

## 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.

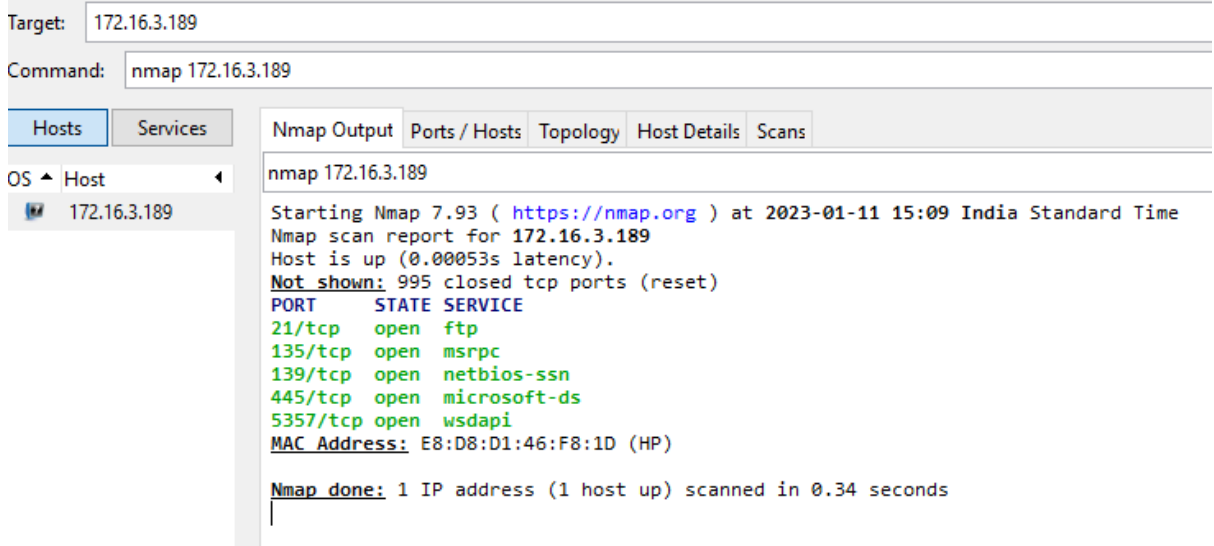
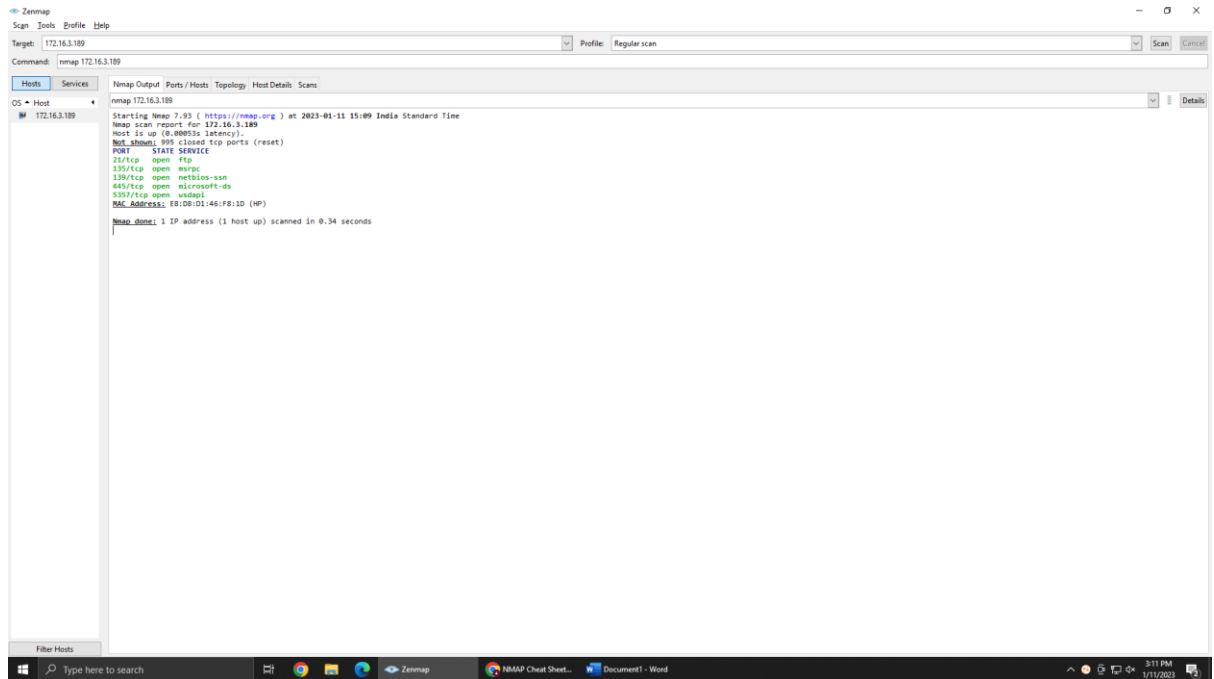
**Nmap:** A free and open source tool for network discovery and security auditing is called Nmap ("Network Mapper"). It is helpful for duties like managing service update schedules, network inventory, and host or service uptime, according to several systems and network managers.

- 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.

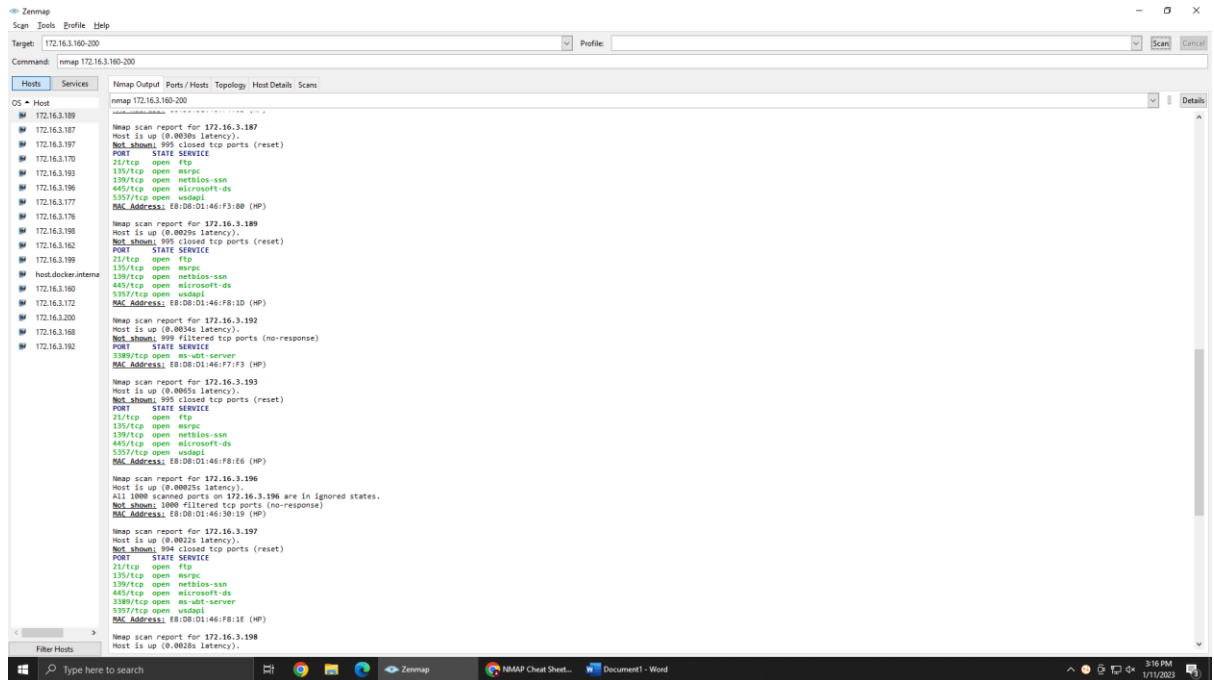
### Advantages and Disadvantages

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



Target: 172.16.3.160-200

Command: nmap 172.16.3.160-200

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

172.16.3.189  
172.16.3.187  
172.16.3.197  
172.16.3.170  
172.16.3.193  
172.16.3.196  
172.16.3.177  
172.16.3.176  
172.16.3.198  
172.16.3.162  
172.16.3.199  
host.docker.internal  
172.16.3.160  
172.16.3.172  
172.16.3.200  
172.16.3.168  
172.16.3.192

nmap 172.16.3.160-200

**MAC Address:** E8:D8:D1:46:30:19 (HP)

Nmap scan report for 172.16.3.197  
Host is up (0.0022s latency).  
**Not shown:** 994 closed tcp ports (reset)

PORT	STATE	SERVICE
21/tcp	open	ftp
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5357/tcp	open	wsdapi

**MAC Address:** E8:D8:D1:46:F8:1E (HP)

Nmap scan report for 172.16.3.198  
Host is up (0.0028s latency).  
**Not shown:** 994 closed tcp ports (reset)

PORT	STATE	SERVICE
21/tcp	open	ftp
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5357/tcp	open	wsdapi

**MAC Address:** E8:D8:D1:46:F3:E3 (HP)

Nmap scan report for 172.16.3.199  
Host is up (0.0024s latency).  
**Not shown:** 995 closed tcp ports (reset)

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5357/tcp	open	wsdapi

**MAC Address:** E8:D8:D1:46:F7:D3 (HP)

Nmap scan report for 172.16.3.200  
Host is up (0.0064s latency).  
**Not shown:** 995 closed tcp ports (reset)

PORT	STATE	SERVICE
22/tcp	open	ssh
111/tcp	open	rpcbind
3389/tcp	open	ms-wbt-server
7070/tcp	open	realserver
9090/tcp	open	zeus-admin

**MAC Address:** 3C:EC:EF:3A:AB:6A (Super Micro Computer)

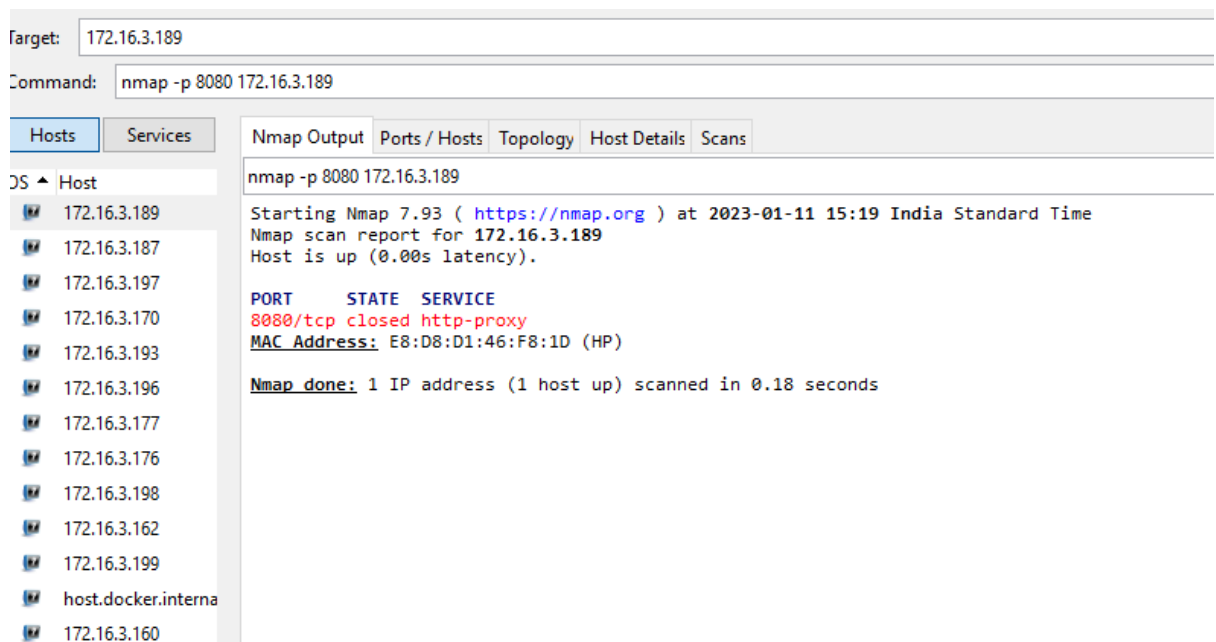
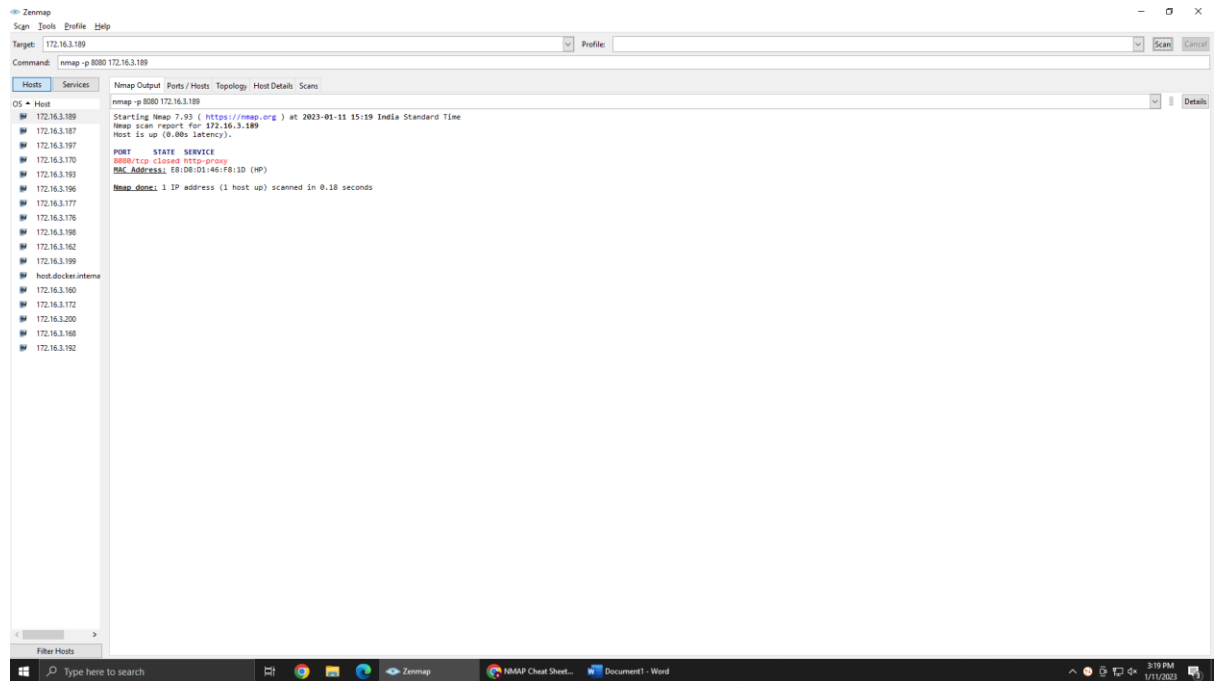
Nmap scan report for host.docker.internal (172.16.3.190)  
Host is up (0.00012s latency).  
**Not shown:** 994 closed tcp ports (reset)

PORT	STATE	SERVICE
21/tcp	open	ftp
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5357/tcp	open	wsdapi

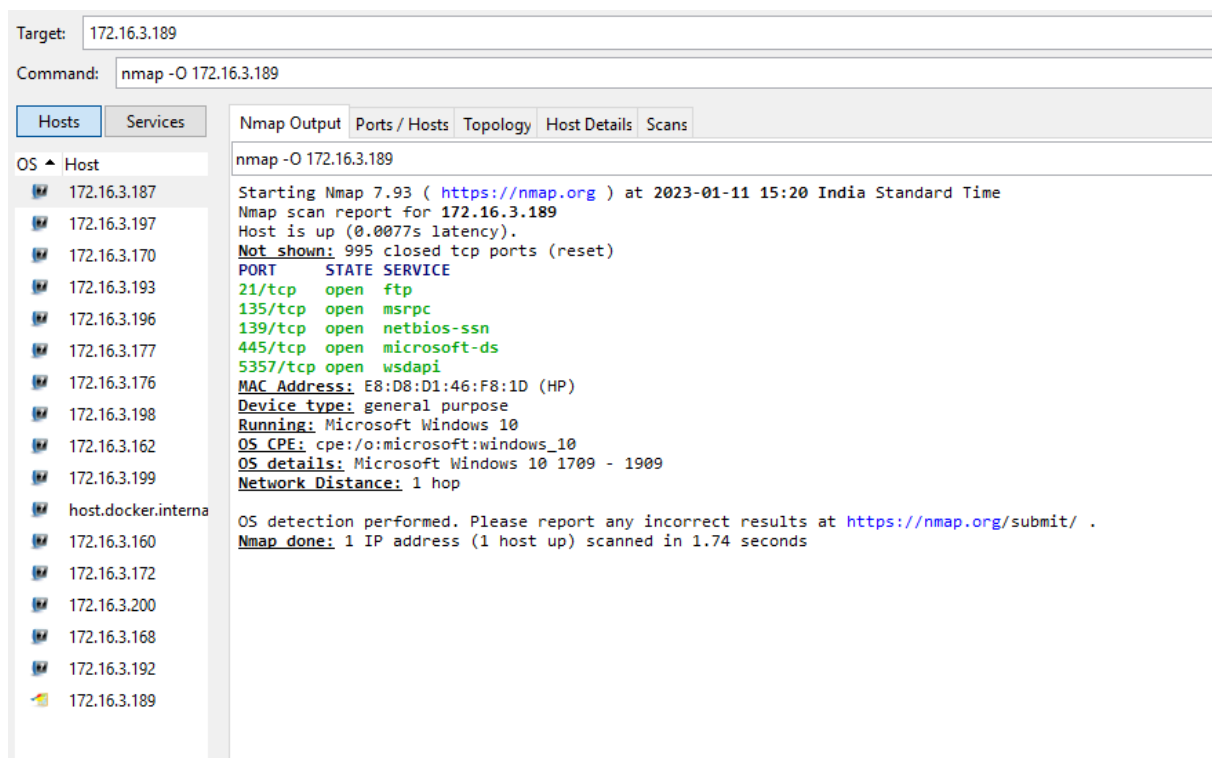
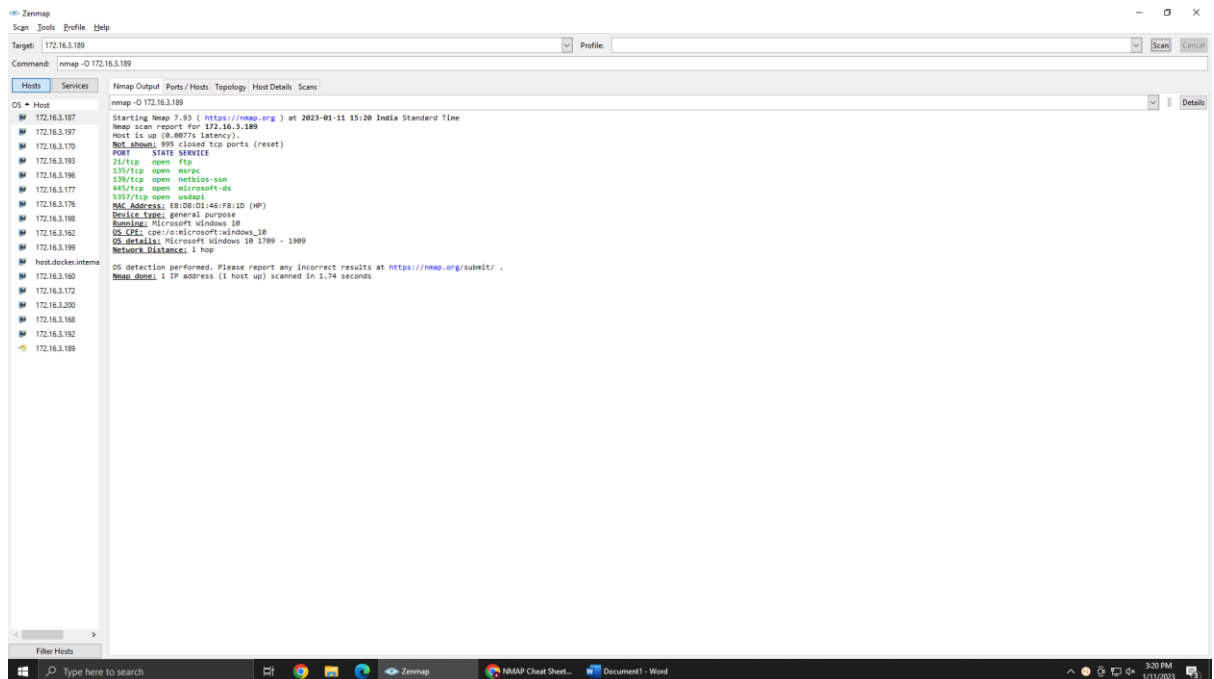
**Nmap done:** 41 IP addresses (17 hosts up) scanned in 9.39 seconds

Filter Hosts

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`

Target: 172.16.3.189

Command: nmap -sR 172.16.3.189

Hosts: 172.16.3.187, 172.16.3.197, 172.16.3.170, 172.16.3.193, 172.16.3.196, 172.16.3.177, 172.16.3.176, 172.16.3.198, 172.16.3.162, 172.16.3.199, 172.16.3.160, 172.16.3.172, 172.16.3.200, 172.16.3.168, 172.16.3.192, 172.16.3.189

Services: Nmap Output Ports/Hosts Topology Host Details Scans

OS: Host

172.16.3.187: WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan. Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-01-11 15:21 India Standard Time NSOCK ERROR [0.0608s] ssl\_init\_helper(): OpenSSL legacy provider failed to load.

172.16.3.197: Nmap scan report for 172.16.3.189 Host is up (0.00043s latency).

172.16.3.170: Not shown: 995 closed tcp ports (reset)

172.16.3.193: PORT STATE SERVICE VERSION

172.16.3.196: 21/tcp open ftp?

172.16.3.177: 135/tcp open msrpc Microsoft Windows RPC

172.16.3.176: 139/tcp open netbios-ssn Microsoft Windows netbios-ssn

172.16.3.198: 445/tcp open microsoft-ds?

172.16.3.162: 5357/tcp open http Microsoft HTTPAPI Httpd 2.0 (SSDP/UPnP)

172.16.3.199: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :  
SF-Port21-TCP-V7.93NI-7NDX-1/11NTI-ne63BE668NP-1686-pc-windows-windowsNrf(SF-NULL,4D,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-project.org/\r\n")&#x201F;(GenericLines,4D,"220-FileZill

172.16.3.160: SF-a-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-p

172.16.3.172: SF-project.org/\r\n")&#x201F;(Help,17C,"220-FileZilla-v20Server-v201.4.1.1\r\n22

172.16.3.200: SF-0-v20PLease-v20visit-v20https://filezilla-project.org/\r\n214-The-v20F

172.16.3.168: SF-following-v20commands-v20are-v20recognized.\r\n\r\n20NOP-v20x20USER-v20T

172.16.3.192: SF-YPE-v20SYST-v20SIZE-v20RNTQ-v20RNFQ-v20RND-v20x20REST-v20QUIT\r\n\r\n20H

172.16.3.189: SF-ELP-v20XKQD-v20MLST-v20MKD-v20x20EP5V-v20XCHD-v20NODP-v20AUTH-v20OPT5\

SE-x20DEL-v20LE-v20XCD-v20x20XCDPU-v20APPE-v20STOR-v20ALLQ-v20RETR-v20RDUx

SE-x20x20FEAT-v20CLNT-v20WFHT\r\n\r\n20MODE-v20XAND-v20PROT-v20ADAT-v20ABOR\

SE-x20XPMD-v20MDTH-v20LIST-v20MLSD-v20PBSZ\r\n\r\n20NLST-v20EPRT-v20PASS-v20

SE-STRU-v20PASV-v20STAT-v20PORT\r\n214x20HELPx20ok\.\r\n")&#x201F;(GetRequest,

SE-76,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20ht

SE-ps://filezilla-project.org/\r\n501x20What-v20are-v20you-v20tryng-v20

SE-to-v20do\?)x20Go-v20away\.\r\n")&#x201F;(HTTPOptions,61,"220-FileZilla-v20Ser

SE-ver-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-project.v

SE-org/\r\n500x20Wrong-v20command\.\r\n")&#x201F;(RTSPRequest,61,"220-FileZilla

SE-a-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-pr

SE-object.org/\r\n500x20Wrong-v20command\.\r\n")&#x201F;(RPCCheck,4D,"220-FileZ

SE-illa-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezill

SE-a-project.org/\r\n")&#x201F;(DNSVersionBndReqTCP,4D,"220-FileZilla-v20Serve

SE-r-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-v20serve

SE-g/\r\n")&#x201F;(DNSStatusRequestTCP,4D,"220-FileZilla-v20Server-v201.4.1.1\r

SE-i-v220-v20PLease-v20visit-v20https://filezilla-project.org/\r\n")&#x201F;(SSL

SE-iSessionReq,4D,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20v

SE-ist-v20https://filezilla-project.org/\r\n")&#x201F;(TerminalServerCookie,4D

SE-i,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https

SE-i://filezilla-project.org/\r\n")&#x201F;(TLSSessionReq,4D,"220-FileZilla-v20S

SE-iServer-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-project

SE-a-vorg/\r\n")&#x201F;

MAC Address: E8:D8:01:46:F8:1D (HP)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 34.68 seconds

Target: 172.16.3.189

Command: nmap -sR 172.16.3.189

Hosts: 172.16.3.187, 172.16.3.197, 172.16.3.170, 172.16.3.193, 172.16.3.196, 172.16.3.177, 172.16.3.176, 172.16.3.198, 172.16.3.162, 172.16.3.199, 172.16.3.160, 172.16.3.172, 172.16.3.200, 172.16.3.168, 172.16.3.192, 172.16.3.189

Services: Nmap Output Ports/Hosts Topology Host Details Scans

OS: Host

172.16.3.187: WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan. Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-01-11 15:21 India Standard Time NSOCK ERROR [0.0608s] ssl\_init\_helper(): OpenSSL legacy provider failed to load.

172.16.3.197: Nmap scan report for 172.16.3.189 Host is up (0.00043s latency).

172.16.3.170: Not shown: 995 closed tcp ports (reset)

172.16.3.193: PORT STATE SERVICE VERSION

172.16.3.196: 21/tcp open ftp?

172.16.3.177: 135/tcp open msrpc Microsoft Windows RPC

172.16.3.176: 139/tcp open netbios-ssn Microsoft Windows netbios-ssn

172.16.3.198: 445/tcp open microsoft-ds?

172.16.3.162: 5357/tcp open http Microsoft HTTPAPI Httpd 2.0 (SSDP/UPnP)

172.16.3.199: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :  
SF-Port21-TCP-V7.93NI-7NDX-1/11NTI-ne63BE668NP-1686-pc-windows-windowsNrf(SF-NULL,4D,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-project.org/\r\n")&#x201F;(GenericLines,4D,"220-FileZill

172.16.3.160: SF-a-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-p

172.16.3.172: SF-project.org/\r\n")&#x201F;(Help,17C,"220-FileZilla-v20Server-v201.4.1.1\r\n22

172.16.3.200: SF-0-v20PLease-v20visit-v20https://filezilla-project.org/\r\n214-The-v20F

172.16.3.168: SF-following-v20commands-v20are-v20recognized.\r\n\r\n20NOP-v20x20USER-v20T

172.16.3.192: SF-YPE-v20SYST-v20SIZE-v20RNTQ-v20RNFQ-v20RND-v20x20REST-v20QUIT\r\n\r\n20H

172.16.3.189: SF-ELP-v20XKQD-v20MLST-v20MKD-v20x20EP5V-v20XCHD-v20NODP-v20AUTH-v20OPT5\

SE-x20DEL-v20LE-v20XCD-v20x20XCDPU-v20APPE-v20STOR-v20ALLQ-v20RETR-v20RDUx

SE-x20x20FEAT-v20CLNT-v20WFHT\r\n\r\n20MODE-v20XAND-v20PROT-v20ADAT-v20ABOR\

SE-x20XPMD-v20MDTH-v20LIST-v20MLSD-v20PBSZ\r\n\r\n20NLST-v20EPRT-v20PASS-v20

SE-STRU-v20PASV-v20STAT-v20PORT\r\n214x20HELPx20ok\.\r\n")&#x201F;(GetRequest,

SE-76,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20ht

SE-ps://filezilla-project.org/\r\n501x20What-v20are-v20you-v20tryng-v20

SE-to-v20do\?)x20Go-v20away\.\r\n")&#x201F;(HTTPOptions,61,"220-FileZilla-v20Ser

SE-ver-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-project.v

SE-org/\r\n500x20Wrong-v20command\.\r\n")&#x201F;(RTSPRequest,61,"220-FileZilla

SE-a-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-pr

SE-object.org/\r\n500x20Wrong-v20command\.\r\n")&#x201F;(RPCCheck,4D,"220-FileZ

SE-illa-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezill

SE-a-project.org/\r\n")&#x201F;(DNSVersionBndReqTCP,4D,"220-FileZilla-v20Serve

SE-r-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-v20serve

SE-g/\r\n")&#x201F;(DNSStatusRequestTCP,4D,"220-FileZilla-v20Server-v201.4.1.1\r

SE-i-v220-v20PLease-v20visit-v20https://filezilla-project.org/\r\n")&#x201F;(SSL

SE-iSessionReq,4D,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20v

SE-ist-v20https://filezilla-project.org/\r\n")&#x201F;(TerminalServerCookie,4D

SE-i,"220-FileZilla-v20Server-v201.4.1.1\r\n220-v20PLease-v20visit-v20https

SE-i://filezilla-project.org/\r\n")&#x201F;(TLSSessionReq,4D,"220-FileZilla-v20S

SE-iServer-v201.4.1.1\r\n220-v20PLease-v20visit-v20https://filezilla-project

SE-a-vorg/\r\n")&#x201F;

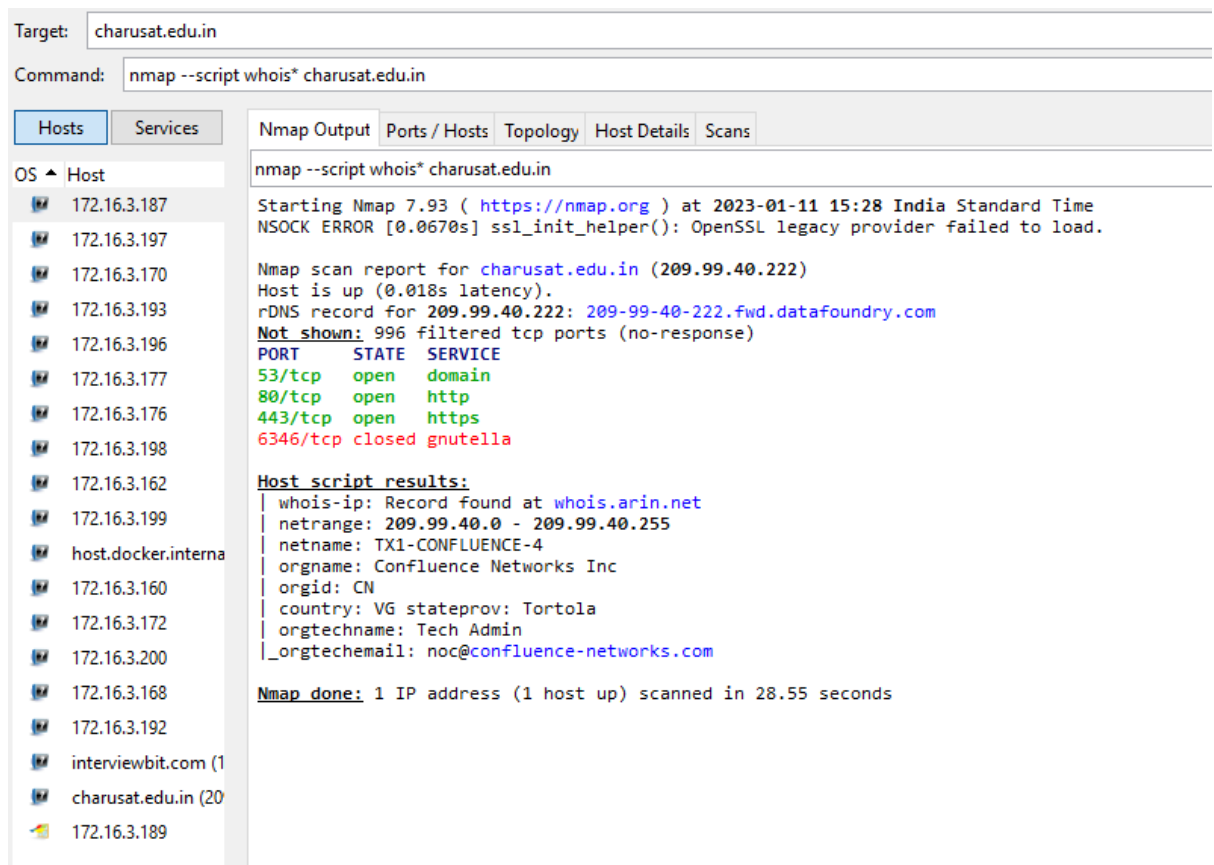
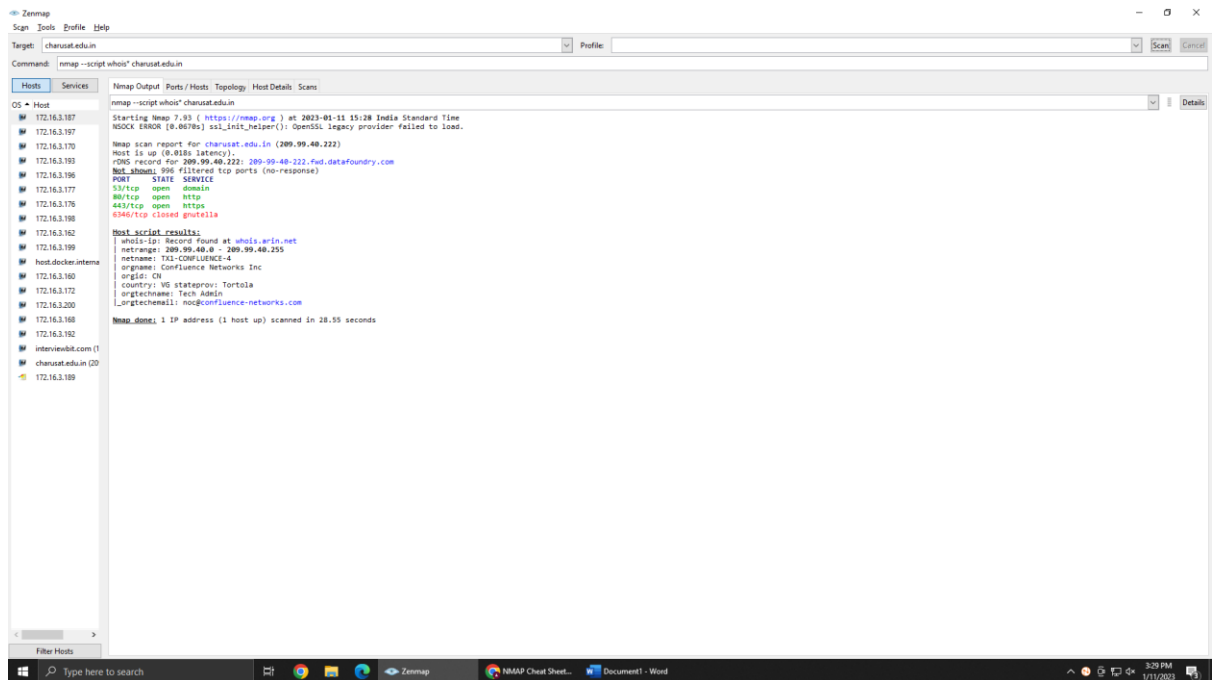
MAC Address: E8:D8:01:46:F8:1D (HP)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

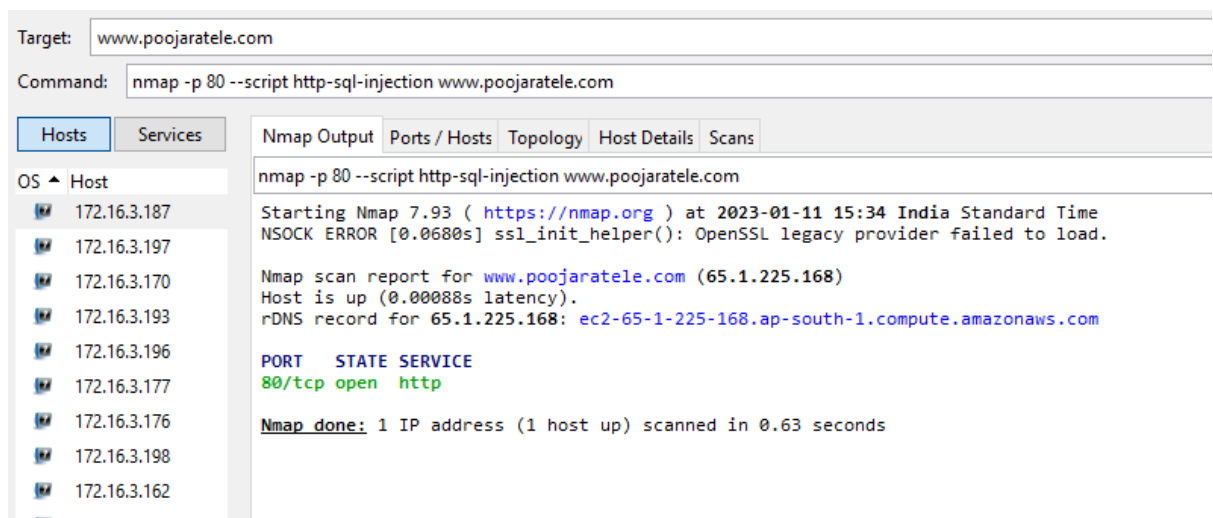
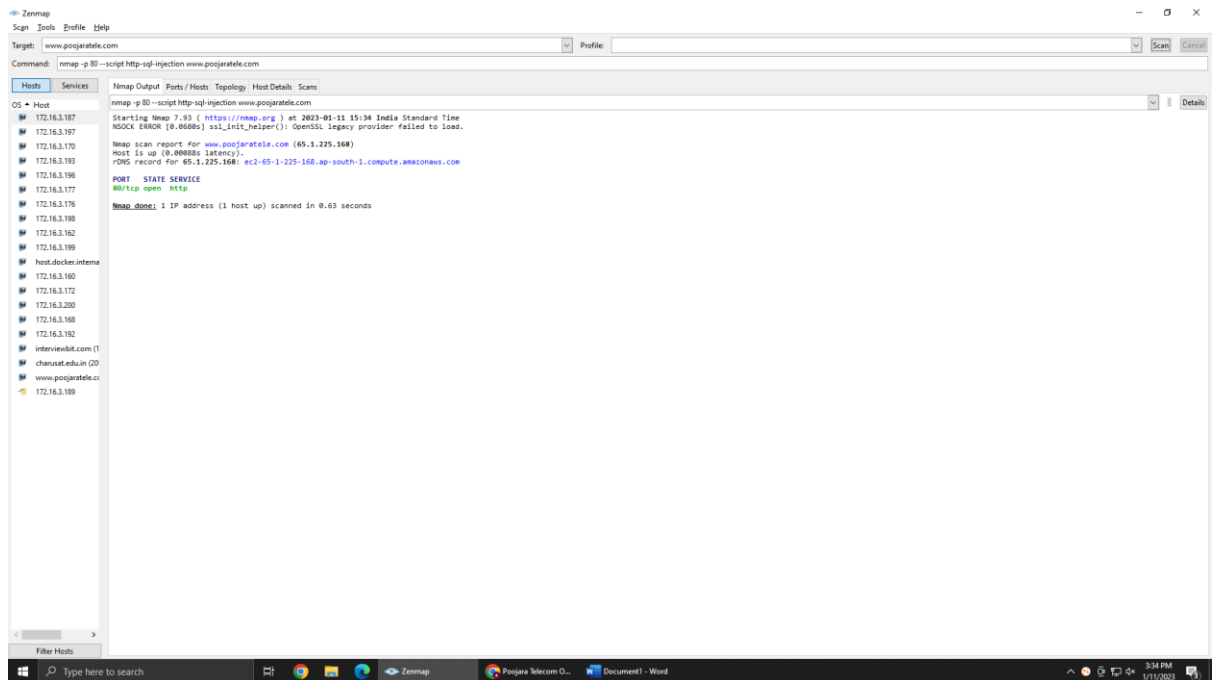
Nmap done: 1 IP address (1 host up) scanned in 34.68 seconds

Perform a RPC scan – nmap -sR 172.16.3.189



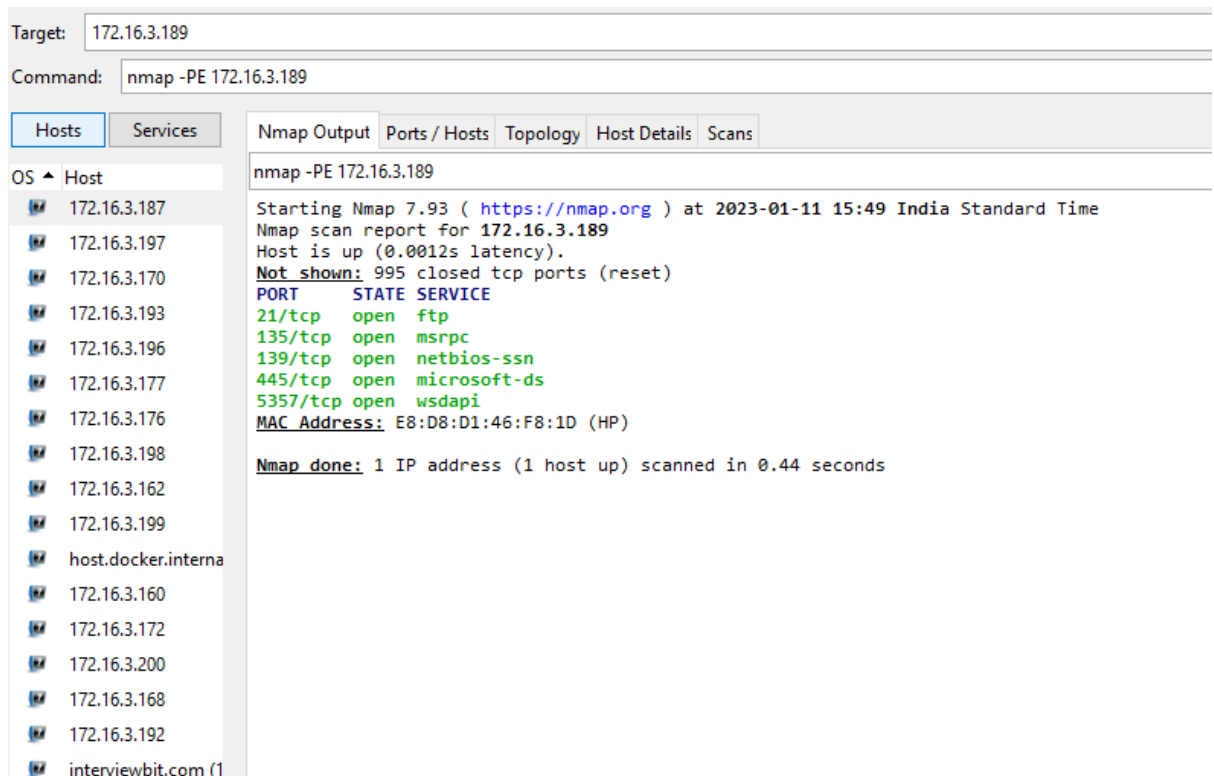
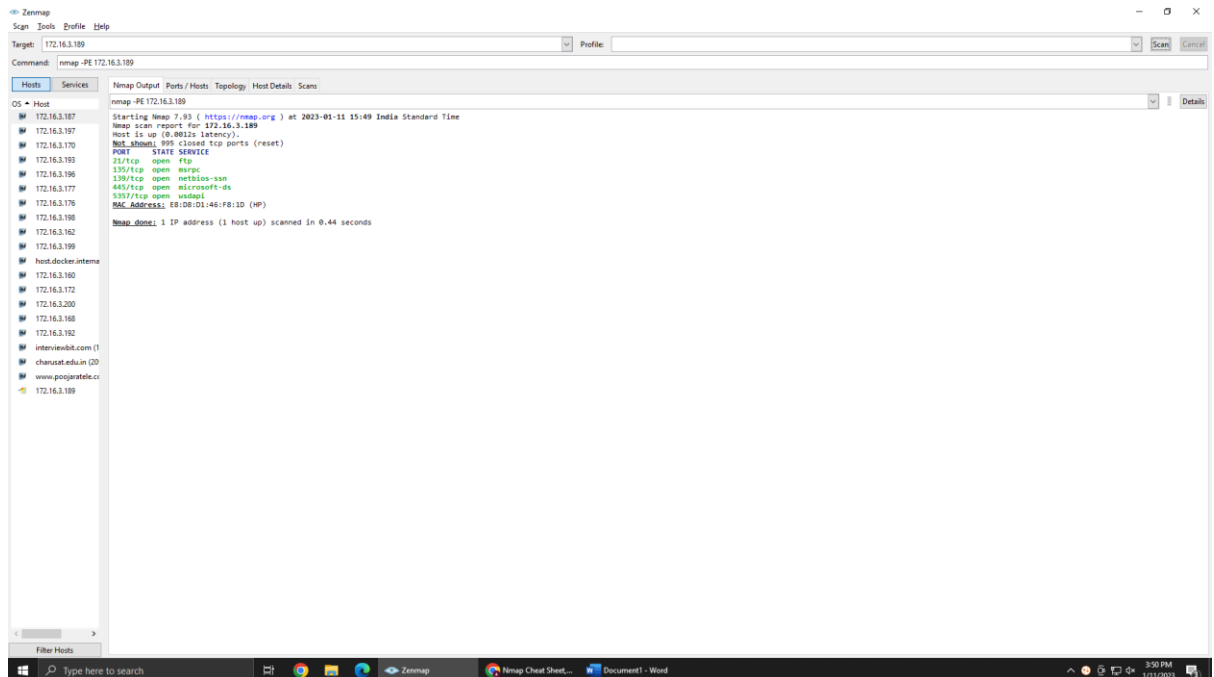
Query for who is - `nmap --script whois* charusat.edu.in`



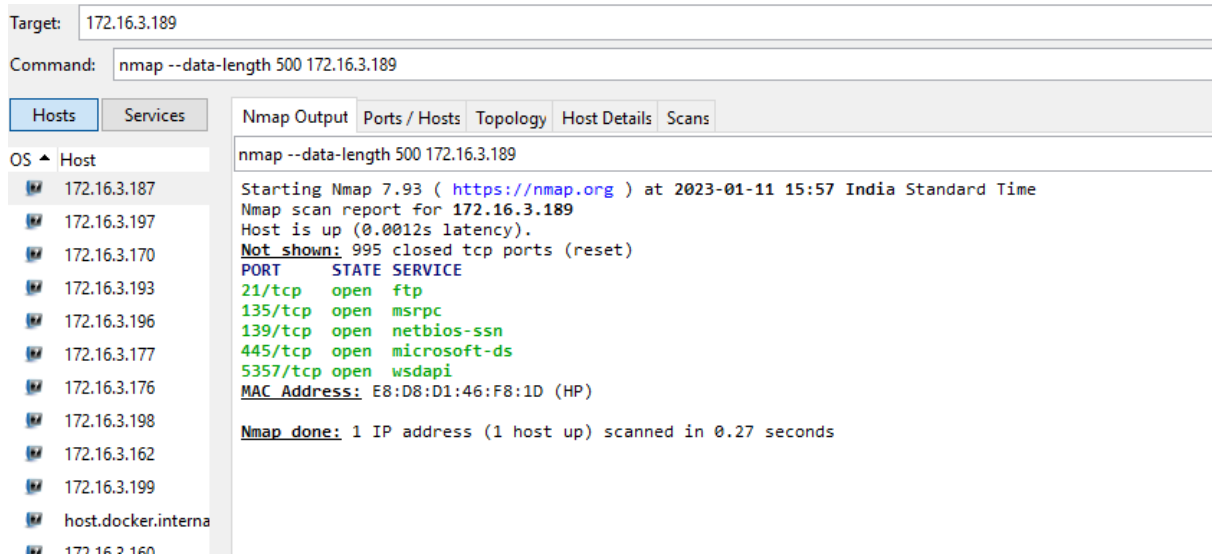
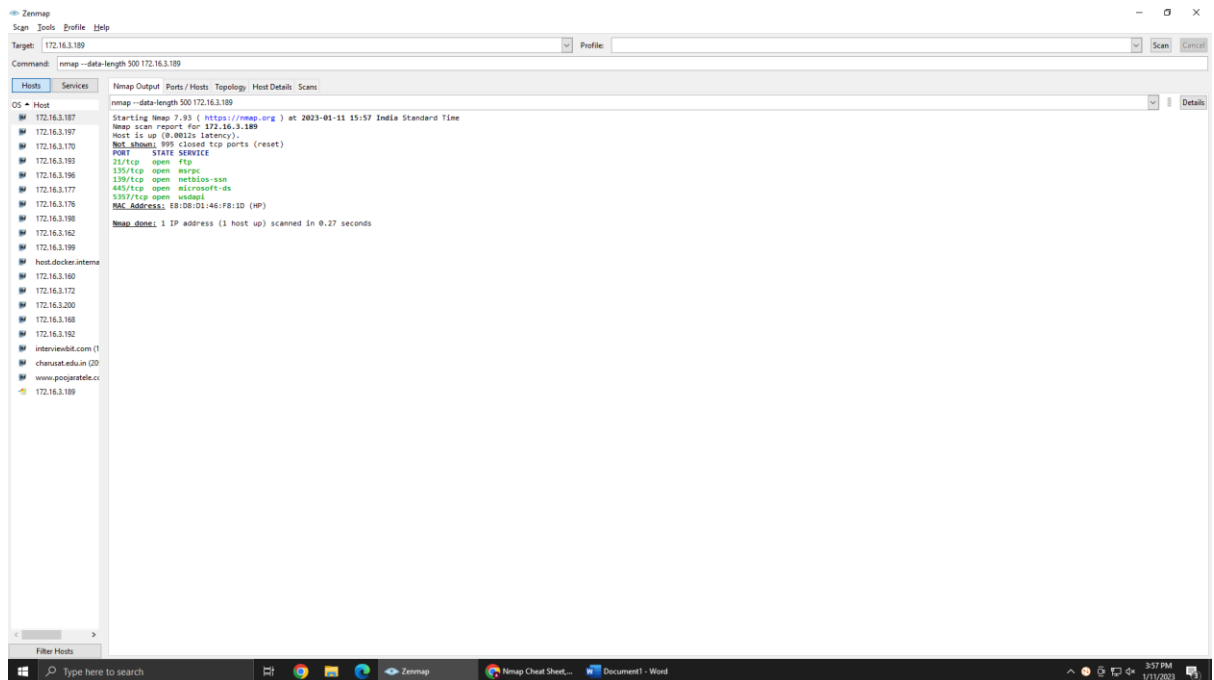


### SQL injection detection

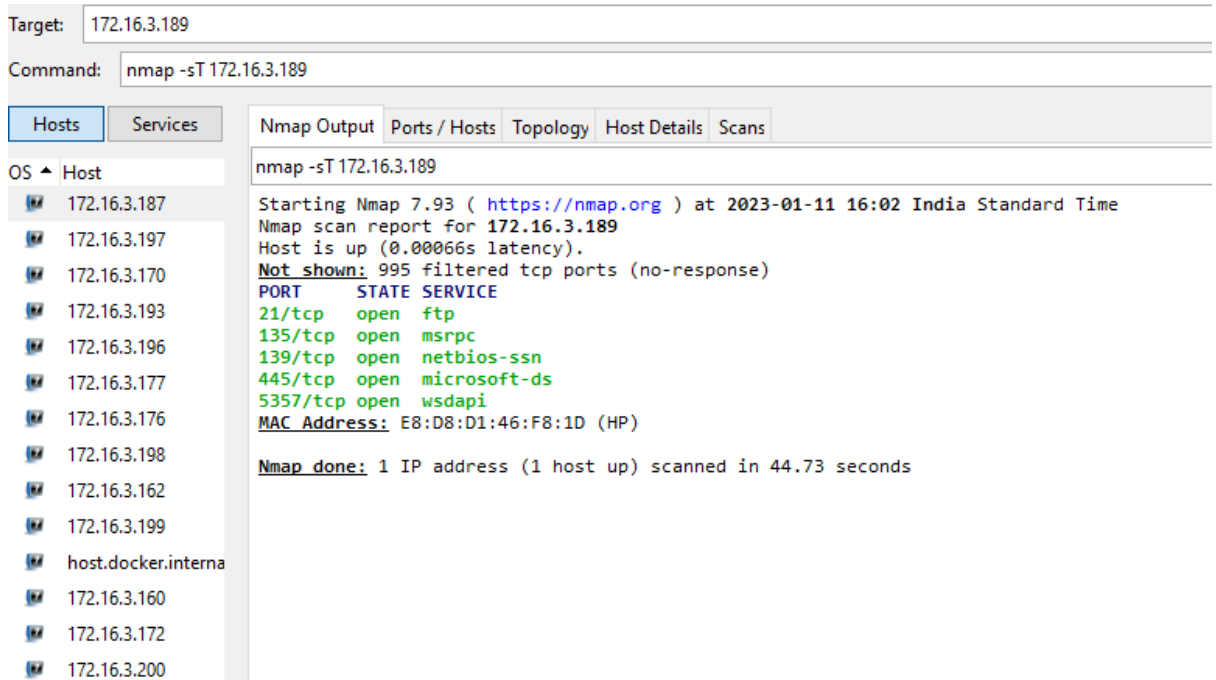
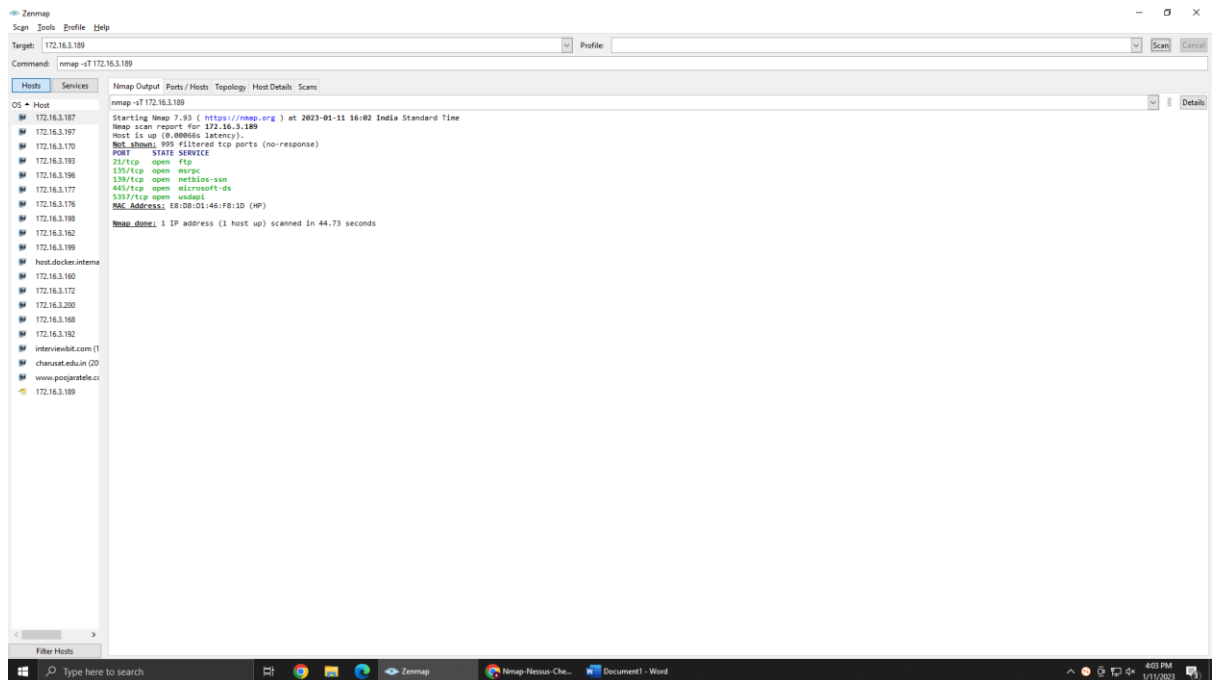
Nmap -p 80 --script http-sql-injection [www.poojaratele.com](http://www.poojaratele.com)



ICMP echo ping – nmap -PE 172.16.3.189



Randomly 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>