19CSC10 Ethical Hacking and Network Defence

Assignment I

Application to perform Port Scanning

CODE:

"""portScanning.py: A console application to perform port scanning"""

\_\_author\_\_ = "Ramkumar"

\_\_email\_\_ = "kram.cse.2001@gmail.com"

import ipaddress

import socket

import sys

def portScanning(ip):

    try:

        ports=[80,443,3306,5000,8090]

        for i in ports:

            sock = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

            socket.setdefaulttimeout(1)

            response = sock.connect\_ex((ip, i))

            if response == 10060:

                print("Connection Time-out")

                print("Couldn't connect to "+ ip)

                return

            if response == 0:

                print("Port ", i ," is open")

            else:

                print("Port ", i ," is closed")

            sock.close()

    except KeyboardInterrupt:

        print("\n Quiting Scanning !!!!")

        sys.exit()

    except socket.gaierror:

        print("\n Hostname Could Not Be Resolved !!!!")

        sys.exit()

    except socket.error:

        print("\ Server not responding !!!!")

        sys.exit()

print("MENU")

print("1. Scan one IP address")

print("2. Scan Multiple IP addresses")

print("3. Scan a Subnet")

print("4. Enter Host name")

choice= int(input("Enter your choice: "))

if choice==1:

    ip= input("Enter the ip addr to scan: ")

    portScanning(ip)

elif choice==2:

    ips=input("Enter the IP addresses: ")

    ipsList= ips.split(",")

    print(ipsList)

    for i in ipsList:

        print("Scanning "+ i)

        portScanning(i)

elif choice==3:

    subnetId= input("Enter the subnet id: ")

    net4 = ipaddress.ip\_network(subnetId)

    j=1

    for ip in net4.hosts():

        print("Scanning "+ str(ip))

        portScanning(str(ip))

        j=j+1

        if j==3:

            break

elif choice==4:

    hostName= input("Enter the host name ")

    ip = socket.gethostbyname(hostName)

    print(ip)

    portScanning(ip)

output:

**Case 1:**

**Scan a single IP**

C:\Users\karth\Desktop\COLLEGE\Sem 7\EthicalHacking\Assignments\Ass1>python portScanning.py

MENU

1. Scan one IP address

2. Scan Multiple IP addresses

3. Scan a Subnet

4. Enter Host name

Enter your choice: 1

Enter the ip addr to scan: 172.16.5.167

Port 80 is open

Port 443 is open

Port 3306 is closed

Port 5000 is closed

Port 8090 is closed

**Case 2:**

**Scan multiple IP addresses**

C:\Users\karth\Desktop\COLLEGE\Sem 7\EthicalHacking\Assignments\Ass1>python portScanning.py

MENU

1. Scan one IP address

2. Scan Multiple IP addresses

3. Scan a Subnet

4. Enter Host name

Enter your choice: 2

Enter the IP addresses: 172.16.5.167,172.16.4.235

['172.16.5.167', '172.16.4.235']

Scanning 172.16.5.167

Port 80 is open

Port 443 is open

Port 3306 is closed

Port 5000 is closed

Port 8090 is closed

Scanning 172.16.4.235

Port 80 is closed

Port 443 is closed

Port 3306 is closed

Port 5000 is closed

Port 8090 is closed

**Case 3:**

**Scan a network using subnet ID**

C:\Users\karth\Desktop\COLLEGE\Sem 7\EthicalHacking\Assignments\Ass1>python portScanning.py

MENU

1. Scan one IP address

2. Scan Multiple IP addresses

3. Scan a Subnet

4. Enter Host name

Enter your choice: 3

Enter the subnet id: 172.16.0.0/19

Scanning 172.16.0.1

Port 80 is closed

Port 443 is closed

Port 3306 is closed

Port 5000 is closed

Port 8090 is closed

Scanning 172.16.0.2

Port 80 is closed

Port 443 is closed

Port 3306 is closed

Port 5000 is closed

Port 8090 is closed

**Case 4:**

**Scan an IP using the hostname**

C:\Users\karth\Desktop\COLLEGE\Sem 7\ EthicalHacking \Assignments\Ass1>python portScanning.py

MENU

1. Scan one IP address

2. Scan Multiple IP addresses

3. Scan a Subnet

4. Enter Host name

Enter your choice: 4

Enter the host name mepcoeng.ac.in

210.212.254.68

Port 80 is open

Port 443 is open

Port 3306 is open

Port 5000 is closed

Port 8090 is closed