IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

A Descriptive study of Active Scanning & Reconnaissance tools

Manjit Kaur[1], Gurpreet Kaur[2], Er. Gurjot Singh[3]

Post Graduate, P.G. Department of Computer Science & Applications, K.M.V., Jalandhar, Punjab, India [1,2]

Asstt. Prof., P.G. Department of Computer Science & Applications, K.M.V., Jalandhar, Punjab, India [3]

Abstract: Scanning is a skilled of pinpointing active and communicable system via internet. It makes use of assorted approaches such as operating system identification and port scanning to be aware of various services which are solicited by the system. It offers us information concerning the TCP/UDP services which are active on each discovered system, architecture of the system, type of operating system etc. Today, there is a constant increase in the number of automated scanners which further provides a path for the successful set up of attacks. A part scanner is a piece of software framed to rummage a network for open ports. This is commonly used by administrators to keep an eye on the security of their networks and by hackers to compromise it. Programs make use of ports to see and acknowledge the out of doors world. Viruses now have inbuilt port scanners that rummage the internet searching for unsuspecting computers with open ports, when they discover them, they cripple our software or worse, stay hidden and report our secret activity and subject matter to another system. In this paper, we have studied the detailing of ports, relative services running on particular ports and also extend the critical subject matter concerning port scanning tools. We have also discussed the literature of active scanning.

Keywords: Port Scan, Nmap, Zenmap, Scanrand, ultra scan, unicornscan.

I. INTRODUCTION

The port scanning is a process of scanning all the ports of a computer system. A port is a spot or a point from where information goes in and out of a computer. The port scanning identifies open ports or we can say open doors of a system. Port scanning helps in network management, but it can also be used in a destructive way by the attacker or the hacker who tries to sniff for a weak access point to breach into the computer system with critical attacks like DOS, Botnet and DDOS. An attacker can also compromise the vulnerable hosts by performing port scanning of IP addresses. In this paper we talk about various port scanning tools and the security techniques to prevent port attacking [21].

Every computer runs on many different ports. For example, when a person opens his or her email, the server of a computer will open a port through which we can download a new mail through a connection to the email server. There are certain ports which are opened continually on an individual's personal computer, making them a target for any potential hacker who is searching for individuals to victimize. With this the person's sensitive and personal information can fall into the hands of those who can use it for criminal activity. Unluckily, criminals and computer hackers are always looking for new victims to exploit, and this can be accomplished with the help of port scanning.

Port scanning is the invasive examining of system ports on the transport and network level. Port Scanning can be defined as a technique which is used to identify services and open ports available on a network host. It is sometimes used by security technicians to check system for vulnerabilities; however, it is also used by hackers to target victims. It can also be used to send requests to make connections to the targeted computers, and then keep track of the open ports, or those that respond to the request.

When a criminal comes to a house for a burglary, the first thing that he or she makes sure of is if there is an open window or door through which he or she can enter into the house. A Port scan is also same, only the windows and doors are the ports of the personal computer of an individual. While a hacker may not decide to "break in" at that moment, he or she can find out if easy access is available or not. However, many people feel that this activity should be illegal, but in most areas is not regarded as a crime because an attacker merely checks if a possible connection could be made or not. However, if port scanning is done repeatedly, a denial of service can be created. Hackers make use of port scanning because it is a simple method of quickly discovering services they can exploit. In some cases, hackers can even open the ports themselves in order to gain access to the targeted computer. Hackers also make use of port scanners to check for open ports on personal computers on the web.

Port scanning can be defined as a process of testing a range of IP addresses to know the services which are running on a network. It means to find the ports which are open on a computer and the services which are running on it. It can be regarded as a most popular technique which is used by attackers to discover services that they can exploit to break into the individual's computer. All systems which are connected to a LAN or the Internet through a modem run services that listen to most used and less used ports.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

With the help of port scanning, the attacker can find much information about the targeted systems such as what services are currently running, under which users those services are running, whether anonymous logins are supported, and whether the network services require authentication etc.

1.1 **Well-known ports**

Only port numbers from 0 to 1024 are reserved for privileged services and are called as well-known ports. Well-known ports are stated in RFC 1700. In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way in which a client program designates a specific server program on a computer in a network. The port number detects what type of port it is. For example, port 80 is reserved for HTTP traffic. Some ports have numbers which are pre-allocated to them by the IANA, and these are designated as "well-known ports" which are stated in RFC 1700. List of Well-known ports are shown in table 1.

Port numbers range from 0 to 65536, but only the port numbers which are in range of 0 to 1024 are reserved for privileged services and designated as well-known ports. These well-known port numbers specifies the port used by the server process as its contact port.

Table1. Description of well known ports

Port Number	**Description**
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP – Data
21	FTP – Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)
118	SQL Services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
1080	Socks

II. LITERATURE SURVEY

Port scanning permits a hacker to deduce what services are running on the systems that have been pointed out. If vulnerable or insecure services are tracked down, the hacker may be able to exploit these to gain unauthorized access. We have a total of 65,535 * 2 ports (TCP & UDP). While a complete scan of all these ports may not be feasible, analysis of popular ports should be performed.
By port scanning, one is able to find out which ports are accessible. Factually, a port scan consists of sending a message to each port, one at a time and analyzing the response received. If the port is in use, it can then be examined further for weakness. Port Scanning is one of the most favoured reconnaissance techniques which attackers use.

By port scanning, one discovers which ports are available (i.e. being listened to by a service). Essentially, a port scan consists of sending a message to each port, one at a time and examining the response received. If the port is in use, it can then be probed further for weakness. Port Scanning is one of the most popular among the reconnaissance techniques attackers use.

In [1] Fyodor has suggested many techniques used to discover what ports (or similar protocol abstraction) of a host are listening for connections. These ports typify potential communication channels. Mapping their existence smooth`s the exchange of information with the host, and thus it is very useful for anyone who wants to investigate their networked environment, including hackers.

In [2] Marco de Vivo, Eddy Carrasco, Germinal Isern and Gabriela O. de Vivo have set forth that TCP port scanners

are distinctive programs used to discover what TCP ports of a host have processes listening on them for viable connections. Since these ports specify, in part, the amount of manifestation of the hosts to potential external attacks, knowing their existence is a elementary matter for network and/or security administrators.

In [3] Pete Herzog has suggested that Port scanning is an invasive examining of system ports on the transport and network level. The paper also includes the validation of system reception to encapsulated, tunneled or routing protocols. This parameter is to calculate live or accessible Internet services as well as penetrating the firewall to discover additional live systems. Testing for different protocols will depend on the system type and services it provides.

In [4] Roger Christopher has described that Port Scanning is one of the most favourable techniques attackers use to find services that they can enslave to break into systems. All systems connected to a LAN or the Internet with a modem run services that listen to the ports which are well-known and not so well-known. By port scanning, the attacker can gather the following information about the targeted systems: what services are executing, under what users those services run, whether anonymous logins are supported or not, and whether certain network services require authentication or not.

In [5] Brenden claypool have described that Port scanning is a skillful and efficient way which is used by attackers, curious individuals, and administrators to gather information from computers on a network. System and network administrators take the help of port scans to find out open ports to a system so that they may be able to access those ports, or shut them off fully. The way attackers and administrators use port scanning is the same but the only difference lies in their purpose. The attackers use port scanning for malicious purpose. There are many techniques which are used in stealth scanning, ranging from those that prevent their detection by logging systems, identity concealment, to confusing the server with invalid information. All of these techniques are interesting in their implementation and execution.

In [6] Harry Anderson has described that Port scanning appears simple on the surface but is actually a very complicate subject. One factor which makes port scanning tough is the response system. Accuracy, stealth and speed are the principal factors to stabilize when scanning the ports. The factors which affect these are timeouts, the type of scan and what ports to scan. The two most often used types of scans are the SYN scans and connect (). There is disparity of both in Nessus and in the optional NMap component.

In [7] Nazar El-Nazeer and Kevin Daimi have put the light on network port scanning tools. A port is an application noticeable software construct acting as an endpoint in many communications. The Transmission Control Protocol (TCP) and the User Diagram Protocol (UDP) of the Transport Layer mainly uses the ports. Ports are recognized by numbers. For example, Port 25 is used for Simple Mail Transfer, and port 80 is reserved by HTTP. A port scan is an attack that tries to discover known vulnerabilities of a service running on active ports. Both network administrators and attackers use port scanner tools to examine servers/hosts for open ports, but with different purposes.

In [8] Gadge, J. Patil, and A.A. have proposed that Port scanning is a phase in foot printing and scanning; this comes in reconnaissance which is regarded as the first phase of a computer attack. Port scanning aims at finding open ports in a system. These open ports are taken as an advantage by attackers to carry out attacks and exploits. There are a number of tools which are used for scanning open ports. However, very few tools are present to detect port scanning attempts.

In [9] Zhang and Fang have proposed a new port scan detection approach known as time-based flow size distribution sequential hypothesis testing (TFDS) for transit networks which are having high speed where only unidirectional flow information is available. TFDS makes use of the foremost ideas of sequential hypothesis testing to detect scanners that exhibit abnormal access patterns in terms of flow size distribution entropy.

In [10] Monowar H Bhuyan, D K Bhattacharyya and J K Kalita, have described that the Scanning of ports on a computer occur habitually on the Internet. An attacker conducts port scans of IP addresses to discover vulnerable hosts so as to compromise them. However, it is also helpful for system administrators and other network defenders to discover port scans as possible preparatory measures to more serious attacks. It is a very tough task to recognize instances of malicious port scanning. Port scanning is designed to examine a network host for open ports and other services accessible. From the attacker's viewpoint, a port scan is helpful for collecting relevant information for initiating a successful attack. Thus it is of appreciable interest to attackers to determine whether or not the defenders of a network are scanning ports frequently. Defenders do not often conceal their identity during port scanning while attackers do.

In [11] Mehiar Dabbagh, Ali J. Ghandour, Kassem Fawaz, Wassim El Hajj and Hazem Hajj have suggested that port scanning is generally divided into two main parts, horizontal and vertical. In horizontal scans, the same port is scanned on the multiple hosts. This is helpful for attackers who want to gain access on victim hosts by exploiting a known vulnerability of a definite service running on that port. While in vertical attacks, multiple ports are scanned over the same host. This is common for attackers who are collecting information to attack a particular target host. Port scanning is the most favorable reconnaissance technique which attackers use to determine services they can exploit. Port scanning detection has got a lot of attention by researchers.Nevertheless, a slow port scan attack can defraud most of the existing Intrusion Detection Systems (IDS).

In [12] Mustafa Al-Tamimi, Wassim El-Hajj and Fadi Aloul have suggested that Port scanning is one of the most favourable reconnaissance methods that many attackers use to profile running services on a prospective target before starting an attack. Many port scanning detection techniques have been put forth in literature. However, very little work has been done on creating port scanning benchmarks that researchers can take help of to test their detection methods.

In [13] Tariq Ahamad Ahanger has suggested that Port scan is an act of efficiently scanning the ports of a computer. As we know that a port is a place where information goes into and out of a computer, port scanning detects open doors to a computer. Port scanning has admissible uses in management of networks, but port scanning also can be harmful in nature if someone is looking for a weak point in order to access your computer.

In [14] Avi Kak has suggested that the main aim of port scanning is to spot out which ports are open, which are closed, and which are filtered. By the term filtered, he means that the packets passing through that port are following the filtering rules of a firewall. If you send a SYN packet on a port which is open for incoming connection requests on remote host, then the remote host will answer back with a SYN+ACK packet. If your computer sends a SYN packet on a closed port on remote host, the remote host will answer back with a RST packet.

In [15] Sunil Kumar, Kamlesh Dutta and Ankit Asati have proposed that a port scan detection technique called CPST to find weather a particular source is scanner or a benign host by using connection status and pattern of the connection. They have shown that this technique works efficiently under different sampling methods. Port scanning is one of the anomaly detection, which is carried out in the network for the purpose of the security. When an intruder or attacker wants to compromise the network, then first he want to examine the whole network, for example, which operating systems are being used in network or what ports are open or available or which service is running on the particular host.

In [16] Rajni Ranjan Singh and Deepak Singh Tomar have described that Stealth is regarded to be a type of port scan which is unidentified by available auditing tools such as routers, firewall, filters etc. A stealth port scan method does not generate any TCP sessions; hence, none of these scans should come into sight in any of the application logs. Therefore, it is of great importance to research and acquire methods for the detection and attribution of stealth port scanning attack. In this paper, they have proposed a network forensic architecture for detection and analysis of stealth port Scanning attack.

In [17] Cynthia Bailey Lee, Chris Roedel and Elena Silenok have described that Port scans represent a fairly large part of today's Internet traffic. Nevertheless, there has been little research specifying port scan activity. One of the popular methods for finding vulnerable hosts is port scanning. Port scanning can be termed as "hostile Internet searches for open 'doors,' or ports, through which intruders can gain access to computers." This technique comprises of sending a message to a port and observing an answer. The received response states the port status and can be useful in finding a host's operating system and other information pertinent to launching a attack in future.

In [18] Susmit Panjwani, Stephanie Tan, Keith M. Jarrin, and Michel Cukier have described an experimental approach to determine the correlation between port scans and attacks. In this paper, attack data were collected using a test-bed devoted to monitoring attackers. The data gathered consist of port scans, ICMP scans, vulnerability scans, successful attacks and management traffic. Two experiments were done to validate the hypothesis of linking port scans and vulnerability scans to the number of packets perceived per connection. Customized scripts were then developed to filter the collected data and batch them on the basis of scans and attacks between a source and destination IP address pair. The correlation of the filtered data groups was assessed.

In [19] Urupoj Kanlayasiri, Wipa Jaratmanachot and Surasak Sanguanpong have presented that Port scanning attack is a technique for spotting out exploitable communication channels that has been used for a prolonged time. The key idea is to examine the network ports and then store the information about them that are helpful for an attack. In some viewpoints, port scanning is not taken as a network intrusion but it is regarded as the method for discovering the possibilities to adverse system. At present, there are many methods to do port scanning probes such as, TCP connect scanning, Stealth scanning, TCP half-connect scanning, NULL scanning and Xmas Tree scanning. All of the above techniques need TCP packet to complete scanning. Port scanning could be categorized as one of the network intrusions.

In [20] Chris Muelder, Kwan-Liu Ma, and Tony Bartoletti have described that many times, network intrusion attempts start with either a network scan, where a connection is endeavored to every possible destination in a network, or a port scan, where a connection is endeavored to each port on a given destination. Being able to discover such scans can be useful in identifying a more harmful threat to a network. Many techniques exist to automatically identify scans, but these are mainly dependant on some threshold that an attacker could possibly circumvent crossing. In this paper, they have put forth a means to use visualization to identify scans interactively.

III. ACTIVE SCANNING TOOLS

Many port scanning tools available for mostly every operating system that can be connected to a TCP/IP network. The most feature-rich one is probably Network mapper. While there are other scanning tools that exploit different problems with TCP/IP implementations such as Hping2, the extensive majority do not have any stealth

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

technologies built-in at all. This is good news for the system administrator, after all these will be very easily picked up by logging programs and even the most basic intrusion detection system. The other details of the port scanners are shown in table 2.

Table 2: Description of Port Scanning tools

Tool name	License	Features	Operating System
NMap	GPL v2	Host discovery, Port scanning, Version detection, OS detection, Scriptable interaction with the target.	Cross platform
Super Scan	freeware	Detect open TCP and UDP ports on a target computer, determine which services are running on those ports, and run queries such as whois, ping, ICMP traceroute, and Hostname lookups.	Windows 2000/XP/ Vista/7
Tcpdump	BSD license	Display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.	Linux/ Solaris/free BSD/net BSD/ open BSD/OS X/android/ Windows
Unicorn-scan	GPL v2	Asynchronous stateless TCP scanning with all variations of TCP flags, asynchronous stateless TCP banner grabbing, and active/passive remote OS, application, and component identification by analyzing responses.	Linux
Ultra scan	GPL v3	Provide you the ability to seek out unauthorized web servers, FTP servers, and any other service which may be running on your network without your knowledge.	Windows, Mac OSX or Linux
Scanrand	Freeware under BSD license	Executes separate scanner and listener processes by embedding and analyzing hashed initial sequence numbers in packets	Linux/ Unix platform
Network Activ Port Scanner	Freeware	○ UDP port scanner with automatic speed control, UDP subnet port scanner, Ping scanning of subnets, TCP subnet port scanner, for finding Web servers and other servers, High performance trace-route.	Windows (c) *98/*ME/* NT/2000/* XP/*2003 Server
Atelier Web Security Port Scanner	Share-ware	Fast reliable UDP Port scanner with intelligent test probing of ports to confirm whether the host is up, State-of-the-art NetBIOS scanner, Unique Mapping of Ports to applications feature, Local Connections and Listening Ports instant report, Local TCP, UDP and ICMP statistics instant report, Local Active Routes, DNS Servers and Persistent Routes.	Windows 2000, Windows 95/98, Windows NT.
Angry IP Scanner	freeware	• Scans local networks as well as Internet, IP Range, Random or file in any format, • Exports results into many formats, Extensible with many data fetchers, Provides command-line interface.	Windows/ mac/Linux
1st Ip Port Scanner	Share-ware	Find IP address, IP trace, IP search, port scanner, port Finder etc.	Win NT 3.x, Win NT 4.x, Windows2 000, WinXP

1. NMap

NMap is considered to be one of the best port scanner tool, and stealth scanning tools available today. NMap is designed to allow system administrators and analytical individuals to scan large networks to determine which hosts are up and what benefits they are offering. NMap is the base for all of the major stealth scanning techniques, and adds new opportunity as they are discovered. It also supports IP spoofing, fragmenting, decoying and a number of useful features. Network Mapper was written with the security auditor in mind to perform intrusion detection and port scanning detection tests. What is accessible to the system administrator is also available to the attacker, so a diligent administrator must be as aware of what NMap can do for him or her, as aware of what it can be used for by attackers. After the usual scanning technology, network mapper can also be used to remotely identify a host's operating system. This is done through a technique known

as TCP/IP fingerprinting. The premise of this is that TCP/IP is a specification, but the implementation of it into a functioning of the computer has differed slightly between software companies. When the data is correct, each and every implementation reacts the same, but when false data is sent to a TCP/IP stack, each implementation reacts a little differently. These differences can be compared to other operating systems and a fingerprint is created. This is useful when scanning for distinct services.
Zenmap is the official NMap security scanner graphical user interface. It is a multi- platform such as Linux, windows, Mac OS X etc. Zenmap is open source and free application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Network mapper users. Generally used scans can be saved as profiles to make them easy to run repeatedly. A command designer allows interactive creation of NMap command lines. Scan results can be viewed and saved later. Saved scan results can be correlated with one another to see how they differ. The result of recent scans is stored in a searchable database.

2. SuperScan
A Windows-only port scanner, resolver and pinger Super Scan is a free Windows-only closed-source TCP/UDP port scanner by Foundstone. It includes a collection of additional networking tools such as http head, ping, whois, traceroute and many others. Superscan provides various features such as superior scanning speed, support for unlimited IP ranges, enhanced host detection using multiple ICMP methods, UDP scanning, simple HTML report generation ETC.

3. Tcpdump
Tcpdump is a tool used for packet capturing, network monitoring and protocol debugging. It is the oldest port scanner tool and most generally used command line tool, which works only on Linux based systems. It is free and open source software. Tcpdump can be used to read live capture or already captured log file. It can be run remotely by telnet or SSH login. It gives the least overhead as it not use any graphical interface and captures data in libpcap formats, which is used in most of the tools. It uses a large range of packet filters. At the end of the communication or whenever TCP dump is stopped, it displays number of packets displayed and number of packets dropped. It does not have any graphical display. Tcpdump works on most Linux like operating systems such as Solaris, BSD, and Android and windows operating system.

4. Unicornscan
Unicornscan is an open source (GPL) tool aimed to assist with security auditing and information gathering. It is an effort at a User-end Distributed TCP/IP stack for gathering the information and their interrelation. It provides a higher-ranking interface for instigating a stimulus into and evaluating a response from a TCP/IP enabled devices. The various features of this scanner includes asynchronous stateless TCP scanning with all disparities of TCP flags, asynchronous stateless banner grabbing, and active/passive remote OS and component identification by examining responses. It provides Scalable, precise and systematic system scan. It is disclosed for the community to use under the terms of the GPL license.

5. Ultrascan
UltraScan is an influential port scanning tool that can impart you the ability to seek out unauthorized web servers, FTP servers, and any other service which may be running on your network without your knowledge. This tool is a important for any network connected to the Internet or large corporate Intranet.

6. Scanrand
Scanrand is a tool that is used to detect hosts on the network i.e whether the host is alive or not. It is trust worthy for efficient fast speeds. It uses best cryptographic techniques to avert users from attackers. This scan is similar to unicornscan. It is a speedy network scanner that can scan single hosts on very large networks efficiently. However, several network mapping utilities brag this same claim. Scanrand can do stateless TCP scanning, which makes it different from the other network scanners.

7. Network Activ Port Scanner
It is an administration and a network exploration tool that permits you to scan internal LANs and external WANs. The adaptability and closable operating mode nature available in NetworkActiv Port Scanner makes it of great help to experienced network administrators. It imparts all the basic functionality that you should presume in an advanced network scanner, but also provides many more features and technologies, some of which being entirely unique to this scanner. It provides scanning performance which is not found in other Windows based network scanners [21].

8. Atelier Web Security Port Scanner
AWSPS can provide significantly beneficial information about other networked Machines user. It provides first rate listing of port set up on the local machine detailing which ports are open. It shows traffic detail for TCP, UDP as well as for control packets ICMP including ping. Atelier Web Security Port Scanner is an innovative network diagnostic tool that adds a new dimension of abilities to the network administrators, security professionals and all people concerned with safety of systems. It provides TCP scanning functionality and UDP port scanning, local network enumeration and a remarkable detail on the local network which is set-up for a machine on a local area network [21].

9. Angry IP Scanner
Angry Ip scanner is a tool that examines network for open Ip addresses designed for network administrator to check the network security. Angry IP Scanner is a cross-platform port and IP scanner. The application is developed in java, so it is cross platforms compatible with different OS. It is a great program for doing a network audit or for just finding out more information about your network. It can locate in any network device that responds to the scan. It can locate on any device in the network that has an IP

address and that doesn't have any firewall. It performs basic host discovery and port scans on Windows. The size of its binary file is very small as compared to other scanners and other pieces of information about the target hosts that can be extended with plug-in[21].

10. 1st Ip Port Scanner

1st Ip Port Scanner is a very efficient Ip Scanner and Port Scanner. It is intended for both system administrators and general users to examine and manage their networks. Powered with multi-thread scan technology, this program can scan hundreds of computers per second. It simply pings each IP address to check if it's alive, then optionally it scans ports and resolves its hostname. Free IP scanner can also display NetBIOS information: host name, workgroup, currently logged user and MAC address and it can also find port, search port and scan port. Its speed of scanning is very fast.1st Ip Port Scanner tests whether a remote computer is alive with three types: ICMP, SYN and UDP and testing whether a TCP port is being observed with two types: CONNECT and SYN [21].

IV. CONCLUSION

In this paper, we have studied port scanning literature and tools opted for port scanning. The main goal of port scanners is to scan the ports but they may differ in the way they scan the ports and the services running on them. These port scanning tools not only scan the ports but provide may other features too. For example, Nmap which is a popular port scanning tool, besides scanning the ports, it also discover the hosts, detects operating system etc.

The port scanner offers many technological benefits such as system monitoring and its performance enhancement. In addition to these, it also extends system security. This is also commonly used by administrators to check security policies of their networks and by attacker to discover services active on a host and enslave these vulnerabilities. By multi threading concept, port scanner can scan multiple ports simultaneously, which is quite time saving.

REFERENCES

[1] Fyodor, "The Art of Port Scanning", Volume 7, Issue 51, September 01, 1997.
[2] Marco de Vivo, Eddy Carrasco, Germinal Isern, Gabriela O. de Vivo, "A Review of Port Scanning Techniques", Lacore U.C.V.
[3] Pete Herzog, "Open-Source Security Testing Methodology Manual", 5 july 2001.
[4] Roger Christopher, "Port Scanning Techniques and the Defense Against Them", SANS Institute Infosec reading room, October 5, 2001.
[5] Brenden Claypool, "Stealth Port Scanning Methods" Global Information Assurance Certification Paper, SANS Institute 2000 – 2002, volume 1.4.
[6] Harry Anderson, "Nessus, Part 2: Scanning", December 16, 2003.
[7] Nazar El-Nazeer and Kevin Daimi, "Evaluation of Network Port Scanning Tools".
[8] Gadge, J. Patil, and A.A., "Port scan detection", 16th IEEE International Conference on Networks, 2008.
[9] Zhang, Y. and Fang, B. (2009) A novel approach to scan detection on the backbone. Proceedings of ITNG'09, Washington, DC, USA, April, 27-29, pp. 16–21. IEEE Computer Society.
[10] Monowar H Bhuyan, D K Bhattacharyya and J K Kalita, "Surveying Port Scans and their Detection Methodologies", Volume 54, Issue 10, April 20, 2011.
[11] Mehiar Dabbagh, Ali J. Ghandour, Kassem Fawaz, Wassim El Hajj, Hazem Hajj, "Slow Port Scanning Detection", 2011 IEEE.
[12] Mustafa A1-Tamimi, Wassim E1-Hajj and Fadi Aloul, "Framework for Creating Realistic Port Scanning Benchmarks", 2013 IEEE.
[13] Tariq Ahamad Ahanger, "Port Scan - A Security Concern", International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 10, April 2014.
[14] Avi Kak, "Computer and Network Security", April 9, 2015.
[15] Sunil Kumar, Kamlesh Dutta, Ankit Asati, "Two Pass Port Scan Detection Technique Based on Connection Pattern and Status on Sampled Data" Journal of Computer and Communications, 2015, 3, pp. 1-8, September 2015 in SciRes.
[16] Rajni Ranjan Singh and Deepak Singh Tomar, "Network Forensics: Detection and Analysis of Stealth Port Scanning Attack", International Journal of Computer Networks and Communications Security VOL. 3, NO. 2, February 2015.
[17] Cynthia Bailey Lee, Chris Roedel, Elena Silenok, "Detection and Characterization of Port Scan Attacks", February 11th-*17th*, 2001.
[18] Susmit Panjwani, Stephanie Tan, Keith M. Jarrin, and Michel Cukier, "An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack", Yokohama, Japan, June 28, 2005 to July 1, 2005.
[19] Urupoj Kanlayasiri, Surasak Sanguanpong and Wipa Jaratmanachot, "A Rule-based Approach for Port Scanning Detection", 23rd Electrical Engineering Conference Chiangmai, November 2000.
[20] Chris Muelder, Kwan-Liu Ma, and Tony Bartoletti, "Interactive Visualization for Network and Port Scan Detection", RAID'05 Proceedings of the 8th international conference on Recent Advances in Intrusion Detection, September 7, 2005.
[21] Rajwinder Kaur, Gurjot Singh, "Analyzing Port Scanning Tools and Security Techniques", International Journal of Electrical Electronics & Computer Science Engineering Volume 1, Issue 5 (October 2014).