Task 1 : Scan your local Network for open port

**Network:**

A network is group of two or more device that are connect to each other to share data, resources and communicate with each other. These connections are made by wired or wireless.

**Working of Network:**

The Network work through communication protocols , that allow device to send , receive and interpret the data , Some protocols are:-

* + TCP/IP
  + HTTP/HTTPS
  + FTP
  + DNS

Example:

When open the website

-browser send the request over the network to website server

-the request travel through router and switches

-the server send back the website data in packet

-browser receives and display the website

**Local Network:**

Local Network or Local area Network , it’s a type of network that connect the computer and other device with limited range ,like :- Home , office ,school…

Key features:

-Scope(small area)

-Speed(Typically fast)

-Connectivity(wired and wireless)

-Security(more secure)

**Working of Local network:**

-Devices like computers, printers, and phones connect to a central device (like a router or switch).

- Each device gets a private IP address (like 192.168.0.5).

- Devices communicate directly with each other using internal IP addresses.

- A router connects the LAN to the internet, if needed.

**Simple diagram:**

[Internet]

|

[Router]

/ | \

[Laptop] [TV] [Phone]

**Port:**

In networking , port is the doorway through which the data enters and leave the device over a network

-it allow specific type of services and application

-Each port is identified by a port number, ranging from 0 to 65535.

**Open port:**

Open port means , actively listening for incoming connection

Ready to accept the data from other device over the network.

it help to direct traffic to the correct application on adevice

How to check for Open port :

\*netstat[built in tool]

\*nmap[network scanning]

**Security Note:**

* Closed Ports: No service is listening – safer.
* Open Ports: Useful but can be a security risk if the service is outdated or unprotected.

**Port scanning:**

Port scanning is the process of probing a computer or network device to identify which ports are open, closed, or filtered. It helps discover services running on a device and is commonly used in network security assessments.

**Working of Port scanning:**

A port scanner (like nmap) sends requests to various port numbers on a target system. Based on the response, it determines:

* Open Port – The port is accepting connections.
* Closed Port – The port is accessible but no service is listening.
* Filtered Port – The port is being blocked by a firewall or security software.

**Common Port Scanning Tools:**

* Nmap (most popular)
* Masscan (faster scanning)
* Zenmap (GUI for Nmap)
* Netcat
* Online scanners like Shodan, Censys

**How Port Scanning Helps**

**Uses and Benefits:**

1. **Network Security Testing**
   * Helps identify vulnerable or unnecessary open ports.
   * Useful for penetration testing and ethical hacking.
2. **Inventory of Services**
   * Reveals running services (like SSH, HTTP, FTP) on each machine.
3. **Firewall Testing**
   * Verifies which ports are correctly blocked or filtered by firewalls.
4. **Troubleshooting**
   * Helps diagnose connectivity or service-related issues.

**IP address:**

An IP (Internet Protocol) address is a unique identifier for a device on a network. It works like a home address for your device on the internet or a local network, allowing it to send and receive data.

Two main type of ip address are: Ipv4 and Ipv6

**IP Range:**

An IP range is a set of IP addresses, often used to define multiple devices in a network or group.

There are two type of range

--- Public ip range:

Assigned by ISP

Globally unique

--- Private IP range

Used in home and office

**TCP SYN scan:**

A TCP SYN scan is a common and stealthy method used in port scanning to determine the status of ports (open, closed, or filtered) on a target device.

It is often referred to as a “half-open scan” because it doesn't complete the full TCP three-way handshake. Instead, it sends only the initial SYN packet and analyzes the response.

**How a TCP SYN Scan Works:**

1. Scanner sends a SYN packet to the target port (start of TCP handshake).
2. Target replies:
   * SYN-ACK → Port is open.
   * RST (Reset) → Port is closed.
   * No response / filtered → Port is filtered by a firewall or device.
3. Scanner sends RST (Reset) instead of ACK to avoid completing the handshake – this keeps the connection half-open and undetectable to some logging systems.

**Network reconnaissance:**

**Network reconnaissance** is the process of **gathering information about a target network** to identify systems, services, vulnerabilities, and potential attack paths. It’s often the **first phase in ethical hacking** or **cyberattacks**, similar to spying before launching an attack.

Type:

\*Passive

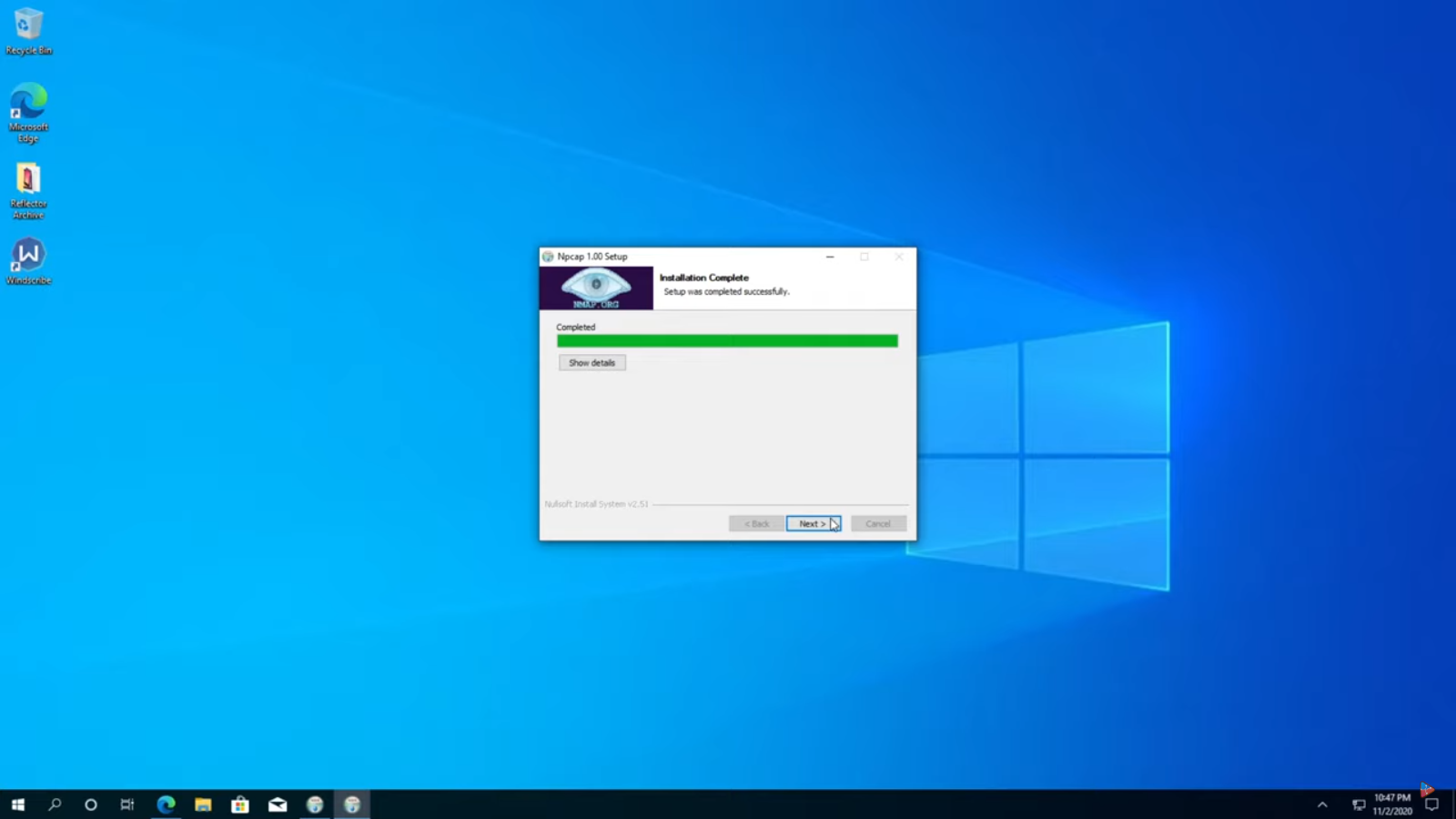
\*Active

**Benefits (in Ethical Hacking / Pentesting)**

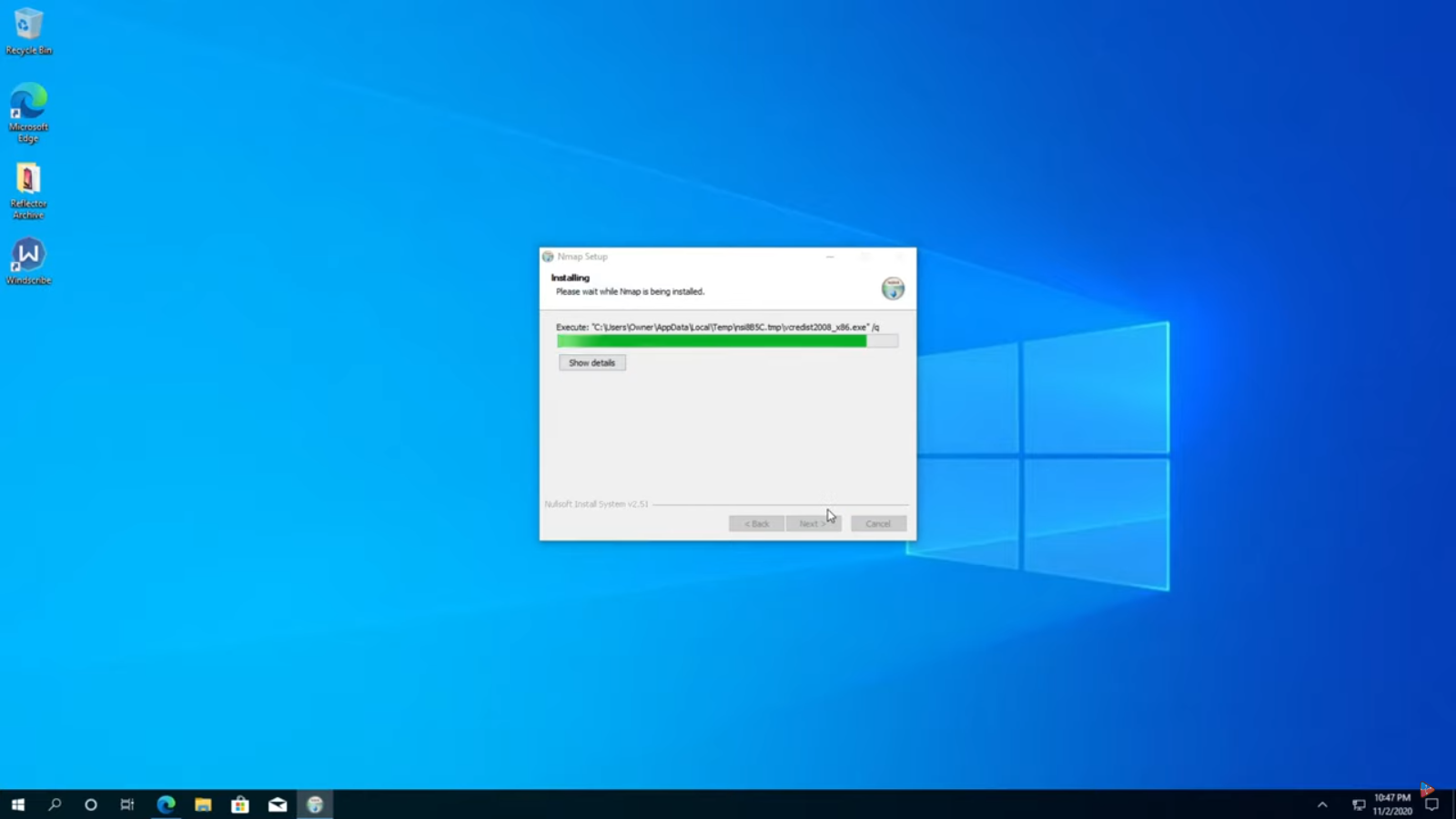
* Helps identify **attack surfaces**
* Maps out **network architecture**
* Detects **weak configurations** (e.g., open ports, outdated services)
* Prepares for **penetration testing**

**Scanning the local network for open port using the nmap**

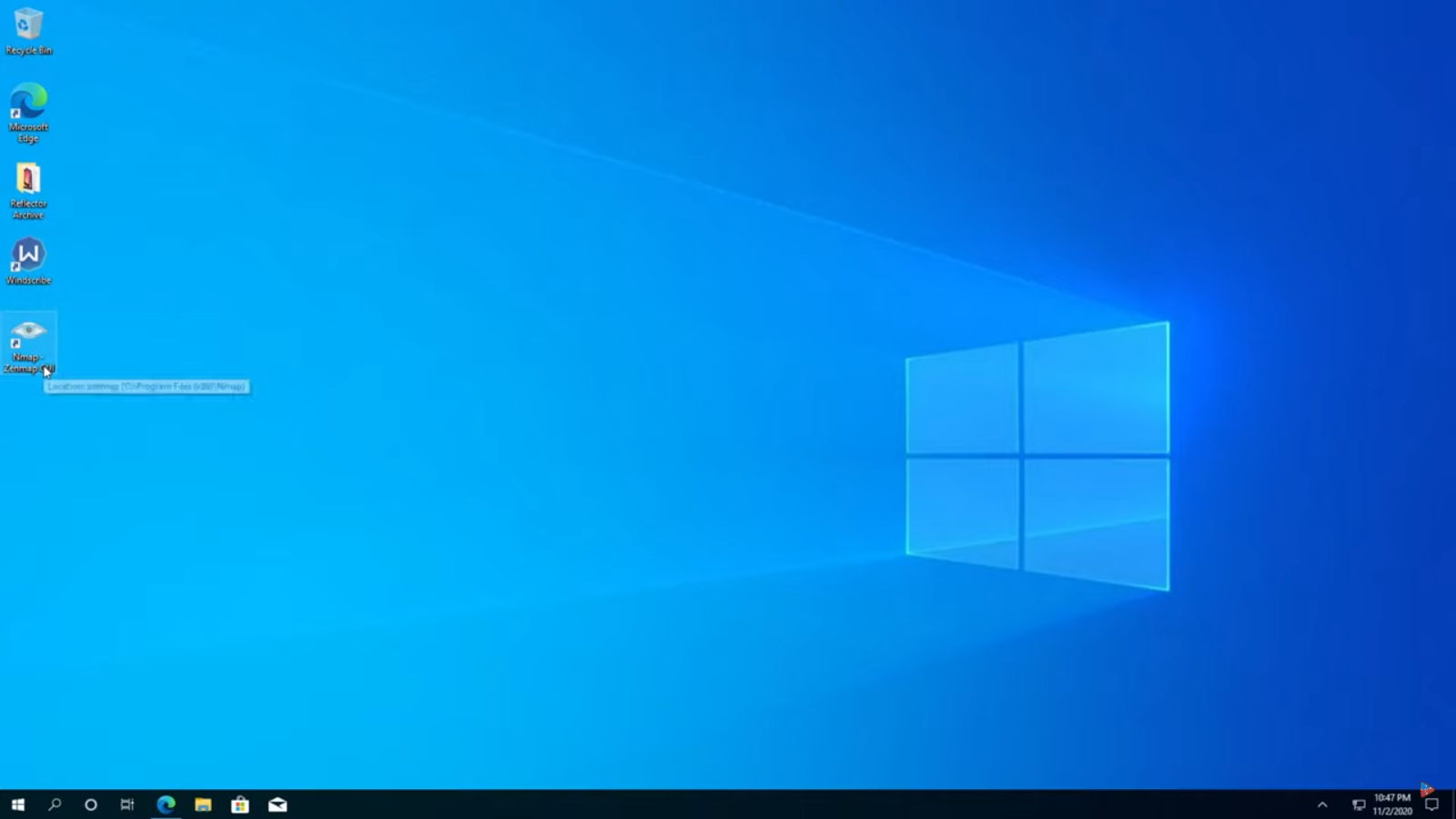
**Install the nmap from the browser(from official wesite)**



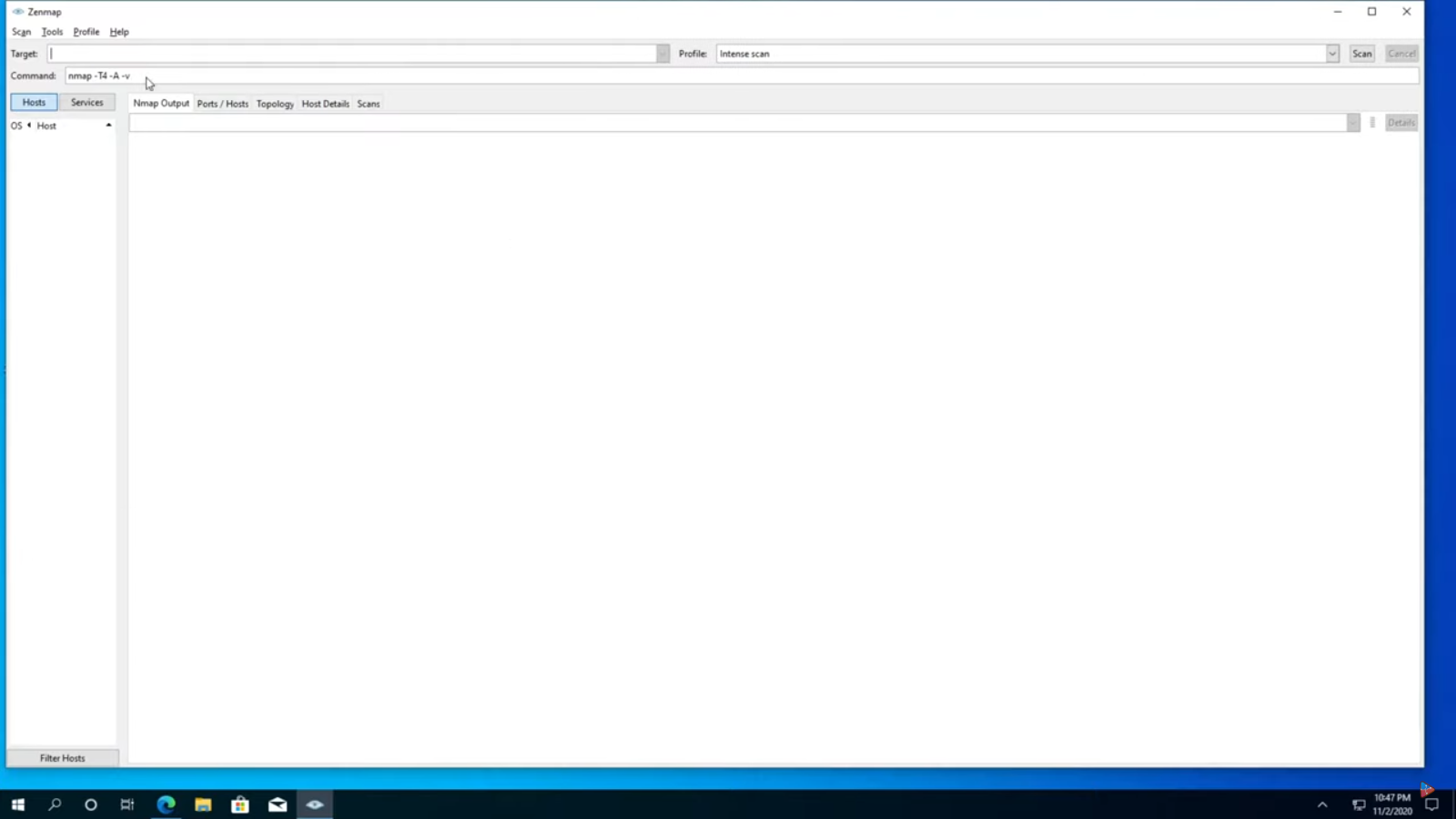
**Set up the nmap for the scanning**



**Then the open the nmap by click the icon on the desktop**

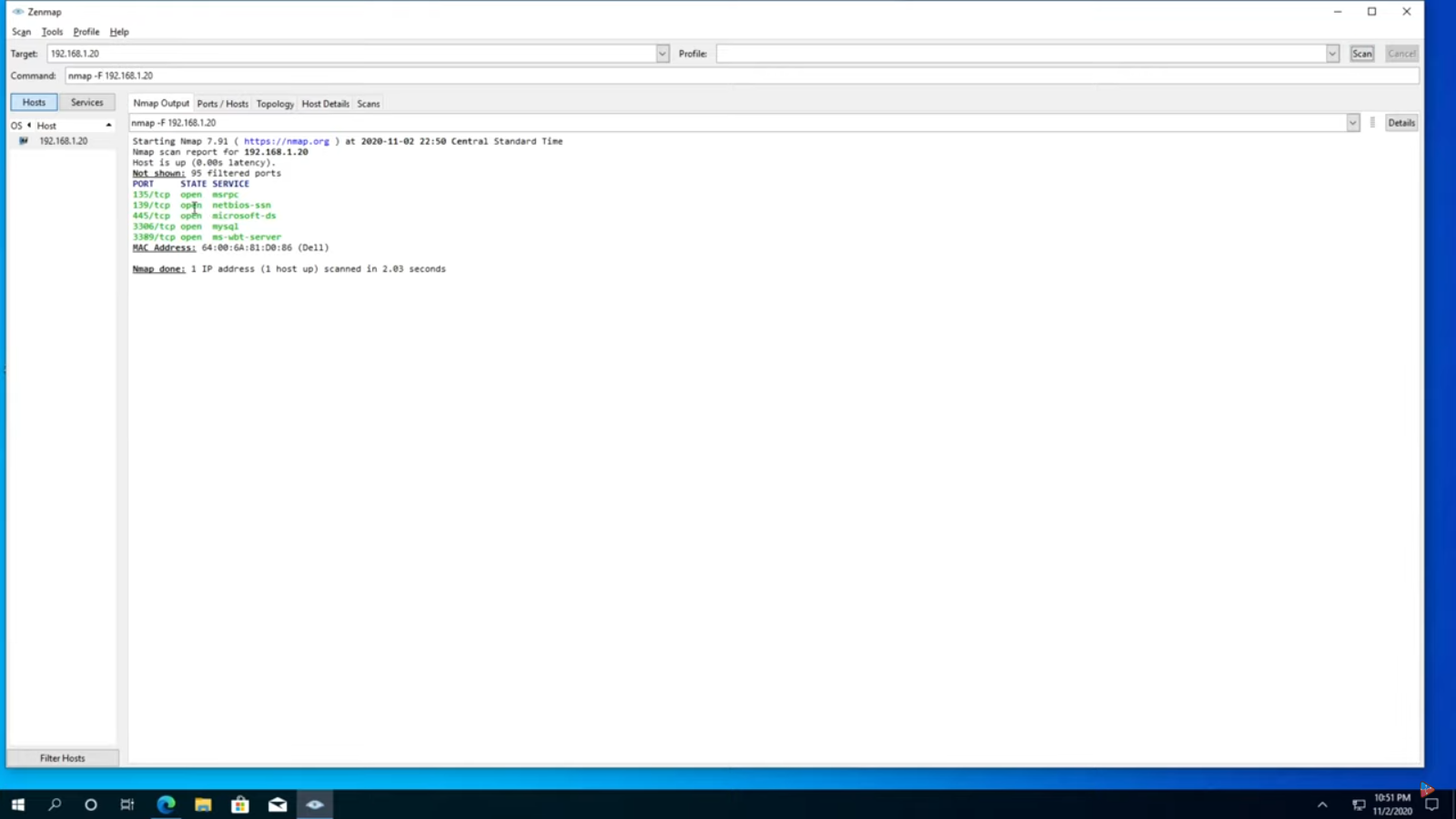


**Then namp pag will open**



**Enter the ip address for the scan for open port**

**Then entering , click for scan in right coner , then it will begin for scanning then give the open port in the ip address**



**This the process of scanning the local network(ip address) for open port .**