PROJECT-2
NETWORK AND PORT SCANNER

SUBMITTED TO

1STOP

SUBMITTED BY

CH.MAMATHA

ABSTRACT

A network and port scanner is a cybersecurity tool used to identify open ports and services on networked systems. It allows security professionals to assess the security posture of a network, identify potential vulnerabilities, and understand attack surfaces. By sending network requests to target systems, the scanner determines the status of specific ports and can often identify the services running on those ports. Network and port scanners help in network discovery, vulnerability assessment, and the development of robust security strategies. They provide detailed reports that aid in prioritizing remediation efforts and making informed decisions. However, it's important to use them responsibly, with proper authorization and adherence to legal and ethical guidelines.

Network and Port Scanner

Introduction:

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. This scanning can't take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

It's important to note that network and port scanning can be used by both IT administrators and cybercriminals to verify or check the security policies of a network and identify vulnerabilities — and in the attackers' case, to exploit any potential weak entry points. In fact, the host discovery element in network scanning is often the first step used by attackers before they execute an attack. As both scans continue to be used as key tools for attackers, the results of network and port scanning can provide important indications of network security levels for IT administrators trying to keep networks safe from attacks.

A network and port scanner is a powerful tool used in cyber security to assess the security posture of computer networks. It works by actively scanning a range of IP addresses and network ports to identify open ports, active hosts and potential vulnerabilities. Network and port scanners are instrumental in penetration testing, vulnerability assessment and network mapping, enabling security professionals to identify points that could be exploited by attackers. They play critical role in proactive network defense and maintaining a secure environment.

A network and port scanner is a tool used in cybersecurity to scan and identify open ports and services on networked systems. It helps in assessing the security posture of a network by discovering potential entry points and vulnerabilities. Here are some key aspects of network and port scanners:

Port Scanning: Port scanning is the primary function of a network and port scanner. It involves scanning a range of network ports on a target system to determine which ports are open, closed, or filtered. The scanner sends network requests to each port and analyzes the response to determine its status.

Network Discovery: Network scanners often include network discovery capabilities. They scan IP ranges or subnets to identify active hosts on the network. This helps in creating an inventory of devices and understanding the network topology.

Service Identification: In addition to port status, network and port scanners can also identify the services running on open ports. By analyzing the banner or response received from a service, the scanner can determine the software or application running on that port. This information is valuable for vulnerability assessment and understanding potential attack vectors.

Scan Techniques: Network and port scanners employ various scan techniques, including TCP scans, UDP scans, SYN scans, and more. Each technique has its advantages and limitations, and they can be used based on the specific requirements and network conditions.

Scripting and Automation: Advanced network and port scanners often provide scripting and automation capabilities. This allows security professionals to customize the scanning process, automate repetitive tasks, and perform complex scans with specific parameters.

Vulnerability Assessment Integration: Some network and port scanners integrate with vulnerability assessment tools or databases. This enables the scanner to cross-reference open ports and services with known vulnerabilities and provide additional insights into the potential risks.

Reporting and Analysis: Network and port scanners generate detailed reports that provide information about open ports, services, and potential vulnerabilities. These reports help security professionals understand the network's security posture, prioritize remediation efforts, and make informed decisions.

Examples of popular network and port scanning tools include Nmap, Nessus, OpenVAS, Zenmap, and Masscan. These tools vary in their capabilities, user interfaces, and complexity, allowing security professionals to choose the one that best suits their requirements.

When using network and port scanners, it's important to adhere to legal and ethical guidelines. Proper authorization and consent must be obtained, and scans should be performed responsibly to avoid disruption or harm to the targeted systems or networks.

Network scanner to detect the live hosts in the network.

Port scanner is to know status of the ports.

They are different scanning tools for doing scanning but most efficient tool is nmap tool.

Code :

```
import socket
import re
port_range_pattern = re.compile(r"([0-9]+)-([0-9]+)")
port_min = 0
port_max = 65535
print("Movidu Technologies Python Scanner\n")
print("*Python Project 1*\n")
open_ports = []
while True:
    ip_address_entered = input("Enter the IP address: ")
    try:
        ip_address = socket.gethostbyname(ip_address_entered)
        print(f"You entered a correct IP address: {ip_address}")
        break
    except socket.gaierror:
        print("You entered an invalid IP address. Please try again.")
while True:
    print("\nEnter the range of ports you want to scan in the network")
    port_range = input("Enter the port range (e.g., 1-100): ")
    port_range_valid = port_range_pattern.search(port_range.replace(" ", ""))
    if port_range_valid:
        port_min = int(port_range_valid.group(1))
        port_max = int(port_range_valid.group(2))
        break
    else:
        print("Invalid port range format. Please try again.")
for port in range(port_min, port_max + 1):
```

```
    try:
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
            s.settimeout(0.5)
            result = s.connect_ex((ip_address, port))
            if result == 0:
                service_name = socket.getservbyport(port)
                open_ports.append((port, service_name))
    except socket.error:
        pass
if open_ports:
    print("\nOpen ports:")
    for port, service_name in open_ports:
        print(f"Port {port} is open. Service: {service_name}")
else:
    print("\nNo open ports found in the specified range.")
```

output:

```
https://aka.ms/powershell
Type 'help' to get help.

┌──(kali㉿kali)-[/home/kali]
└─PS> cd Desktop

┌──(kali㉿kali)-[/home/kali/Desktop]
└─PS> nslookup www.instagram.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.instagram.com       canonical name = geo-p42.instagram.com.
geo-p42.instagram.com   canonical name = z-p42-instagram.c10r.instagram.com.
Name:   z-p42-instagram.c10r.instagram.com
Address: 157.240.228.174
Name:   z-p42-instagram.c10r.instagram.com
Address: 2a03:2880:f268:e6:face:b00c:0:4420


┌──(kali㉿kali)-[/home/kali/Desktop]
└─PS> python scan1.py
Movidu Technologies Python Scanner

*Python Project 1*

Enter the IP address: 157.240.228.174
You entered a correct IP address: 157.240.228.174

Enter the range of ports you want to scan in the network
Enter the port range (e.g., 1-100): 1-500

Open ports:
Port 80 is open. Service: http
Port 443 is open. Service: https
```

- The provided code is a basic network port scanner implemented in Python.
- It prompts the user to enter an IP address and a range of ports to scan within the network.
- The code validates the input, retrieves the corresponding IP address, and performs a scan by attempting to establish a TCP connection to each port in the specified range.
- If a port is open, the code identifies the associated service and stores the open port information in a list.
- Finally, it displays the open ports and their corresponding services, if any, or notifies the user if no open ports are found in the specified range.

CONCLUSION

In conclusion, network and port scanning plays a crucial role in cybersecurity. It enables organizations to proactively identify potential vulnerabilities and assess their network's security posture. By scanning for open ports and services, security professionals can gain insights into potential entry points for attackers. Network and port scanning tools provide valuable information for vulnerability assessment, network mapping, and understanding attack surfaces. The results obtained from scanning activities help prioritize remediation efforts, implement appropriate security measures, and develop effective defense strategies. However, it's essential to conduct scanning activities responsibly, with proper authorization and adherence to legal and ethical guidelines to avoid any potential harm or disruption to targeted systems or networks.