Cyber Security Domain

INTERNSHIP PROJECT – 1

Iam Rakesh Puttala,

I giving this presentation regarding for my first Internship project

NETWORK AND PORT SCANNER:

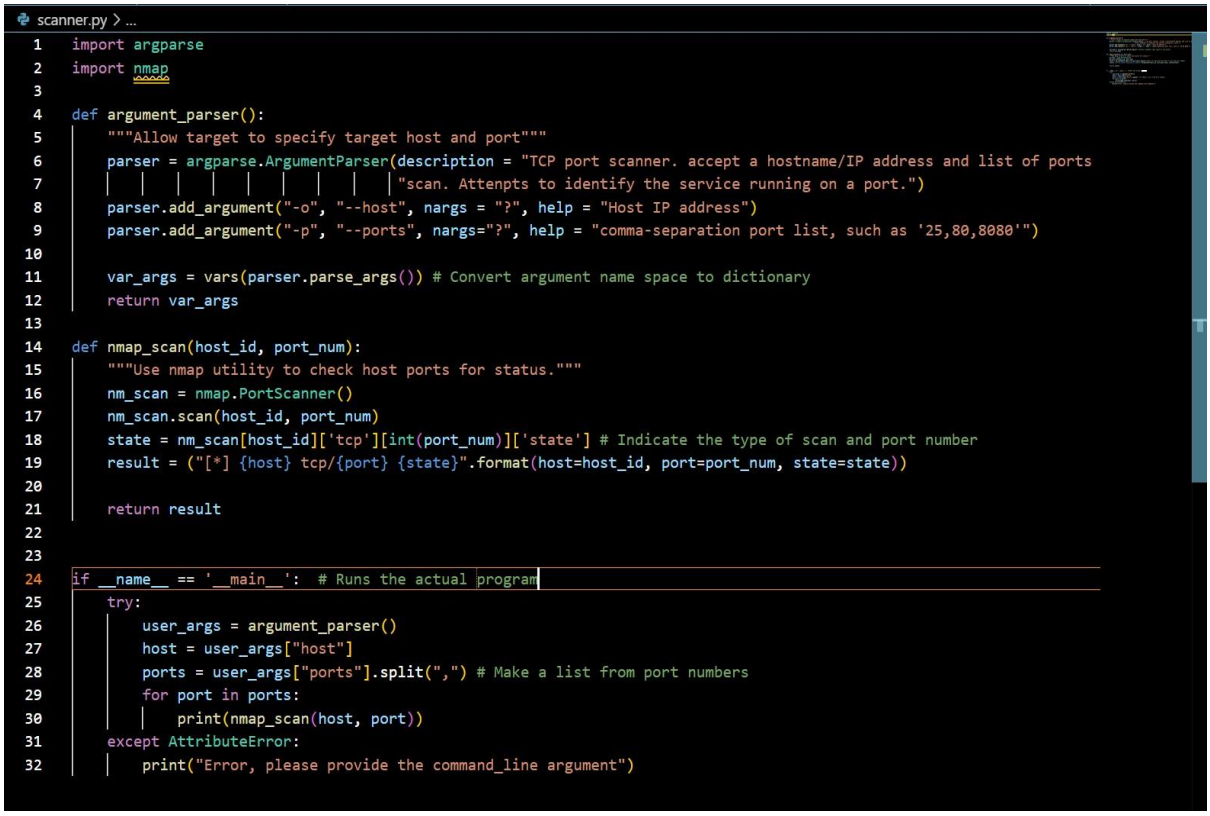
to build a scanner by using the **python** to detect the live and non-live hosts.and

To scan the ports weather that are closed or open for a particular host through **IP Address.**

To build the scanner in the vs code or pycharm we need to install the nmap package That we can install by using the command **pip install python-nmap.**

```
C:\Users\rakes\python>pip install python-nmap
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: python-nmap in c:\users\rakes\appdata\roaming\python\python312\site-packages (0.7.1)
```

After installing of the nmap package the we can proceed to code the scanner I have created the file name as **scanner.py** .



```python
import argparse
import nmap

def argument_parser():
    """Allow target to specify target host and port"""
    parser = argparse.ArgumentParser(description = "TCP port scanner. accept a hostname/IP address and list of ports
                                     "scan. Attenpts to identify the service running on a port.")
    parser.add_argument("-o", "--host", nargs = "?", help = "Host IP address")
    parser.add_argument("-p", "--ports", nargs="?", help = "comma-separation port list, such as '25,80,8080'")

    var_args = vars(parser.parse_args()) # Convert argument name space to dictionary
    return var_args

def nmap_scan(host_id, port_num):
    """Use nmap utility to check host ports for status."""
    nm_scan = nmap.PortScanner()
    nm_scan.scan(host_id, port_num)
    state = nm_scan[host_id]['tcp'][int(port_num)]['state'] # Indicate the type of scan and port number
    result = ("[*] {host} tcp/{port} {state}".format(host=host_id, port=port_num, state=state))

    return result


if __name__ == '__main__':  # Runs the actual program
    try:
        user_args = argument_parser()
        host = user_args["host"]
        ports = user_args["ports"].split(",") # Make a list from port numbers
        for port in ports:
            print(nmap_scan(host, port))
    except AttributeError:
        print("Error, please provide the command_line argument")
```

Or this tool can be access with the file link given below:

https://drive.google.com/file/d/1984xzK4R8_C2qs1RXXhoFu8nAIrfCpZe/view?usp=sharing

And code to access for you I have give that below to execute by copy this code

---

import argparse import

nmap

def argument_parser():

"""Allow target to specify target host and port""" parser = argparse.ArgumentParser(description = "TCP port scanner. accept a hostname/IP address and list of ports to"

"scan. Attenpts to identify the service running on a port.")

parser.add_argument("-o", "--host", nargs = "?", help = "Host IP address")

```
parser.add_argument("-p", "--ports", nargs="?", help = "comma-separation port list, such as '25,80,8080'")   var_args = vars(parser.parse_args()) # Convert argument name space to dictionary  return var_args

def nmap_scan(host_id, port_num):
    """Use nmap utility to check host ports for status."""     nm_scan = nmap.PortScanner()
nm_scan.scan(host_id, port_num)     state = nm_scan[host_id]['tcp'][int(port_num)]['state'] # Indicate the type of scan and port number     result = ("[*] {host} tcp/{port} {state}".format(host=host_id, port=port_num, state=state))
        return result
if name == 'main':  # Runs the actual program     try:
        user_args = argument_parser()        host = user_args["host"]
ports = user_args["ports"].split(",") # Make a list from port numbers
for port in ports:
            print(nmap_scan(host, port))
except AttributeError:
        print("Error, please provide the commad_line argument")
```

---

this will detect the live and non_live hosts and port status of the particular host by giving input as ip address.

I have tested my code on

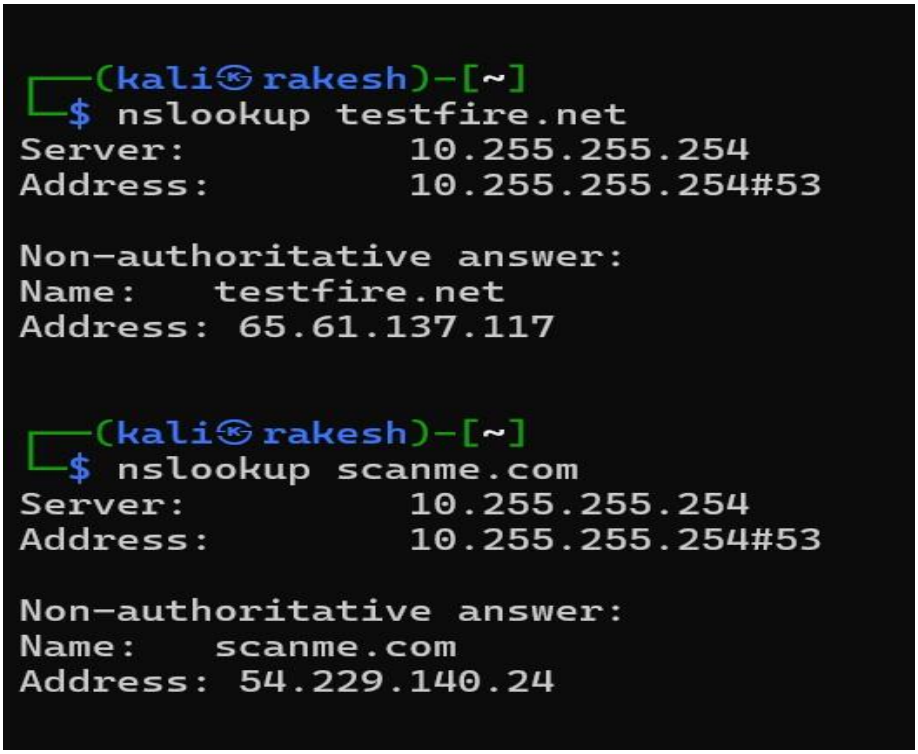
1.testfire.net 2.scanme.com

To get those hosts ip address I have used nslookup in the kali linux Commands

which I have used to get,

nslookup testfire.net nslookup

scanme.com

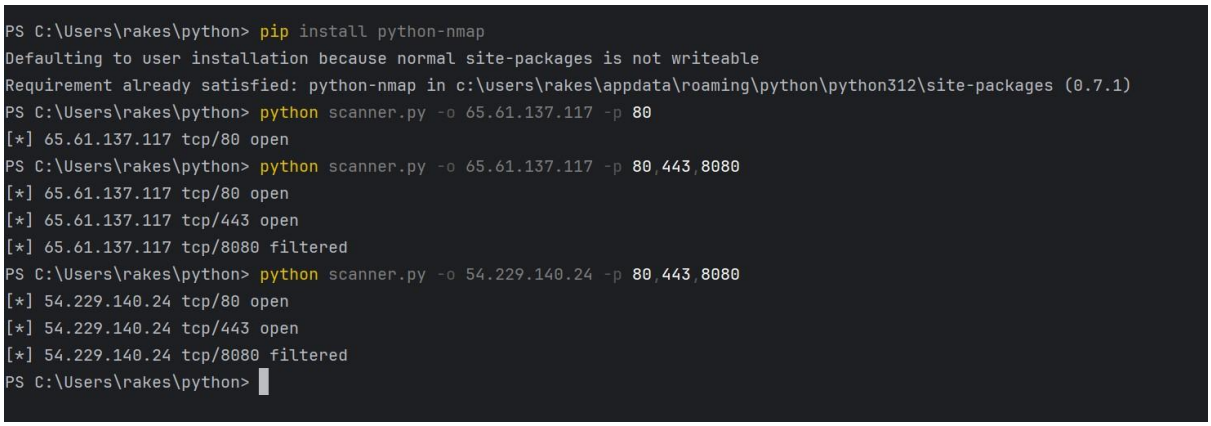


The I have used their ip address to test the tool scanner.py Command to

get output of the tool is

python scanner.py -o <ip_address> -p <port_numbers separating with comma>

Then I have get that which port is open ,or which port is closed,or which port is filtered me amoung the list of ports which I have been searching for.



This scanner was clearly shown that a specific port of the particular host is open or closed or filtered.

Here for the testfire.net server

The port num 80,443 are open state and port num 8080 was filtered me from the server.

By this scanner we scan any port of the host weather it is live or non-live host.

Thank U