DOI: https://doi.org/10.53555/nncse.v2i3.468 **Publication URL: http://nnpub.org/index.php/CSE/article/view/468**

PORT SCANNING AND ITS DETECTION IN PHYSICAL NETWORK

Nitish G. Pandey[1]*, Roshan S. Thakur[2]
*[1]*Dept. of CSE, DBACER, Nagpur,* [2]*Assistant professor, DBACER, Nagpur,*

Corresponding Author: -

Abstract: -

The networking infrastructure is growing day by day and becoming more complex. With the increase in the networks, the number of attacks on these networks or some hosts in the network also increases. The main concern now-a-days is to provide network security. The attackers carry out various types of malicious activities in order to harm the system or to get some information. One of the techniques is port scanning. The attackers carry out scanning of various ports in order to gain information of about various types of services that are available. The attackers send messages to various ports and waits for an answer. This message helps to get information about various types of services that are present at all the ports. The network administrators also use port scan in order to check the system vulnerabilities. The port scan detection helps to know the IP address of the hosts that are doing the port scan in a network. The detection of these scanning activities thus becomes very important. The detection helps to take the necessary preventive measures after port scanning of the ports on a system is been detected.

Keywords: - *Port scan, Ports, attackers, malicious activities, Port scan detection, Network, Network Administrator.*

I. INTRODUCTION

With the advancement in the internet technology there is also the huge web of networking infrastructure that is spreading around the world. The networks can be local or global and the number of users or hosts in these networks can vary. The attacks on these networks and the hosts inside the networks can be made frequently. These attacks can be made using various types of techniques. One of the techniques is port scanning.

Port scanning is a technique which is used by both the attackers and network administrators. Attackers use it to launch future attacks and network administrator uses it to look for any sort of intrusions in the network.

Ports are categorized into three types:

1) Well known ports (0-1023)
2) Registered ports (1024-49151)
3) Dynamic ports (49152-65535)

These port scanning techniques can be a huge threat to any system. In order to protect the system by the port scanning activities a port scan detection system needs to be developed. The detection plays a key role for figuring out intrusions in the network. This detection system can be huge advantage for the network administrator who is responsible for providing network security. This detection of intrusion in the network can be beneficial for the network administrator to take further steps to avoid such intrusions.

II. LITERATURE REVIEW

1) In this paper, the packet sampling technique is used to avoid usage of large amount of memory and also not to all allow huge processes to be carried out by the CPU. There are two types of sampling techniques used. They are packet sampling technique and Flow sampling technique. Packet sampling technique is mostly preferred over flow sampling technique. As packet sampling requires less memory and CPU power. Port scan detection technique is used in this packet sampling technique to alert about potential port scan that is being carried out on various ports.
These port scan detection technique uses two algorithms TRWS (Threshold Random Walk) and TAPS (Time Access Pattern Scheme) to detect port scans. TRWS checks for the connection status to determine whether scanning source is an intruder or a host. In TAPS the time plays a crucial role to determine the detection success rate and the threshold helps to tell about failure rate of the connection.

2) In this paper, the various types of port scanning tools and security techniques are used. The features about all available port scanning tools like Nmap, 1st IP port scanner, Angry IP port scanner etc are given. The paper also shows some of the basic security techniques like Turn off ping service, closed unused ports, Bind IP to MAC address, Use Intrusion Detection and Intrusion Prevention System.

III. METHODOLOGY

There are four types of scans in port scanning techniques. They are:

1) Vertical scans
2) Horizontal scans
3) Strobe scans
4) Block scans

1) Vertical scans:

Vertical scan is a type of port scan in which several ports of a single host is scanned in order to gather information. This type of port scanning is very easy as the scanning is carried out on a single system.

2) Horizontal scans:

Horizontal scan is a scan in which the single port which is present in all the system in the network is scanned.

3) Strobe scans:

Strobe scan is used to scan few more ports as compared to horizontal scan.

4) Block scans:

Block scan is a combination of both vertical scan and horizontal scan. It scans the entire system.

IV. WORKFLOW

Port scanning can be a more beneficial tool for the attackers. They can use this technique to learn about a vulnerable system and launch future attacks on a system. Thus, Port scanning detection plays a very important part in an intrusion detection system. Port scan detection can be a healthy tool for the network administrator who can check for all the attacks that are carried out. They can even analyze the packets and gather the information of this attack.

Port scanning:

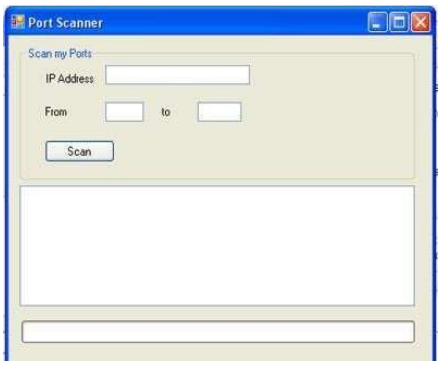

Figure (a): Port scanner

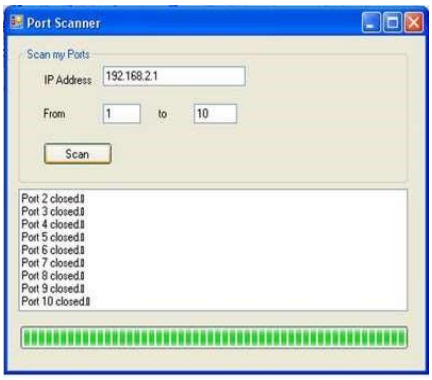

Figure (b): finds open and closed ports

Port scanning can be helpful for checking the range of ports of a given IP's. This will give a list of all the ports that are open or close. Thus it can play a vital role in identifying the intrusion.

Port scan detection:

The main purpose of this module is going to be the detection of all the hosts that are performing port scanning on a particular host. The three main parts of the port scan detection module are: Detection of port scanning IP's, Identifying open ports and frequently incoming requests on ports.

Detection of port scanning IP's:

This part of the module will be helpful in detecting the IP's of all the hosts which are carrying out port scanning on a particular system. This detection part presents a column of port scanning IP's. It can be worthwhile in distinguishing between a attackers and non-attackers.

Identifying open ports:

The number of open ports that are present on a system can be displayed. This gives a clear picture of the all ports which is been used by other system.

Frequently incoming requests on ports:

The detection of number of frequently incoming requests on various ports can be advantageous for identifying the attack on the system.

These three parts are going to provide all the basic information that is required to differentiate between the attacker and the actual user.

V. CONCLUSION

In this paper, we studied various types of port scanning techniques. We also came to know about different category in which all the ports are divided.

We concluded that, the port scans can be beneficial when used with good intention but can be disadvantageous when used to fulfill false goals.

Port scan detection module is another part which helps to detect the port scanning attacks which is performed by various attackers. In the detection part we concluded that if there is any type of attack on any host then it can detect the IP's of that attacker which is carrying out intrusion in the system.

VI. FUTURE SCOPE

Port scan detection module can be combined with various other Intrusion detection or Intrusion prevention modules to build an integrated module which can detect and take the required steps on the attackers. With the further advancements, Port scan detection module can be helpful in building antihacking software's.

Port scanning module can be made more effective if integrated with network intrusion detection module. For developing better and more efficient intrusion detection system the more powerful port scanning technique can be performed.

REFERENCES

[1].Jianning Mai, Ashwin Sridharan, Chee-Nee Chuah, Hui Zang and Tao Ye," Impact of Packet Sampling Detection",IEEE
[2].Rajwinder Kaur, Gurjot Singh"Analysing Port Scanning Tools and Security Techniques, "IEEE, International Journal of Electrical Electronics & Computer Science Engineering Volume1, Issue 5 October 2014.
[3].Cyntia Bailey Lee, Chris Roedel, Elena Silenok," Detection and Characterization of Port Scan Attacks."
[4].Stuart Stanford, James A. Hoagland, Joseph M. McAlerney," Practical Automated Detection of Stealthy Port scans."
[5].Monowar H.Bhuyan, DK Bhattacharya and JK Kalita, "Surveying Port Scan and Their Detection Methodologies."
[6].Chris Muelder, Kwan-Liu Ma and Tony Bartoleth," Interactive Visualization for Network and Port Scan Detection."
[7].Susmit Panjwani, Stephanie Tan,Keith M.Jarrin and Michel Cukier, "An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack."
[8].Leonardo Aniello, Giorgia Lodi and Robert Baldoni," Inter-Domain Stealthy Port Scan Detection through Complex Event Processing."