Question 3

Need to be perform below tasks

Task 1: Install Nginx inside the Ubuntu machine and host a website.
Task 2: Come back to your host machine (windows/Linux/mac) and scan the virtual machine using Nmap.
Task 3: Create the documentation of the process and the output of the scan.
Task 4: Observe the ports which are open.

Soln.
I'm using windows WSL Ubuntu - 22.04. I have installed Ubuntu on my laptop & going to host a simple website on it & scan the VM from my laptop OS using Nmap.

root@DESKTOP-0532ICS:~# **cat /etc/os-release**
PRETTY_NAME="Ubuntu 22.04.2 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
:
:
root@DESKTOP-0532ICS:~#

Installing nginx by using below steps:

- First update the OS

root@DESKTOP-0532ICS:~# **apt update**

- Install the nginx service

root@DESKTOP-0532ICS:~# **apt install nginx**

Creating our own website

Default page is placed in `/var/www/html/` location. We have to be placed our static pages here.

Let's create simple HTML page in `/var/www/Israr/` index.html

```
root@DESKTOP-0532ICS:~# mkdir /var/www/Israr
root@DESKTOP-0532ICS:~# cd /var/www/Israr/
root@DESKTOP-0532ICS:/var/www/Israr# nano index.html
root@DESKTOP-0532ICS:/var/www/Israr#
```

```
<!doctype html>
<html>
<head>
    <meta charset="utf-8">
    <title>Hello, Nginx!</title>
</head>
<body>
    <h1>Hello, Nginx!</h1>
    <p>We have just configured our Nginx web server on Ubuntu Server!</p>
</body>
</html>
```

Setting up virtual host
To set up virtual host, we need to create file in `/etc/nginx/sites-enabled/` directory.

- For this Israr directory, we will make our site available on 81 port, not the standard 80 port.

```
root@DESKTOP-0532ICS:/var/www/Israr# cd /etc/nginx/sites-enabled
root@DESKTOP-0532ICS:/etc/nginx/sites-enabled# nano israr
root@DESKTOP-0532ICS:/etc/nginx/sites-enabled#
```

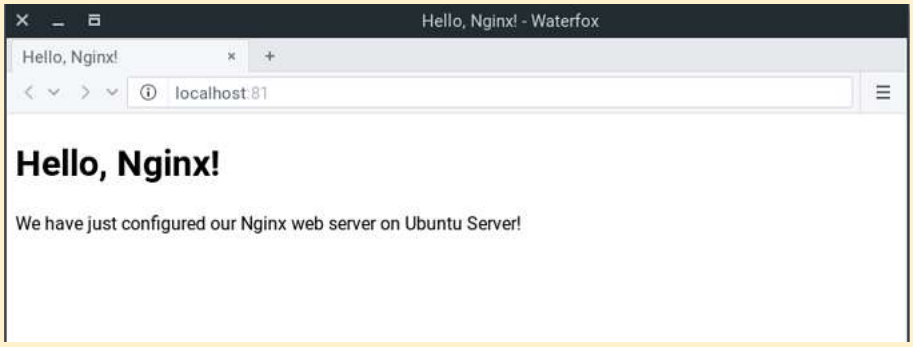
```
server {
        listen 81;
        listen [::]:81;

        server_name example.ubuntu.com;

        root /var/www/tutorial;
        index index.html;

        location / {
                try_files $uri $uri/ =404;
        }
}
```

- `root` is a directory where we have placed our .html file. `index` is used to specify file available when visiting root directory of site. `server_name` can be anything you want, because you aren't pointing it to any real domain by now.

Activating virtual host and testing results
To make our site working, simply restart Nginx service.

```
root@DESKTOP-0532ICS:~#
root@DESKTOP-0532ICS:~# service nginx restart
 * Restarting nginx nginx
root@DESKTOP-0532ICS:~#
root@DESKTOP-0532ICS:~# service nginx status
 * nginx is running
root@DESKTOP-0532ICS:~#
```

Let's check if everything works as it should. Open our newly created site in web browser. Remember that we used :81 port.



Scan the virtual machine using Nmap

check the Ip address of my VM by using: 'ifconfig'

inet 192.168.164.211 netmask 255.255.255.0 broadcast 192.168.164.255

```
root@DESKTOP-0532ICS:~# ifconfig
eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.227.1  netmask 255.255.255.0  broadcast 192.168.227.255
        inet6 fe80::e8a7:6144:4143:b7a6  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 00:50:56:c0:00:00  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::59ee:e77d:ad05:2de2  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 0a:00:27:00:00:08  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 1500
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0xfe<compat,link,site,host>
        loop  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.164.211  netmask 255.255.255.0  broadcast 192.168.164.255
        inet6 2409:4050:2e41:8a0b:27d5:6f7c:97c6:763c  prefixlen 64  scopeid 0x0<global>
        inet6 2409:4050:2e41:8a0b:c065:4656:d51c:c9a9  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::2855:1661:1f33:151  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 78:e4:00:23:70:e4  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@DESKTOP-0532ICS:~#
```

then check the Ip address and check the ports which are opened

Discovered open port 135/tcp on 192.168.164.211

Discovered open port 139/tcp on 192.168.164.211

Discovered open port 443/tcp on 192.168.164.211

Discovered open port 80/tcp on 192.168.164.211

Discovered open port 22/tcp on 192.168.164.211

Discovered open port 445/tcp on 192.168.164.211

Discovered open port 81/tcp on 192.168.164.211

Discovered open port 8090/tcp on 192.168.164.211

Discovered open port 902/tcp on 192.168.164.211

Discovered open port 912/tcp on 192.168.164.211

```
WARNING: Could not import all necessary Npcap functions. You may need to upgrade to the latest
version from https://npcap.com. Resorting to connect() mode -- Nmap may not function completely
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-06 17:29 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:29
Completed NSE at 17:29, 0.01s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating Ping Scan at 17:29
Scanning 192.168.164.211 [2 ports]
Completed Ping Scan at 17:29, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:29
Completed Parallel DNS resolution of 1 host. at 17:30, 16.54s elapsed
Initiating Connect Scan at 17:30
Scanning 192.168.164.211 [1000 ports]
Discovered open port 135/tcp on 192.168.164.211
Discovered open port 139/tcp on 192.168.164.211
Discovered open port 443/tcp on 192.168.164.211
Discovered open port 80/tcp on 192.168.164.211
Discovered open port 22/tcp on 192.168.164.211
Discovered open port 445/tcp on 192.168.164.211
Discovered open port 81/tcp on 192.168.164.211
Discovered open port 8090/tcp on 192.168.164.211
Discovered open port 902/tcp on 192.168.164.211
Discovered open port 912/tcp on 192.168.164.211
Completed Connect Scan at 17:30, 4.99s elapsed (1000 total ports)
Initiating Service scan at 17:30
Scanning 10 services on 192.168.164.211
Completed Service scan at 17:30, 12.18s elapsed (10 services on 1 host)
```