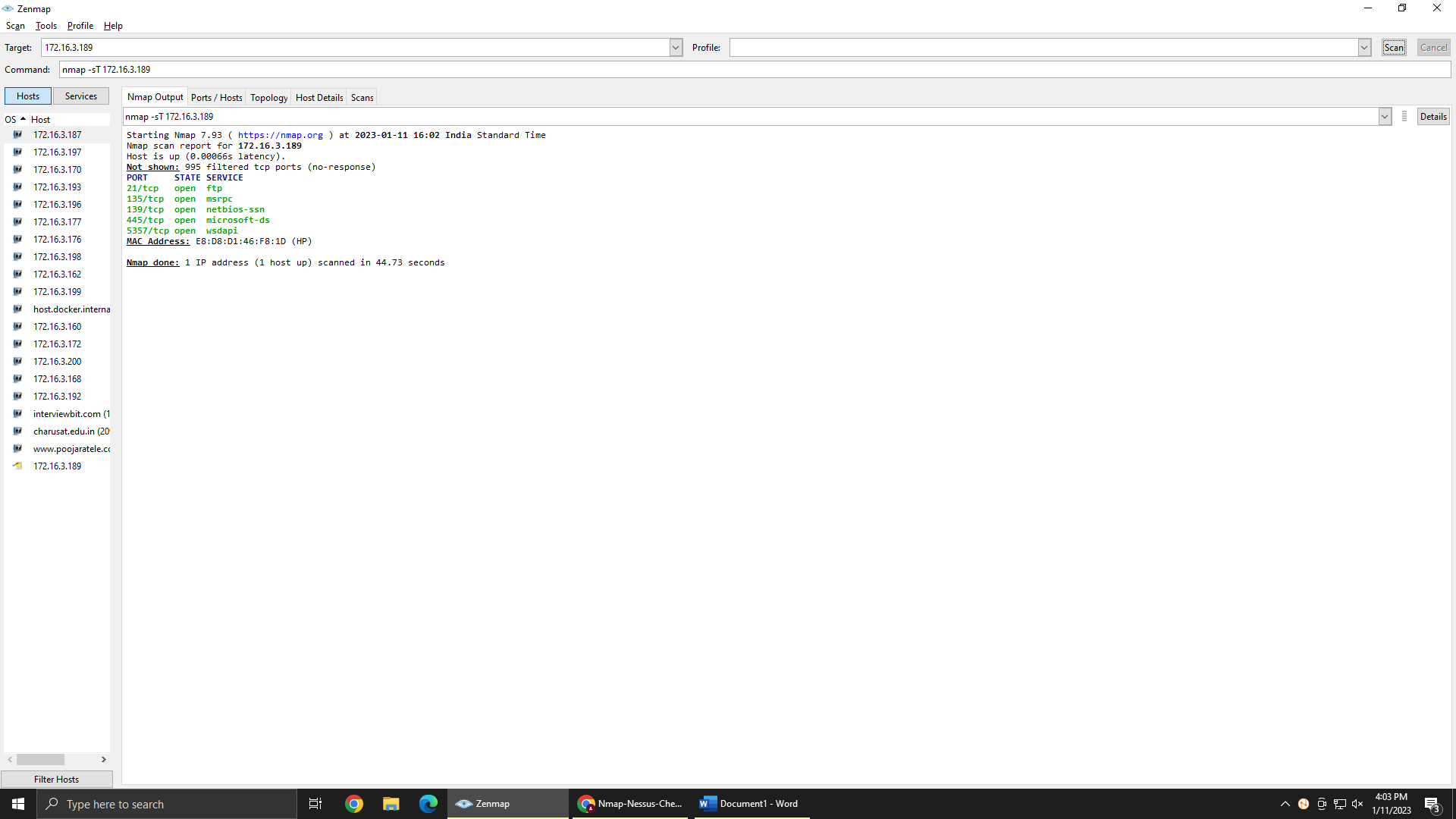


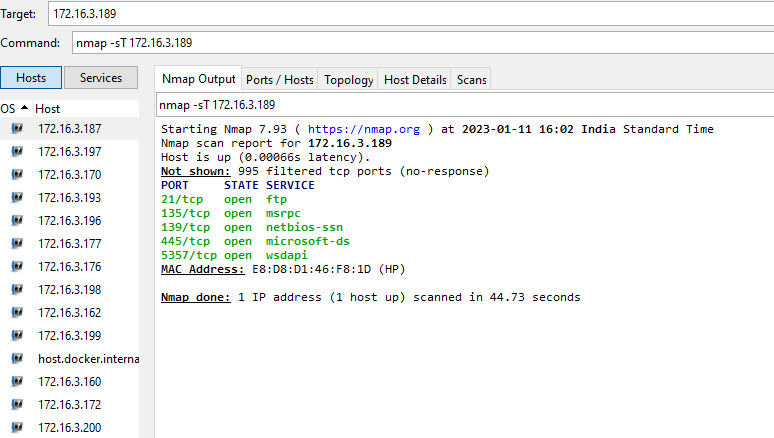
ICMP echo ping – nmap -PE 172.16.3.189





Randomally Append data





TCP connect port

**LATEST APPLICATIONS:**

**The most commonly used port are:** A ping scan. These ICMP (Internet Control Message Protocol) scans look over a full IP address range or a single target IP address to see if the target is online.

TCP , UDP scan commonly used port scan by port scanning tools.

Scan every IP address.Automate systems and vulnerability scans

**LEARNING OUTCOME:**

How to check how many ports are open or closed to particular pc, we can check a series of pc’s.also and how to know operating system of another pc’s .also check UDP,TCP ports and many more about Mapping the network using IP address of any targeted organization using Nmap

**REFERENCES:**

1. Nmap download: <https://nmap.org/download.html#windows>