PORT SCANNER DETECTION

Suuraj kumar s
pratheep k

Abstract

A port scanner is a tool or software program that is used to identify open ports on a computer or network device. It works by sending a series of packets to a target host and then analyzing the response to determine which ports are open or closed. This information can be used for a variety of purposes, such as network security assessments, identifying potential vulnerabilities, or troubleshooting connectivity issues. There are many different types of port scanners available, including both command-line and GUI-based tools, and they can be used in both internal and external network environments.

Exiting System

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 Analyzing responses to identify vulnerabilities. The 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. The 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

Literature Survey

Port scanning is designed to probe a network host for open ports and other services available. It is useful for system administrators and other network defenders to detect port scans as a useful technique for recognizing precursors to serious attacks. From the attacker's viewpoint, a port scan is useful for gathering relevant information for launching a successful attack. Thus it is of considerable interest to attackers to determine whether or not the defenders of a network are scanning ports regularly. Defenders do not usually hide the iridentity during port scanning while attackers do

Proposed System

The sys library to access command line arguments, the socket library to interact with the target's network socket, and the datetime library to record the initiation time of the scan. The script accepts a single command line argument, which is the hostname or IP address of the target, and utilizes the name function from the socket library to convert it to an IP address. Subsequently. The script conducts a scan on any ports to the specified target by creating a socket and utilizing the method to determine if the port is open. The script also includes try-except blocks to handle potential errors such as invalid arguments, hostname resolution failure, server not responding, and also keyboard interrupt

Tools Used

- **Hardware Requirements**: This library is used to access command line arguments, it is included in Python's standard library

- **Software Requirements**: This library is used to record the start time of the scan, it is included in Python's standard library and does not need to be installed.
- **A target host**: The script takes one command line argument, which is the hostname or IP address of the target, so a valid target host is required to run the script
- **Socket library**: This library is used to interact with the target's network socket, it can be installed by running "pip install sockets" command in the terminal

- **Other requirements**: Python interpreter is required to run the script

Modules

This project presents a method for conducting a port scan. The script utilizes various libraries such as pyfiglet, sys, socket, and datetime to achieve. Functionality, making it a reliable and proficient tool for the purpose of port scanning. This project serves as an ideal starting point for individuals who have an interest in the field of network security

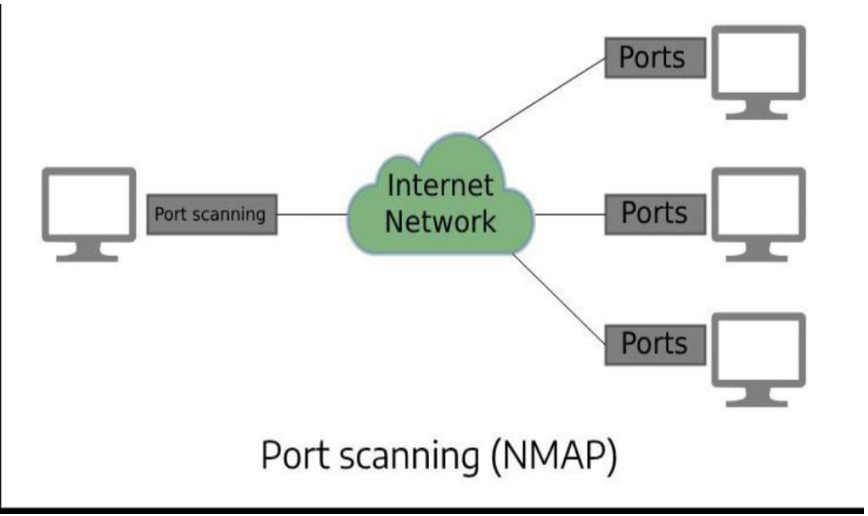
Status of the Project

This project introduced a flexbile, scalable architecture and a new algorithm to detect and block network port scans scalability is achieved by storing information of a subnet rather than keeping states of individual flows and the project has not finished, and work on the project will continue in future also and I do Masters studies that time the project will be more development in port scanner Project.

Project Guide Meeting Details

S.No	Date	Suggestions from Guide
1	12.12.2022	Select project tittle
2	26.12.2022	Search base papper on iEEE
3	17.1.2023	About Project ABSTRACT
4	25.1.2023	Present Project to Guide and need improvement

Sample Screen shoots



Port scanning (NMAP)

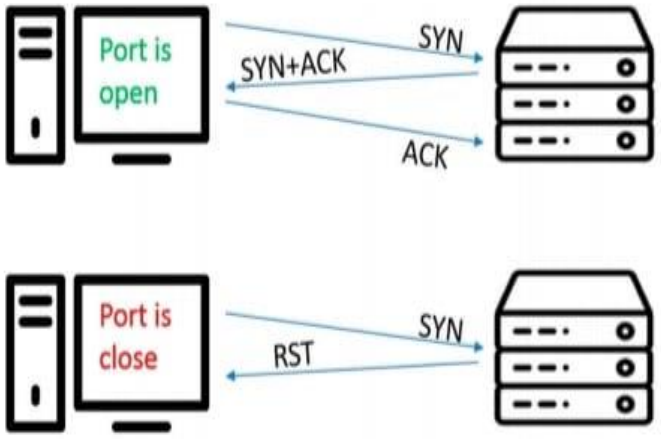


Figure 2. TCP three-way handshake port scanning.

Github screen shoot