Project: Python Port Scanner

Contents

Project: Python Port Scanner

1. Introduction

This project demonstrates the development of a basic TCP port scanner using Python. The objective of this task is to understand how network reconnaissance works, how services listen on ports, and how attackers and defenders identify exposed network services. The project was implemented strictly in a controlled and authorized environment for educational and cybersecurity learning purposes.

2. Objective of the Project

The main goals of this task are:

- To understand how TCP connections are established
- To identify open and closed ports on a target system
- To perform basic banner grabbing for service identification
- To learn how port scanning is used in cybersecurity reconnaissance

3. Tools and Technologies Used

- **Programming Language:** Python 3
- **Libraries:** socket, termcolor
- **Environment:** Local machine / authorized network

4. How the Port Scanner Works (High-Level)

The port scanner attempts to establish a TCP connection with a target IP address on a range of ports. If a connection is successful, the port is considered open. If the connection fails or times out, the port is treated as closed or filtered. When possible, the scanner attempts to read a service banner to identify the running service.

5. Code Implementation

network.py

```python
# Basic port scanner (Educational)
# Purpose: Network Reconnaissance
# Scope: Authorized & Local network

import socket
from termcolor import colored


# First Function

def scan(ipaddress, max_ports):
    print(colored("[*] Starting scan for this {ipaddress}","cyan"))

    for port in range(1, max_ports):
        scan_port(ipaddress, port)

# Get service banner

def get_banner(sock):
    return sock.recv(1024)
```

```python
# Scan single port

def scan_port(ip, port):
    try:
        sock = socket.socket()
        sock.settimeout(0.3)

        # Try connecting to port
        sock.connect((ip, port))

        try:
            banner = get_banner(sock)
            print(colored(f"[+] Port {port} Open : {banner.decode().strip()}","green"))
        except:
            print(colored(f"[+] Port {port} Open","green"))

        sock.close()

    except:
        # Closed and filtered port
        pass
```

```python
# ──────────────────────────
#        Main Program
# ──────────────────────────

if __name__ == "__main__":
    targets = input("[+] Enter target(s) (comma separated if multiple): ")
    ports = int(input("[+] Enter number of ports to scan: "))

    # Multiple targets
    if "," in targets:
        print(colored("\n[+] Multiple targets detected\n","yellow"))
        for target in targets.split(","):
            scan(target,ports)

    else:
        scan(targets,ports)
```

6. Sample Output

```
┌──(kali㉿kali)-[~/Desktop/projects]
└─$ python3 port_scanner.py
[+] Enter target(s) (comma separated if multiple): 10.0.2.4
[+] Enter number of ports to scan: 100
[*] Starting scan for this 10.0.2.4
[+] Port 21 Open : 220 (vsFTPd 2.3.4)
[+] Port 22 Open : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
[+] Port 23 Open
[+] Port 25 Open : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] Port 53 Open
[+] Port 80 Open
```

7. Key Networking Concepts Learned

- TCP/IP communication
- Three-way handshake (SYN, SYN-ACK, ACK)
- Difference between open, closed, and filtered ports
- Role of firewalls in blocking or filtering ports

Attacker Perspective:

- Identify entry points
- Discover vulnerable services

Defender Perspective:

- Detect unauthorized scans
- Reduce attack surface
- Harden network configurations

8. Security and Ethical Considerations

- The scanner was tested only on systems with permission
- Unauthorized scanning of networks is illegal and unethical
- The project focuses on learning defensive and analytical skills

9. Conclusion

This project provided hands-on experience with network reconnaissance and TCP communication. Building a port scanner helped in understanding how attackers discover services and how defenders can detect and mitigate such activities. The project strengthened foundational networking and cybersecurity concepts and is suitable for inclusion in a cybersecurity portfolio.