Assignment Hero-Vired 3

All files are uploaded to github repo HeroVired_Assignment 3.

1. *Index.html for question1, python script for question 2 and documentation with a screenshot of NMAP for question 3.*
2. *I will use both wamp apache servers to host index.html.*
3. *Python script to check the status of subdomains using sleep for 60 seconds and then again run the loop.*

GIthub - [nksharma063/server_assigment_herovired: Assignment number three for herovired for configuration on apache and niginx (github.com)]

Question 1

Ans:. Steps, i took to complete the given assignment.

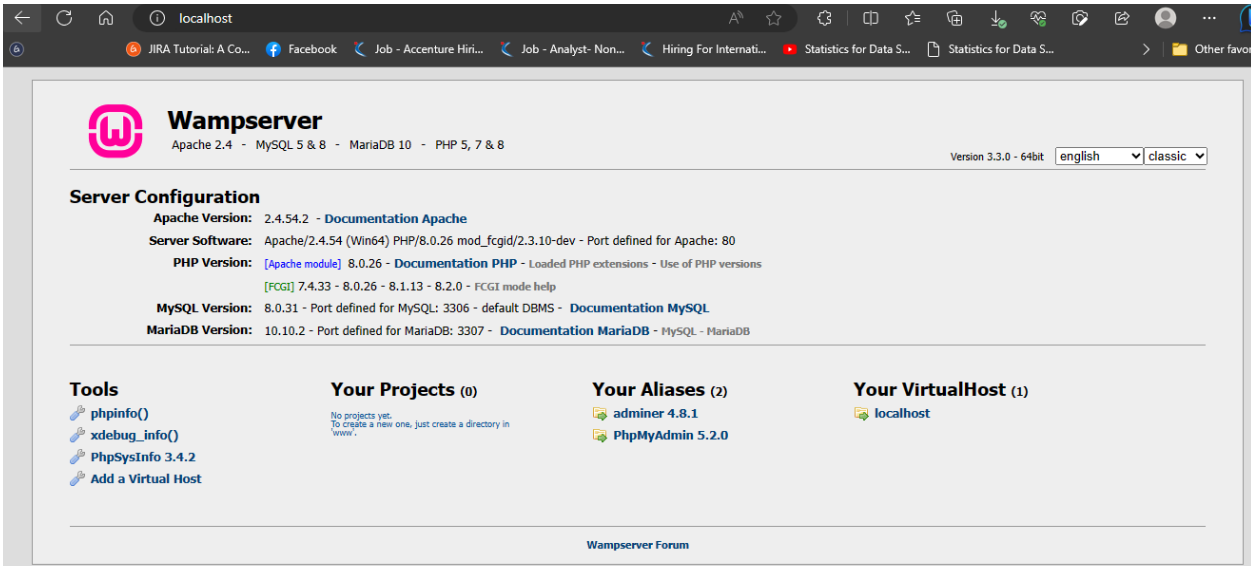
1. I created one index.html file.
2. I tested the port 80 using wamp server itself which is using netstat.

```
Test which uses port 80
Tested by command netstat filtered on port 80
Test for TCP. Your port 80 is used by a processus with PID = 2056
The processus of PID 2056 is 'httpd.exe' Session: Services
The service of PID 2056 for 'httpd.exe' is 'wampapache64'
This service is from Wampserver - It is correct
Test for TCPv6
Your port 80 is used by a processus with PID = 2056
The processus of PID 2056 is 'httpd.exe' Session: Services
The service of PID 2056 for 'httpd.exe' is 'wampapache64'
This service is from Wampserver - It is correct
Tested by attempting to open a socket on port 80 =====

Your port 80 is actually used by :Server: Apache/2.4.54 (Win64) PHP/8.0.26
mod_fcgid/2.3.10-dev
```

“””

3. I will deploy the index.html on wamp server on port 80.

4.



Wampserver
Apache 2.4 - MySQL 5 & 8 - MariaDB 10 - PHP 5, 7 & 8

Version 3.3.0 - 64bit english classic

Server Configuration

Apache Version:	2.4.54.2 - Documentation Apache
Server Software:	Apache/2.4.54 (Win64) PHP/8.0.26 mod_fcgid/2.3.10-dev - Port defined for Apache: 80
PHP Version:	[Apache module] 8.0.26 - Documentation PHP - Loaded PHP extensions - Use of PHP versions
	[FCGI] 7.4.33 - 8.0.26 - 8.1.13 - 8.2.0 - FCGI mode help
MySQL Version:	8.0.31 - Port defined for MySQL: 3306 - default DBMS - Documentation MySQL
MariaDB Version:	10.10.2 - Port defined for MariaDB: 3307 - Documentation MariaDB - MySQL - MariaDB

Tools
- phpinfo()
- xdebug_info()
- PhpSysInfo 3.4.2
- Add a Virtual Host

Your Projects (0)

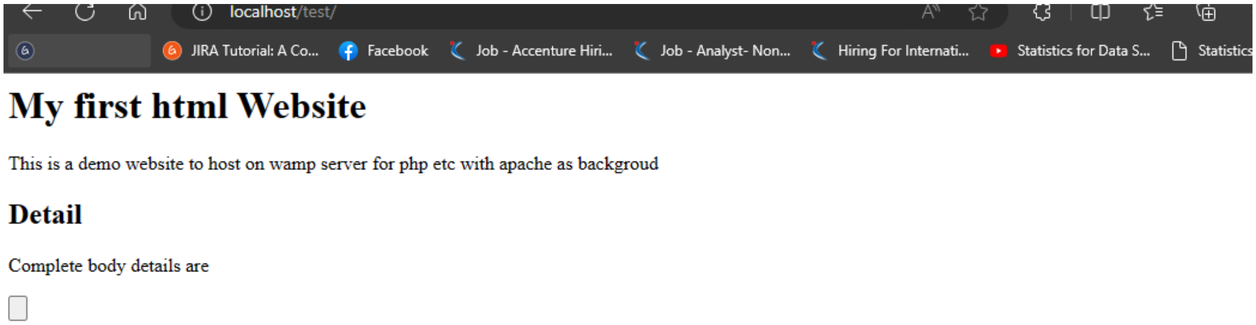
No projects yet.
To create a new one, just create a directory in 'www'.

Your Aliases (2)
- adminer 4.8.1
- PhpMyAdmin 5.2.0

Your VirtualHost (1)
- localhost

Wampserver Forum

5. I created one folder inside www as test and copied pasted by index.html there . I was able to open the 127.0.0.1/test and result as



My first html Website

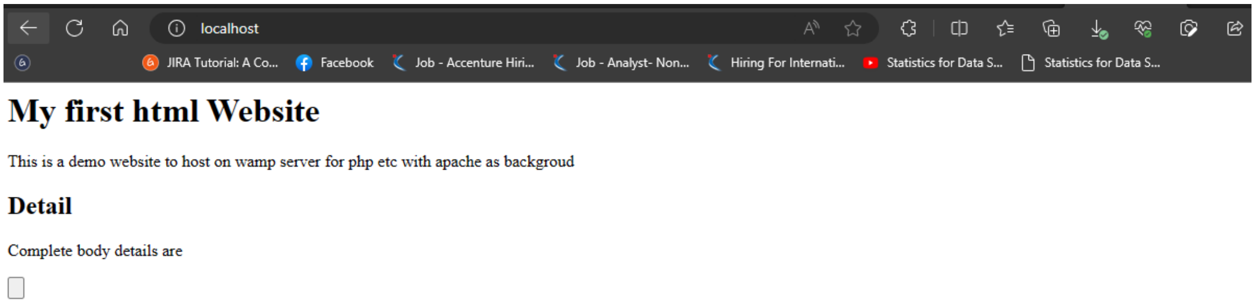
This is a demo website to host on wamp server for php etc with apache as backgroud

Detail

Complete body details are

□

6. I removed the test folder and intended the direction of the world wide web interface to index.html and it worked fine as well.



My first html Website

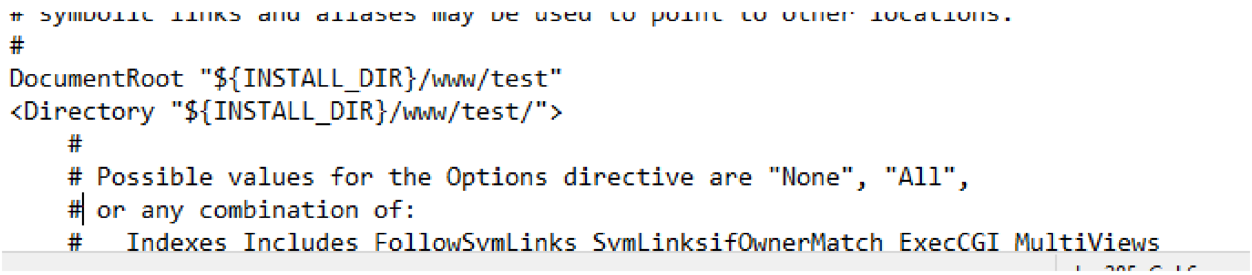
This is a demo website to host on wamp server for php etc with apache as backgroud

Detail

Complete body details are

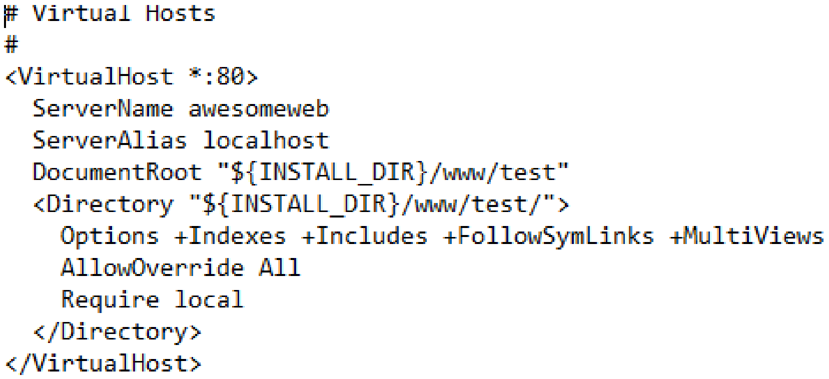
□

7. I changed the httpd.conf file under ~/bin/apache/conf/httpd.conf , and changed teh directory to /test/ /www/test



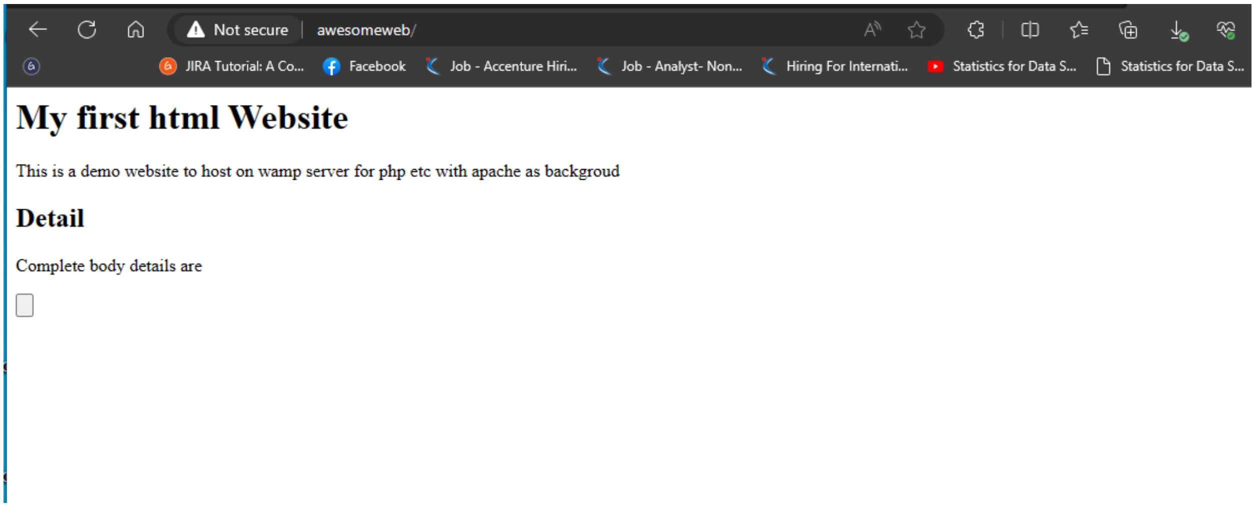
```
# Symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "${INSTALL_DIR}/www/test"
<Directory "${INSTALL_DIR}/www/test/">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
```

8. I also updated the virtual directory.conf fi



```
# Virtual Hosts
#
<VirtualHost *:80>
  ServerName awesomeweb
  ServerAlias localhost
  DocumentRoot "${INSTALL_DIR}/www/test"
  <Directory "${INSTALL_DIR}/www/test/">
    Options +Indexes +Includes +FollowSymLinks +MultiViews
    AllowOverride All
    Require local
  </Directory>
</VirtualHost>
```

9. I changed the C:\Windows\System32\drivers\etc as suggested on the internet. I created the server alias along with localhost. It seems to be working fine.



My first html Website

This is a demo website to host on wamp server for php etc with apache as backgroud

Detail

Complete body details are

.

10. I also installed nginx and checked the configuration to deploy my website on port number 80 for localhost on linux through wsl.

Ques 2 A website can have many subdomains and different services are running on them. Write a Python script to check the status of the subdomains which are up or down. The script should automatically check the status every min and should update it in tabular format on the screen. Write a detailed documentation of it.

Ans.
Tools:
Library : Googlesearch, flask
Module : os, time, search, request, render_request,
ChatGPT
Steps i took to accomplish the task:

1. I have called the google search library which I found on the internet for python to collect all the subdomains.
2. I also created one iterated loop while appending *site: with domain to collect all the available subdomains.
3. I created the filter which will split the string by / and then fetch the 0 index value that is subdomain.(subdomain.domain.com)
4. I added the subdomain with domain in sorted loop through set to get the uniqueness
5. I implemented os.system library to check the availability of the subdomains
6. I also rendered the result on port number 3000, to render the results on the browser, which I collected in dict format.
7. I will display either the results or create on a jinja 2 template and redirect these results into that so that a tabular format can be displayed on the browser.
8. Once done, i will submit or upload my github repository in the link

Ques3. Now, complete the given 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.

Ans. We took the following steps as suggested above and performed experiments on virtual box and wsl2.

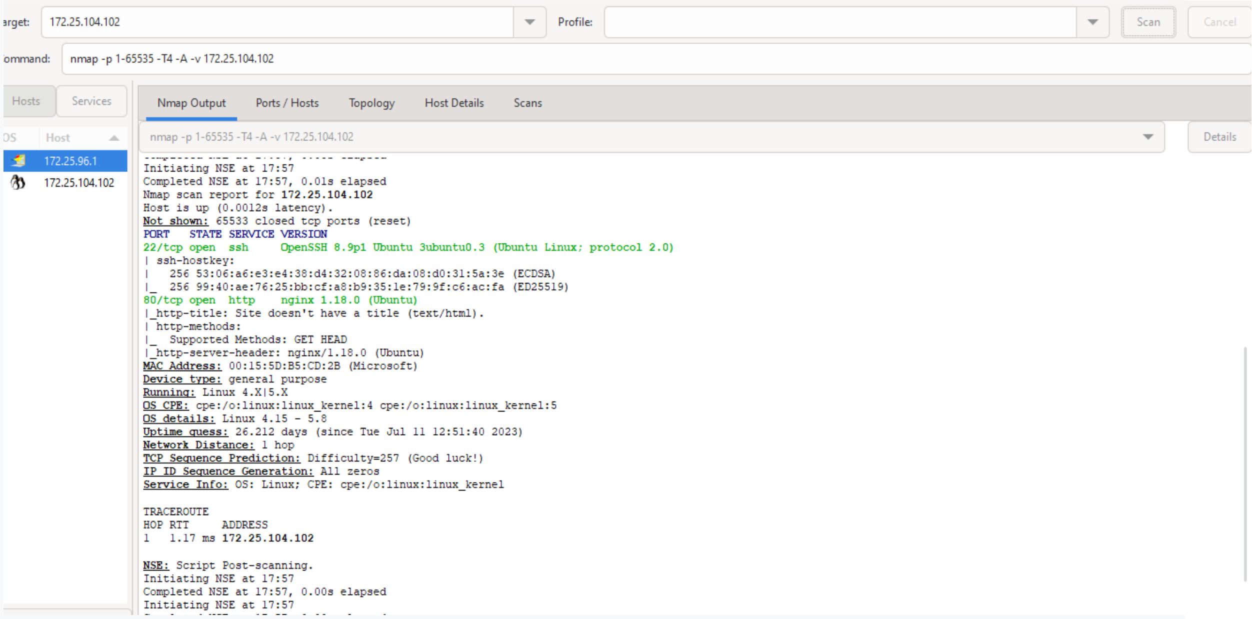
1). Installed the Nginx and hosted the website on port 80.

2) When we did scanning from host machine to virtual machines sin oracle and wsl2, we found two ports are 80 as of nginx and 22 for ssh server which we installed for experiment.

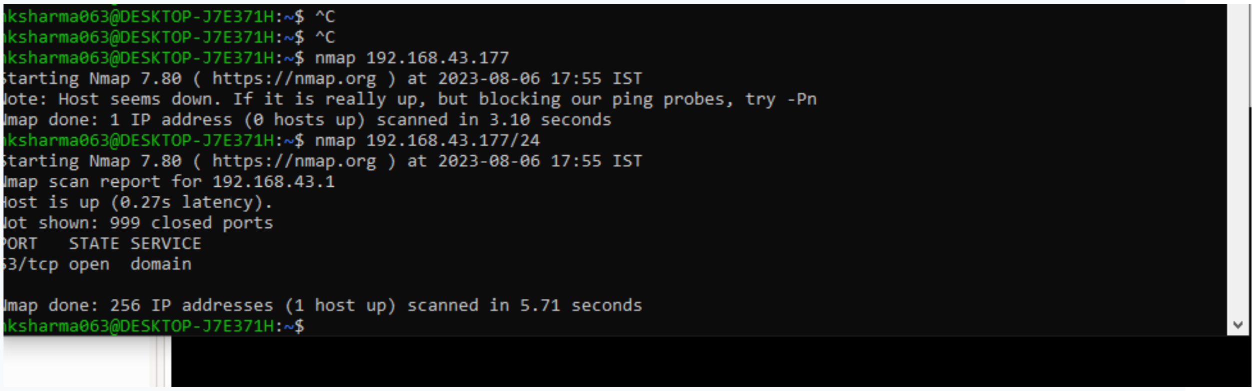
3) We performed scanning from host to vm and vice versa and found that host can scan servers with ports of server inside the machine but not the services and everything like you can scan your local ip with nmap.

VM can reach the gateway of the internet and nothing else on host, once nmap is performed from VM.

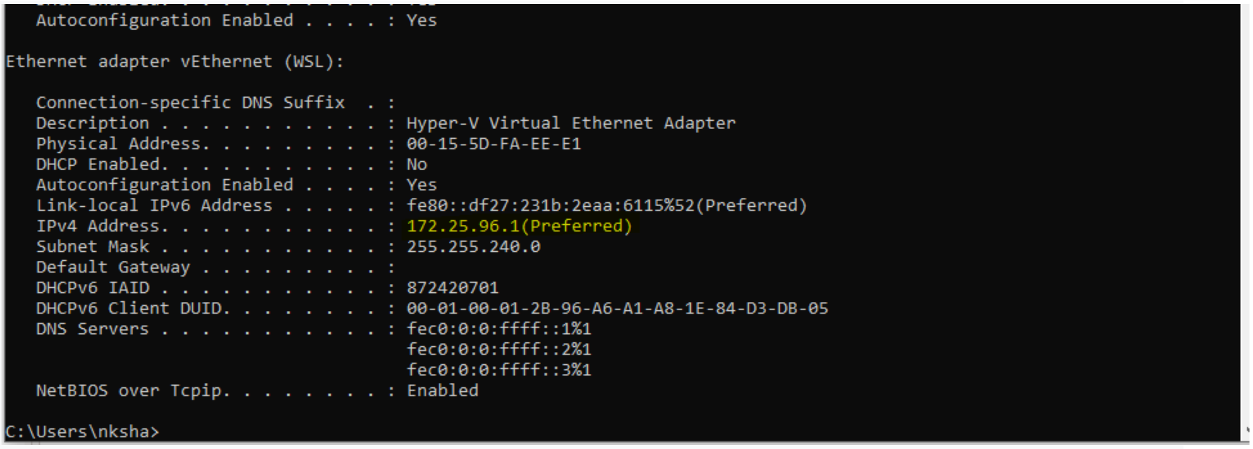
4) Port Open are 80 and 22



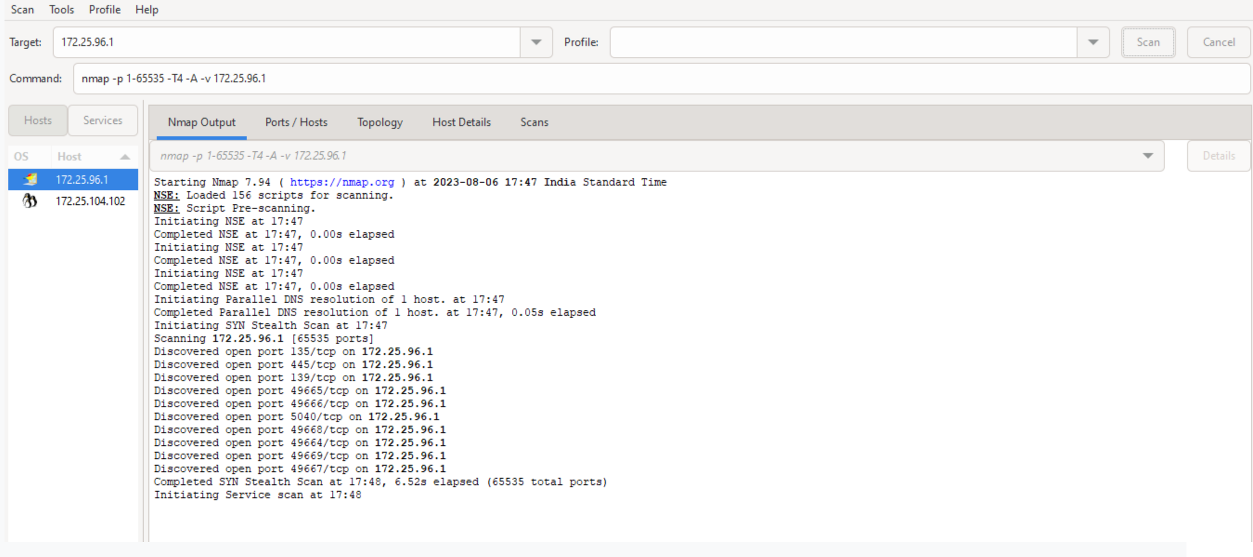
```
Initiating NSE at 17:57
Completed NSE at 17:57, 0.01s elapsed
Nmap scan report for 172.25.104.102
Host is up (0.0012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 53:06:a6:e3:e4:38:d4:32:08:86:da:08:d0:31:5a:3e (ECDSA)
|_  256 99:40:ae:76:25:bb:cf:a8:b9:35:1e:79:9f:c6:ac:fa (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.18.0 (Ubuntu)
MAC Address: 00:15:5D:B5:CD:2B (Microsoft)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 26.212 days (since Tue Jul 11 12:51:40 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.17 ms 172.25.104.102

NSE: Script Post-scanning.
Initiating NSE at 17:57
Completed NSE at 17:57, 0.00s elapsed
Initiating NSE at 17:57
```



```
ksharma063@DESKTOP-J7E371H:~$ ^C
ksharma063@DESKTOP-J7E371H:~$ ^C
ksharma063@DESKTOP-J7E371H:~$ nmap 192.168.43.177
tarting Nmap 7.80 ( https://nmap.org ) at 2023-08-06 17:55 IST
ote: Host seems down. If it is really up, but blocking our ping probes, try -Pn
map done: 1 IP address (0 hosts up) scanned in 3.10 seconds
ksharma063@DESKTOP-J7E371H:~$ nmap 192.168.43.177/24
tarting Nmap 7.80 ( https://nmap.org ) at 2023-08-06 17:55 IST
map scan report for 192.168.43.1
ost is up (0.27s latency).
ot shown: 999 closed ports
ORT   STATE SERVICE
3/tcp open  domain

map done: 256 IP addresses (1 host up) scanned in 5.71 seconds
ksharma063@DESKTOP-J7E371H:~$
```



```
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-FA-EE-E1
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::df27:231b:2eaa:6115%52(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.25.96.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 872420701
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-96-A6-A1-A8-1E-84-D3-DB-05
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\nksha>
```



Target: 172.25.96.1

Command: nmap -p 1-65535 -T4 -A -v 172.25.96.1

172.25.96.1
172.25.104.102

nmap -p 1-65535 -T4 -A -v 172.25.96.1

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-06 17:47 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:47
Completed NSE at 17:47, 0.00s elapsed
Initiating NSE at 17:47
Completed NSE at 17:47, 0.00s elapsed
Initiating NSE at 17:47
Completed NSE at 17:47, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:47
Completed Parallel DNS resolution of 1 host. at 17:47, 0.05s elapsed
Initiating SYN Stealth Scan at 17:47
Scanning 172.25.96.1 [65535 ports]
Discovered open port 135/tcp on 172.25.96.1
Discovered open port 445/tcp on 172.25.96.1
Discovered open port 139/tcp on 172.25.96.1
Discovered open port 49665/tcp on 172.25.96.1
Discovered open port 49666/tcp on 172.25.96.1
Discovered open port 5040/tcp on 172.25.96.1
Discovered open port 49668/tcp on 172.25.96.1
Discovered open port 49664/tcp on 172.25.96.1
Discovered open port 49669/tcp on 172.25.96.1
Discovered open port 49667/tcp on 172.25.96.1
Completed SYN Stealth Scan at 17:48, 6.52s elapsed (65535 total ports)
Initiating Service scan at 17:48
```