Computer Networks

Assignment - 2

TCP Port Scanner using Python

Team Members:

VIDULA.L.S : PES2UG21CS602

YAMAN GUPTA : PES2UG21CS619

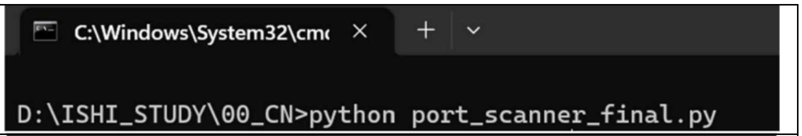
CODE

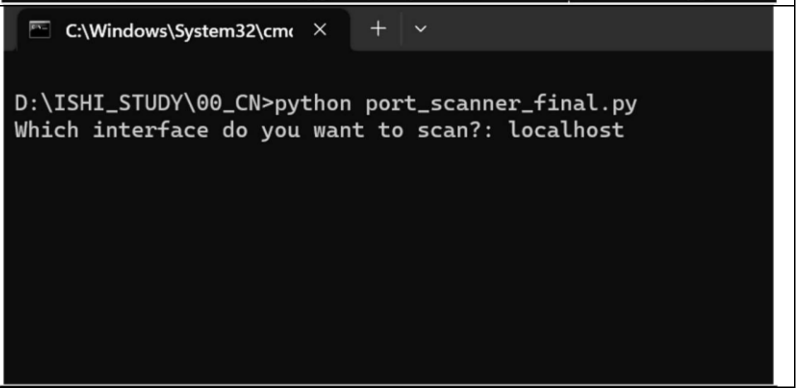
Server code:port_scanner.py

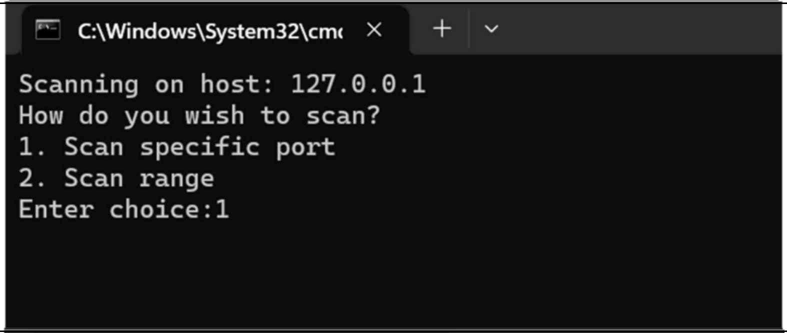
```
import socket
import time
import os


s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)


target = input('Which interface do you want to scan?: ')

target_ip = socket.gethostbyname(target)
print('Starting scan on host:', target_ip)




def port_scan(port):
    try:
        s.connect((target_ip, port))
        return True
    except:
        return False




# time.sleep(1)
os.system('cls')
print('Scanning on host:', target_ip)
print("How do you wish to scan?")
print("1. Scan specific port")
print("2. Scan range")
ch=int(input("Enter choice:"))

time.sleep(1)
os.system('cls')


if ch==1:
    start = time.time()
    port = int(input("Enter the port number to be scanned: "))
    if port_scan(port):
        print('Port', port, 'is open')
    else:
        print("Port", port, "is closed")
elif ch==2:
    start = time.time()
    s_port = int(input("Enter the starting port to be scanned: "))
    l_port = int(input("Enter the last port to be scanned: "))
    for port in range(s_port, l_port+1):
        if  port_scan(port):
            print(f'Port {port} is open')
        else:
            print(f'Port {port} is closed')



end = time.time()
print(f'Time taken {end-start:.2f} seconds')
```

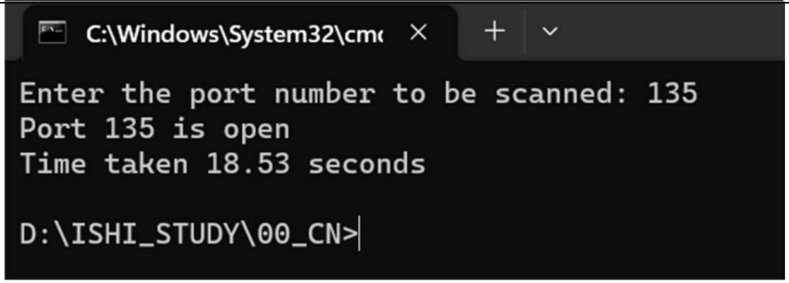
SCREENSHOTS

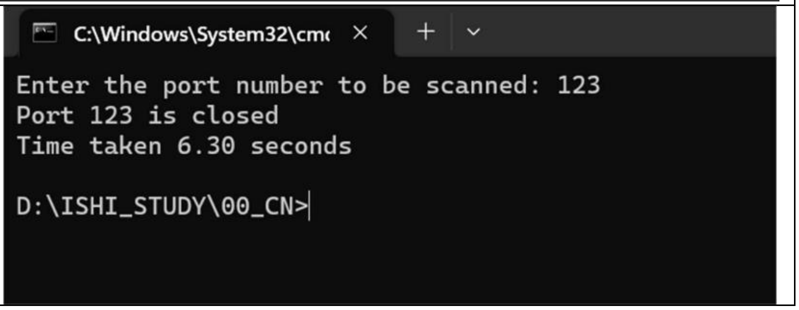
1. Scanning TCP ports on “localhost” for specific ports

Initializing the connection	 `D:\ISHI_STUDY\00_CN>python port_scanner_final.py`

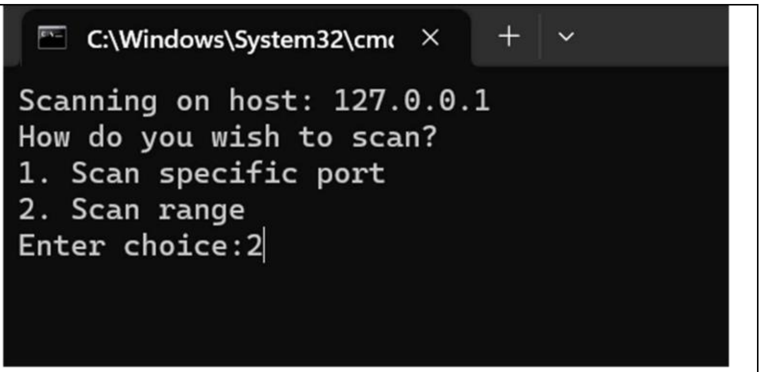
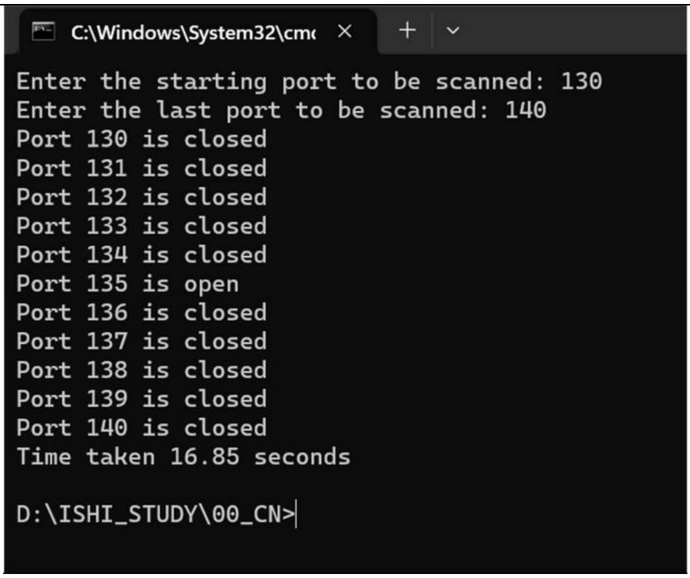
Scanning the “localhost” on the system	
	
	`D:\ISHI_STUDY\00_CN>python port_scanner_final.py`
	`Which interface do you want to scan?: localhost`

Entering specific choice for scanning, here we are scanning a specific port	
	
	`Scanning on host: 127.0.0.1`
	`How do you wish to scan?`
	`1. Scan specific port`
	`2. Scan range`
	`Enter choice:1`

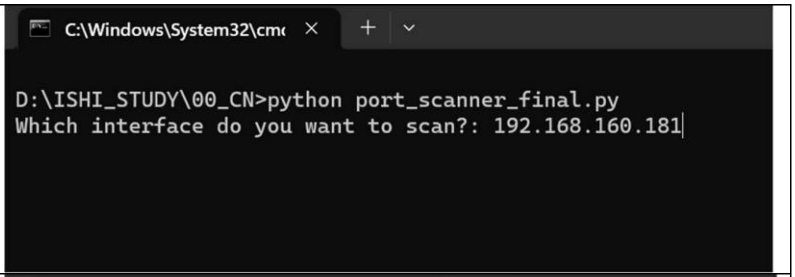
The port number 135 is open and can be used.	
	
	`Enter the port number to be scanned: 135`
	`Port 135 is open`
	`Time taken 18.53 seconds`
	
	`D:\ISHI_STUDY\00_CN>`

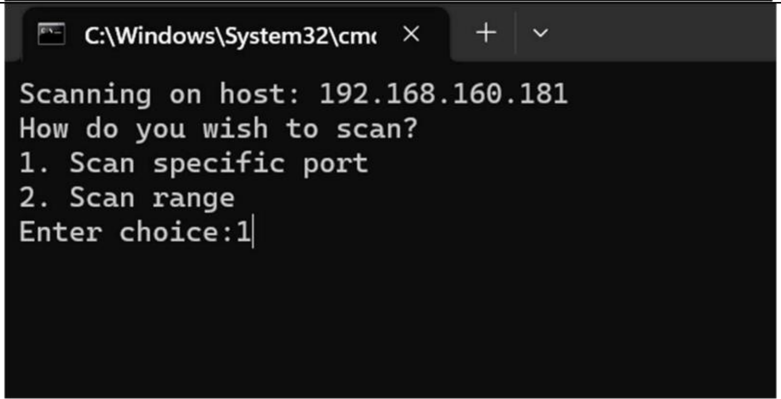
The port number 123 is closed and cannot be used.	
	
	`Enter the port number to be scanned: 123`
	`Port 123 is closed`
	`Time taken 6.30 seconds`
	
	`D:\ISHI_STUDY\00_CN>`

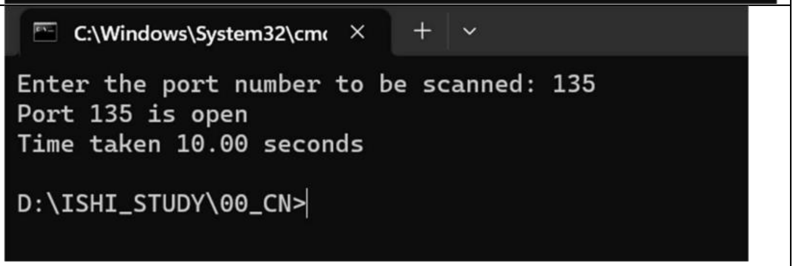
2. Scanning TCP ports on “localhost” for range of ports

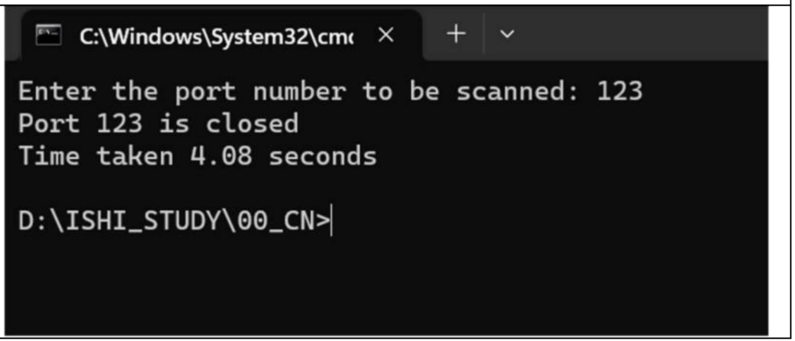
Entering specific choice for scanning, here we are scanning a range of ports	 Scanning on host: 127.0.0.1 How do you wish to scan? 1. Scan specific port 2. Scan range Enter choice:2
The port range from 130 to 140 is scanned. The port 135 is open while the rest are closed.	 Enter the starting port to be scanned: 130 Enter the last port to be scanned: 140 Port 130 is closed Port 131 is closed Port 132 is closed Port 133 is closed Port 134 is closed Port 135 is open Port 136 is closed Port 137 is closed Port 138 is closed Port 139 is closed Port 140 is closed Time taken 16.85 seconds D:\ISHI_STUDY\00_CN>

3. Scanning TCP ports on given IP address on system for specific port

Scanning the given IP on the system	
	`D:\ISHI_STUDY\00_CN>python port_scanner_final.py`
	`Which interface do you want to scan?: 192.168.160.181`

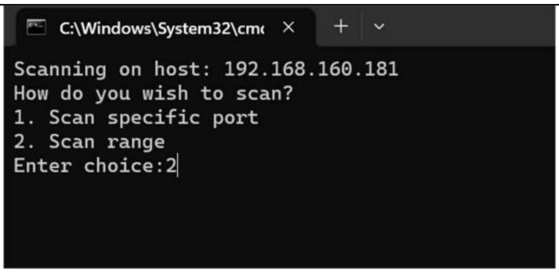
Entering specific choice for scanning, here we are scanning a specific port	
	`Scanning on host: 192.168.160.181`
	`How do you wish to scan?`
	`1. Scan specific port`
	`2. Scan range`
	`Enter choice:1`

The port number 135 is open and can be used.	
	`Enter the port number to be scanned: 135`
	`Port 135 is open`
	`Time taken 10.00 seconds`
	
	`D:\ISHI_STUDY\00_CN>`

The port number 123 is closed and cannot be used.	
	`Enter the port number to be scanned: 123`
	`Port 123 is closed`
	`Time taken 4.08 seconds`
	
	`D:\ISHI_STUDY\00_CN>`

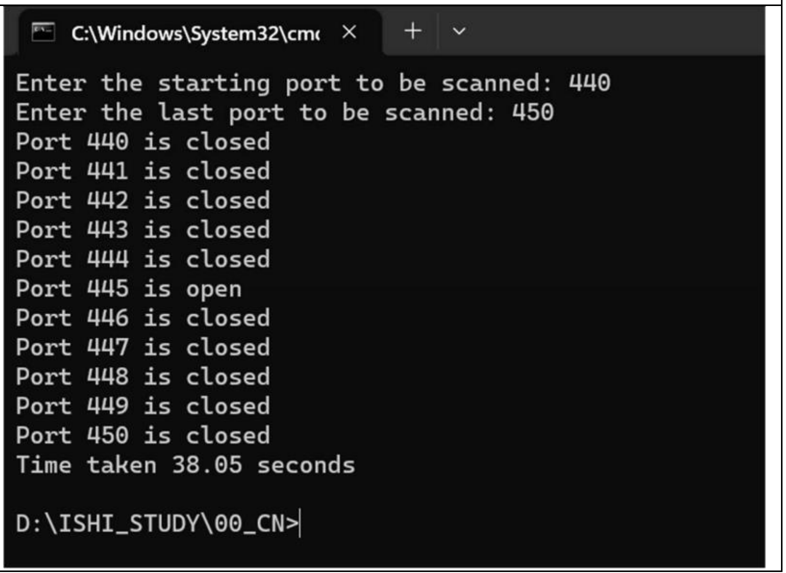
4. Scanning TCP ports on “localhost” for range of ports

<table>
<tr>
<td>Entering specific choice for scanning, here we are scanning a range of ports</td>
<td>



```
Scanning on host: 192.168.160.181
How do you wish to scan?
1. Scan specific port
2. Scan range
Enter choice:2
```

</td>
</tr>
<tr>
<td>The port range from 440 to 450 is scanned.
The port 445 is open while the rest are closed.</td>
<td>



```
Enter the starting port to be scanned: 440
Enter the last port to be scanned: 450
Port 440 is closed
Port 441 is closed
Port 442 is closed
Port 443 is closed
Port 444 is closed
Port 445 is open
Port 446 is closed
Port 447 is closed
Port 448 is closed
Port 449 is closed
Port 450 is closed
Time taken 38.05 seconds

D:\ISHI_STUDY\00_CN>
```

</td>
</tr>
</table>