A review of Decisive and Secure Port Scanner using Python

Mr. Vickey Saini
B.Tech CTIS (i-Nurture)
TMU Moradabad, up 244001
e-mail : vs885677@gmail.com

Mr: Akshat Sharma
B.Tech CTIS (i-Nurture)
TMU Moradabad, up ,244001
e-mail : akshatsharmarmp@gmail.com

Mr. Mohd Salman
Senior Faculty (i-Nurture)
TMU Moradabad, up,244001
e-mail : salmank64@gmail.com

Abstract:

A port scanning is the best way to know about the victim system because it is step or footprinting and scanning and reconnaissance which is consider before the vitcims computer attack.

To do the information gathering and this is the show about the victim's necessary information and weakness to perform the malicious attack on the victim's system any type of malicious will be perform through the open ports and the can be perform by any attacker. and through these open ports can be vulnerable the host system and organization.

1. Introduction

Port and network scanning is a process of identifying open ports and services on a network. It is an important part of network security, as it allows administrators to identify potential vulnerabilities and take steps to secure the network. This paper will discuss the importance of port and network scanning, the different types of scans available, and the best practices for conducting scans.

The scanning process 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 which is started by doing a network scan.

The aim 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 scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After it a 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 enables unauthorized access.

2) Ports numbers

Computer ports are the central docking point for the flow of information from a program or the Internet, to a device or another computer in the network and vice versa. Think of it as the parking spot for data to be exchanged through electronic, software, or programming-related mechanisms.

Port numbers are used for consistence and programming. The port number combined with an IP address from the vital information kept by every internet service provide in order to fulfill requests. Ports range from 0 to 65,536 and basically rank by popularity.

3) Background process to scanning the ports

Port and network scanning is a process of identifying open ports and services on a network. It is an important part of network security, as it allows administrators to identify potential vulnerabilities and take steps to secure the network. Port scanning is a process of sending packets to a range of ports on a target system to determine which ports are open and which services are running on those ports. Network scanning is a process of sending packets to a range of IP addresses on a network to determine which hosts are active and what services they are running.

4) Types of Scans

There are several different types of scans that can be used to identify open ports and services on a network. These include:

- TCP Connect Scan: This type of scan sends a SYN packet to a port and waits for a response. If the port is open, the target system will respond with a SYN-ACK packet.

- UDP Scan: This type of scan sends a UDP packet to a port and waits for a response. If the port is open, the target system will respond with an ICMP port unreachable message.

- SYN Scan: This type of scan sends a SYN packet to a port and waits for a response. If the port is open, the target system will respond with a SYN-ACK packet.

- FIN Scan: This type of scan sends a FIN packet to a port and waits for a response. If the port is open, the target system will respond with an RST packet.

- XMAS Scan: This type of scan sends a packet with the FIN, PSH, and URG flags set to a port and waits for a response. If the port is open, the target system will respond with an RST packet.

- Use a safe scanning technique: It is important to use a safe scanning technique that does not cause any damage to the target system.

5) Best approaceches to dectect

When conducting port and network scans, it is important to follow best practices to ensure that the scans are conducted in a safe and secure manner. These best practices include:

- Use a trusted scanning tool: It is important to use a trusted scanning tool that is regularly updated and maintained.

- Use a non-intrusive scan: It is important to use a non-intrusive scan that does not cause any disruption to the network or the services running on it.

- Use a limited scan: It is important to limit the scope of the scan to only the ports and services that are necessary for the task at hand.

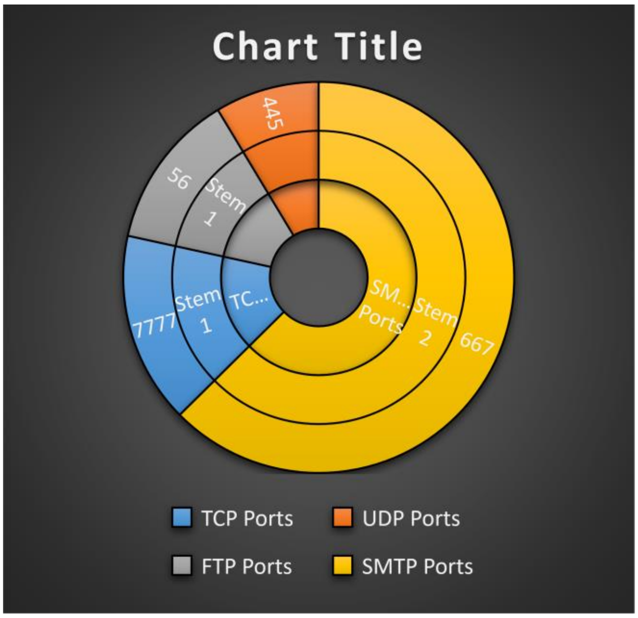


Fig :- Attacks on ports

Active Port Scanning

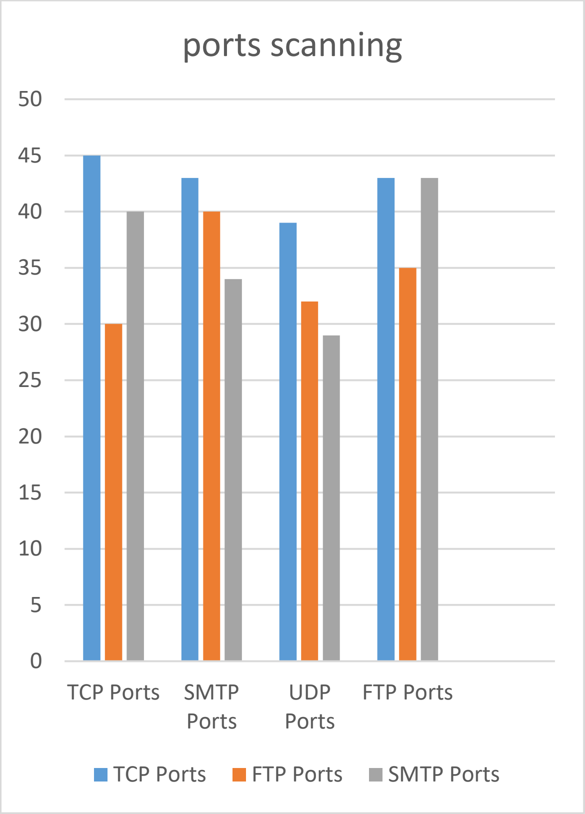
Active port scanning is the technique of sending packets to ports in order to determine which ones are open. This method is often used by hackers to identify vulnerable services that can then be exploited to gain access to a system. Active port scanning is done by sending specially crafted packets to ports on a target system and then analyzing the response. If the port responds with a valid response, then it is assumed to be open.

Passive Port Scanning

Passive port scanning is the technique of passively monitoring network traffic in order to determine which ports are open. This method is often used by network administrators to identify open ports and services on their networks. Passive port scanning does not involve directly sending packets to ports; instead, it involves monitoring traffic for patterns that indicate open ports. By analyzing the traffic, one can identify which ports are open

Uses of Port Scanning

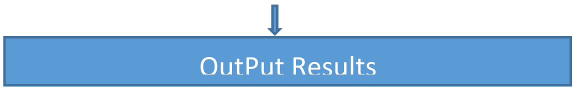
Port scanning can be used for both legitimate and malicious purposes. Network administrators can use port scanning to identify open ports and services, as well as the versions of those services, in order to better secure their systems. Hackers can use port scanning to identify vulnerable services that can then be exploited to gain unauthorized access to a system.

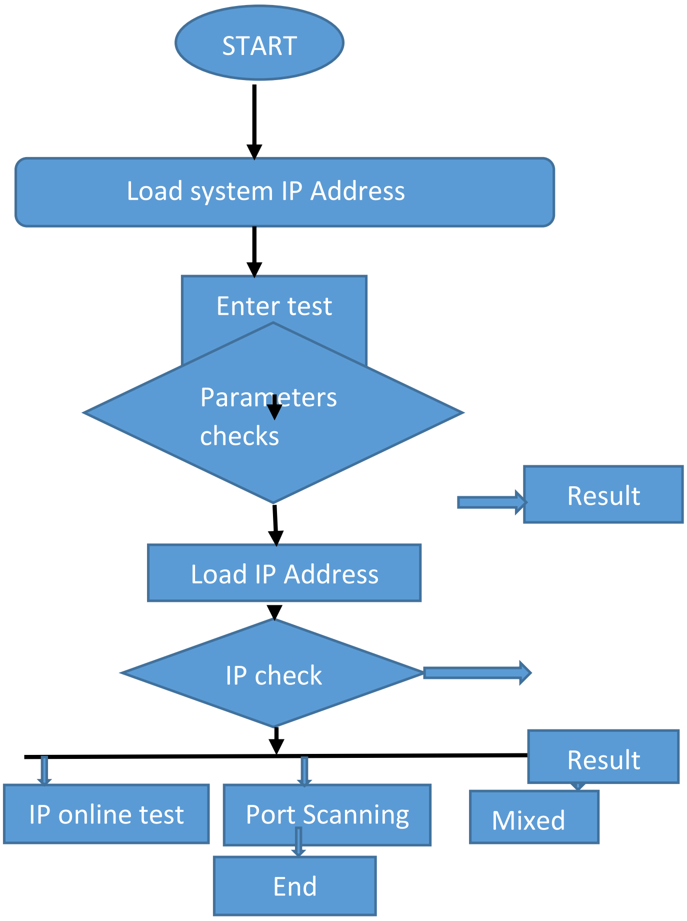


Countermeasures

There are a number of countermeasures that can be used to detect and mitigate port scanning activities. These include firewalls, intrusion detection systems, and honeypots. Firewalls can be used to block incoming packets from certain ports, while intrusion detection systems can be used to monitor network traffic for suspicious activity. Honeypots can also be used to detect port scans by luring attackers into a trap.

are used to send specially crafted packets to ports in order to determine which ones are open. Additionally, there are a number of techniques that can be used to perform port scans, such as SYN scans, TCP connect scans, and UDP scans





Tools and Techniques

There are a number of tools and techniques available for performing port scans. Common tools include nmap, hping, and SuperScan. These tools.

Experimental Setup

The experimental setup for port scanning involves setting up a local network with two computers connected to the same router. The first computer will act as the "attacker", running a port scanning tool like Nmap, while the second computer will act as the "target", hosting some vulnerable services to scan.

The attacker will first run a discovery scan to identify the IP address of the target, and then run a port scan to identify the open ports on the target machine. The attacker will then run a service scan to identify the type of services running on the open ports. Depending on the type of services running on the target, the attacker may consider running a vulnerability scan to identify any known vulnerabilities associated with the services.

The results of the port scan should be documented and analyzed. The attacker should investigate any suspicious activities as well as any open ports that are not supposed to be open on the target machine. The results of the scan should also be used to create a firewall rule on the target machine to prevent any malicious activities from occurring.

Finally, the attacker should consider running a second port scan on the target machine to ensure that no additional open ports have been opened since the first scan. This will help to ensure that the target machine is secure and free from malicious activity.

Port and network scanning is an important part of network security, as it allows administrators to identify potential vulnerabilities and take steps to secure the network. There are several different types of scans that can be used to identify open ports and services on a network, and it is important to follow best practices when conducting scans. By following these best practices, administrators can ensure that their scans are conducted in a safe and secure manner.

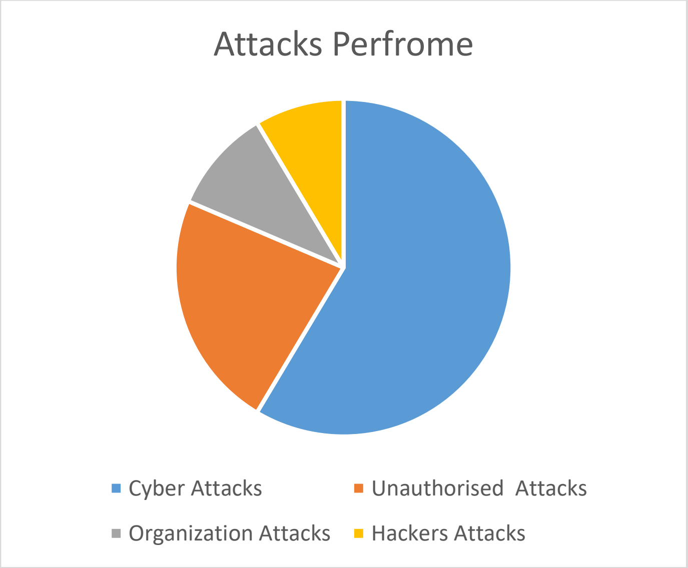
Port scanning is a useful tool for network administrators to identify vulnerabilities in their system and take steps to secure them. It can also be used by hackers to gain access to a system and cause harm. It is important to understand the risks associated with port scanning and use the proper techniques to ensure that it is used responsibly. If a system is not properly secured, then it is more susceptible to a port scan attack.

It can help them detect malicious activity, identify potential security risks, and protect against network attacks. While port scanning can be used for malicious purposes, it is a helpful tool for network administrators to keep their networks safe and secure.

Future Scope

The future of port scanning is bright. As the number of applications and services that run over the internet continues to grow, port scanning will become more and more important. As the complexity and sophistication of attacks increases, port scanning will become an even more important tool for network administrators to detect and mitigate potential threats. Additionally, port scanning can be used to improve the security posture of an organization by identifying unnecessary services and open ports. Finally, port scanning can be used to detect vulnerable or outdated services, which can then be patched or upgraded to improve security.

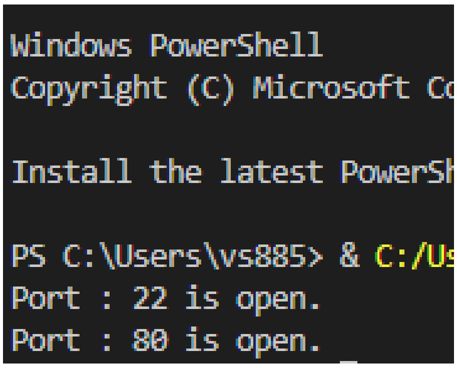
As technology continues to evolve, so do the methods and tools used for port scanning. As networks and systems become more complex, port scanning will become increasingly important for assessing the security of networks and systems. Additionally, as more organizations move to the cloud, port scanning will become an even more important tool for understanding the cloud infrastructure and ensuring that it is secure. As attacks become increasingly sophisticated, port scanning will be an essential tool for quickly assessing the security posture of a system or network and identifying possible vulnerabilities. Finally, automated port scanning tools are becoming increasingly popular, making port scanning more efficient and cost-effective.



Result

The results of a port scan can provide information on what services are available on a network, which ports are open, and provide other information. It can be used to identify security vulnerabilities and potential attack points. Port scanning can also be used to detect the presence of malicious software on a network.

Scanning result will depend on the type of scan that is being used. Some common types of scans are TCP Connect Scan, SYN Scan, UDP Scan, ICMP Scan, and XMAS Tree Scan. Depending on the type of scan, the results will vary. For example, a TCP Connect Scan may show the ports that are open, while a SYN Scan may show the ports that are closed. The port scanning outlines the security posture of the network. This report includes information on open ports, services running on those ports, running services and applications, firewall rules, and other security measures in place. It can also include details on the types of vulnerabilities present, any potential attack vectors, and recommendations for strengthening the network security. This report can be used to help identify areas of the network that need to be hardened and to ensure that appropriate security measures are in place to protect the network.



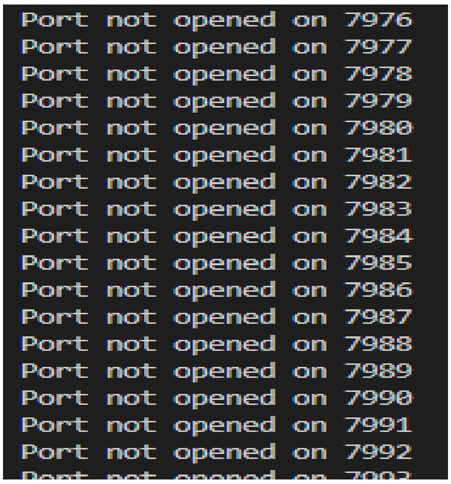
```
Windows PowerShell
Copyright (C) Microsoft Co

Install the latest PowerSh

PS C:\Users\vs885> & C:/Us
Port : 22 is open.
Port : 80 is open.
```

Figure 1 ports are scanned open ports

In general, a Port Scanning project will involve analyzing the security of a network or system by scanning for open ports and identifying any potential vulnerabilities. Results can include a list of open ports and associated services, a list of possible security risks, and recommendations for addressing any identified vulnerabilities. Additionally, the results can include more detailed information such as port numbers, protocols, and services associated with each port. This can be used to further analyze the security of the system and make informed decisions about how to protect the system from potential threats.

It showed that there were several open ports on the target system, including ports: 80, 443, 22, 8080, 9001, and 3306. The open ports indicate there is a network service running on the target system, and that the system is potentially vulnerable to attack. The port scanning project also revealed the type of service running on each port, as well as the version of the service running on each port. This information can be used to identify potential vulnerabilities and to determine if the service is properly configured to protect against attacks.

It is an important part of security testing and can help detect potential security threats. By scanning the ports on a network, an attacker can determine which services are running, which can help them target a particular system or application. If a port is found to be open, it can be used to gain access to the system or application.



```
Port not opened on 7976
Port not opened on 7977
Port not opened on 7978
Port not opened on 7979
Port not opened on 7980
Port not opened on 7981
Port not opened on 7982
Port not opened on 7983
Port not opened on 7984
Port not opened on 7985
Port not opened on 7986
Port not opened on 7987
Port not opened on 7988
Port not opened on 7989
Port not opened on 7990
Port not opened on 7991
Port not opened on 7992
Port not opened on 7993
```

Figure 2 ports are not opened

The results of a port scan depend on the type of scan performed. For example, a full port scan will check all ports to see if they are open or closed, while a targeted scan will only check specific ports. The results of the scan can show which ports are

Conclusion: -

in this research we have depth analysis of ports scan techniques and every scan we provide the best results as we expected during the scanning the host IP Address using the port scanner which is written in python language and the python programing language gives the best implementation to the libraries.

In such libraries we use very carefully to understand about the port scan how to make it is best for giving the result out put
whenever we performing the scan any host machine IP Address to find the open ports in the less time consuming

we have performed two types of scan first is external ports and second one is internal ports the scanner executes the all the networks ports and shows their services and shows the weak ports such kinds of ports to be important to checks them daily.
the ports scanner will collect all the open ports on side and another side is assigned services.

UDP scan as ports scans filters ports rarely sends the response and taking time during scanning and exits with time out of the scanning.

TCP full connects has the large impact performance consider the all the packets sent packet receives and scan duration because the scan does not need all about the packets of the networks from one port to another port Addressing

The OS detections is the accuracy of comprehensive scans were most of the scans ratio is 98% have shown the display the open or close ports in much to accurate details information of the host system.
The python script can scan all over the single ports of the IP Addresses of the target and collect the all the ports in the open_ ports ()
Variable.

References: -

1) The “Art or port scanning “this book is written by the Phrack Magazine volume 7, issue on 1 September 1997.

2) “The Ethics and legality of port scanning “, 8 October 2001.

3) “Remote OS Detection “, using TCP/IP Scanning 2nd Generation.

4) “Port Scanning techniques and the Defence Agents Them “5 October 2001.

5) Official Certified Ethical Hacker Review Guide, Willy 15 February 2007.

6) Self-Port Scanning tool.

7) Nmap Reference Guide.

8) TCPDUMP Reference Guide.

9) Detection of Slow Port Scanning Attacks Reference Guide.

10) A Baseline Modelling Algorithm for internet ports scans

11) Network Reconnaissance investigation.

12) Measuring Vulnerabilities of the computers.

13) Cyber Scanning Tools Guide.

14) IPV6 Deployment Security Risk Assessment.

15) Computer Focuses Crimes Impacted by System Configurations.

16) Network Forensic System for port scanning attacks.