MAT JOURNALS
Journal of Data Mining and Management
e-ISSN: 2456-9437
Volume 03, Issue 02
4th National Conference on Advancements in Information Technology

Analyzing Port Scanning Tools and its Performance

Miss. Bindu S, Mr. Khodanpur B I
Department of Information Science
Dayananda Sagar College of Engineering
Bangalore, India
Email: sbindu63@gmail.com, bi.khodanpur@gmail.com

Abstract
Port scanning is a process of scanning ports of a host. A port is an access point where data flows in and out of a computer. An open or closed port of a host can be identified using a port scan. Port scanning helps in handling the networks, but it can also cause damage as if someone is looking for a weak spot to breach into the system by performing critical attacks like Botnet, DOS or DDOS. To find the hosts that are vulnerable, an attacker performs port scanning of IP addresses. In this paper we will discuss few free port scanning tools and analyze the results generated in a network scan.

Index Terms: *Advanced Port Scanner, Angry IP Scanner, filtered, ICMP, MAC Address, Net Crunch, Nmap, Soft Perfect Network Scanner, TCP, UDP, vulnerability.*

INTRODUCTION

Port scanning is a process of gathering the information (reconnaissance phase) of the computer system. Port scanning is an important step which is used for collecting the loop holes of the system and take preventive measures to safe guard the system from hackers [6]. Gathered information is used by hackers to attack vulnerable systems. The technique used by port scanning is, sending a message and waiting for a response. Port scan is performed to get the present state of the port whether it is open, closed, or filtered. Port scan is a method of scanning ports in the computer [7]. Ports are an access point for data to flow in and out of the computer. Port scanning is like ringing a door bell of a house, if anyone responds then there is someone at home else there is no one at home. In the same way, in hacking we send request to the host to check if whether the port is open or closed; if the host responds with a message then it means that the port is open and active else port is either filtered or closed. Hackers choose port scan because they can easily discover the services on which they can break into. There are some port scanning tools which are being used by network administrators to confirm security policies in their networks and hackers to identify services running in the host and exploit vulnerabilities [2].

Types of Port Scanning

TCP Scanning: TCP Scanning is a simplest port scanner which uses operating system's network function. If it finds an open port, the operating system will complete three-way handshake, and without any delay port scanner will close the connection to avoid DOS attack. If the port is closed, error code is returned [13].

SYN Scanning: SYN Scan is another form of TCP scanning, instead of using operating system's network function, raw packets are generated by port scanner i.e., SYN packet, if there is an open port it responds with a SYN-ACK packet; before completing the handshake, port scanner closes the connection by sending RST packet. A closed and unfiltered port of a targeted host responds with a RST packet. This type of scan is also known as "half-port scanning" as it does not open full

connection [13].

UDP Scanning: To the targeted host, port scanner sends UDP packets, a closed port of target host responds with an ICMP message. If the port is open, target host does not respond. If the port is filtered then the scan falsely reports that the port is open. Application specific UDP packets are used as an alternative approach [13].

ACK Scanning: This scan will not find whether there is an open or close port, but finds if there is a filtered or unfiltered port. This is essentially useful when we are probing with firewalls and its rulesets [13].

FIN Scanning: Firewalls in the target host blocks SYN packets. To bypass the firewall, we use FIN packets. Closed ports in the target host responds with the RST packet while the open port simply ignores the packet [13].

X-mas Scan: This scan is similar to FIN scan. X-mas scan sets URG, FIN and PUSH flags similar to that of a Christmas tree.

Null Scan: No TCP flags are set in the packets sent by the Null Scan [13] i.e., empty packets are sent to the target host.

Protocol Scan: This Scan finds which protocols like TCP or UDP are enabled [13].

Proxy Scan: A proxy is used for performing a scan. Target host sees proxy's IP address as a source [13].

ICMP Scan: This scan determines whether the target system responds to the ICMP messages like echo, netmask, etc [13].

PORT SCANNING TOOLS

NMAP

Tool was built by Fyodor. Nmap (Network Mapper) tool is UNIX and Windows based port scanners. Nmap [8] can also be used as a command-line program. Nmap enables in performing various types of scans in order to identify the services running in the targeted host and also identifies target host's operating system, MAC address, host name, netbios name, and fqdn; it provides options to control the speed of the scan i.e., specifying the time to scan the target host. Nmap is used for security purposes in order to identify which services and applications the host is running, host system fingerprint, or to do a quick inventory on the local network. Nmap is a general purpose network scanner which is used for discovering, monitoring and troubleshooting the systems. It supports most of the operating systems like Windows, Linux, UNIX and Mac OS X.

ANGRY IP SCANNER

Angry IP Scanner tool is developed and maintained by Anton Keks. Angry IP scanner [11] is an IP address and port scanner. Angry IP scanner is program developed using java and hence it is compatible with all OS. It is an open source, light weight and no installation is required. It can scan any range of IP addresses and its ports. Angry IP scanner simply pings each IP address to check if the host is alive, determines host name, MAC address, services, etc. Angry IP Scanner uses multithreaded approach to increase the scanning speed. Results of the scan can be exported into CSV, TXT, and XML files.

ADVANCED PORT SCANNER

Famatech continued to maintain and develop the Advanced port scanner tool after it was launched in 2002. Advanced Port Scanner [12] is a free network scanner which has a friendly user interface and robust functionality allowing user to find

open ports on targeted hosts. Advanced IP Scanner provides program name and version that is running on the detected port. Advanced Port Scanner uses multithreaded approach to complete the scan at the earliest. Advanced Port Scanner allows remote access to the systems discovered in the scan. Advanced Port Scanner allows executing commands remotely on the discovered system and easy access to the resources e.g., shared folders.

NETCRUNCH

NetCrunch [10] monitors the entire IT infrastructure without agent. NetCrunch discover systems with IPv4/IPv6 addresses. NetCrunch monitors network services, bandwidth and traffic flow of switches and routers. NetCrunch supports and monitors most of the operating systems including Windows, Linux, Mac OSX. It monitors files, folders, webpages, WMI or SQL queries. NetCrunch collects the Windows Event log and monitors text log. NetCrunch has a rich user interface that displays network topology, current network traffic structure, volume in the traffic and provides average traffic speed observed in last one hour or 24 hours, detailed view of each node status, dashboards that display top problematic nodes, nodes with slow response, nodes that are heavily loaded, traffic observed in the network, and alerts for user if there are any pending tasks that are to be performed.

SOFTPERFECT NETWORK SCANNER

SoftPerfect is a multipurpose network administration tool for Windows and MAC operating system. SoftPerfect [9] is fast, highly configurable IPv4/IPv6 scanner. SoftPerfect Network Scanner performs both ping and port scan. It identifies shared folders. SoftPerfect scans remote services, registry entries, files and performance. It provides us a feature of exporting network scan results from XML to JSON.

SCANNING APPROACH

To determine performance of a scan on a network, we ran multiple scans using each scanning tool. For every completed scan, we collected information such as time taken to complete the scan, number of hosts discovered, and number of services discovered. We computed average scan time, port discovered for each scanner and depicted in the form of graph.

SCANNING ENVIRONMENT

Machine used for performing the scan is Windows 10 Pro. All the scanning tools were installed on same machine and scans were run one after the other.

Scans were run on a small network with 3 laptops and few mobile phones.
We used free trial version of NetCrunch scanning tool.

SERVICE DISCOVERY

Table 1. *Average Services Discovered By Scan Tool*

Scan Tool	Average Services Discovered
Nmap	4
Net Crunch	3.33
SoftPerfect Network Scanner	3.67
Angry IP Scanner	3
Advanced Port Scanner	3.67

Table 1, depicts the average services discovered by the scanning tool. Average

number of services is computed using the formula,

Average_number_of_services= total number of services discovered by a scanner/ total number of scans run. (1)

We observed that the services discovered by nmap are more compared to that of other scanning tools. SoftPerfect Network scanner and Advanced Port scanner share the same number, average services discovered by Net Crunch and Angry IP Scanner is close to 3.

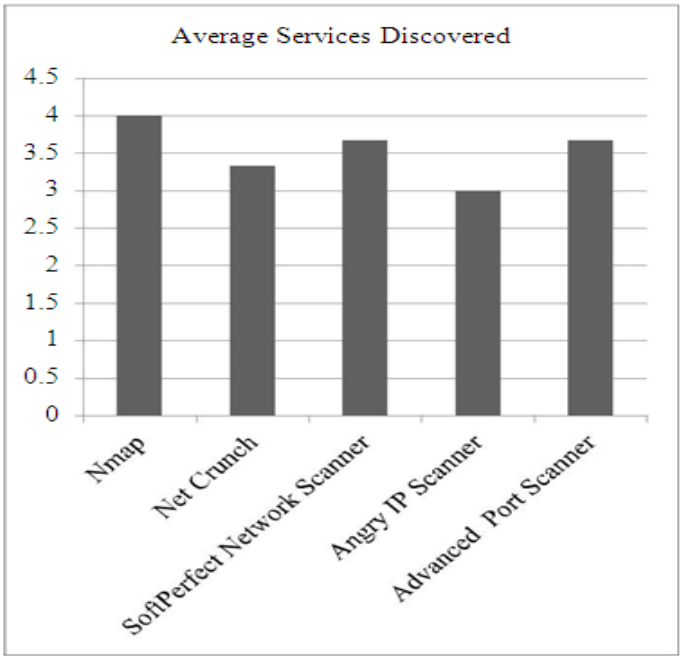

Fig. 1. *Depicted Average Services Discovered by Scanning tool.*

Fig 1, depicts the average services discovered by a scanning tool for the data collected in the Table 1 using a bar graph.

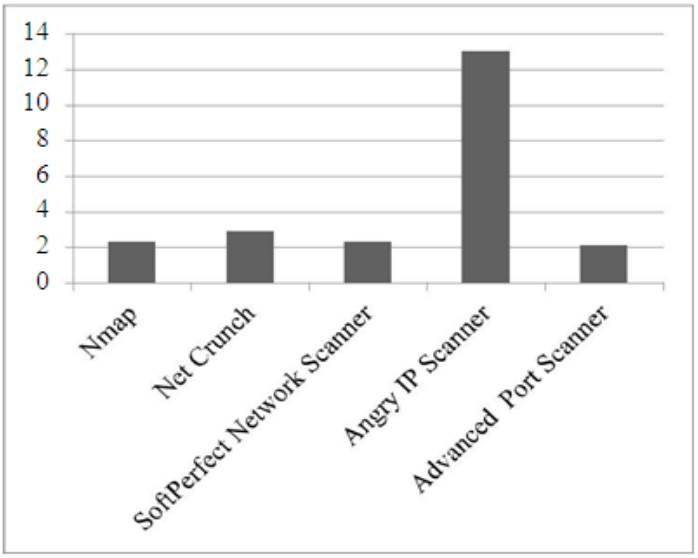

Fig. 2. *Depicted Average Scan Time*

Fig 2, depicts the average scan time taken by the scanners for the data in Table 2 using bar graph.

AVERAGE SCAN TIME

Table 2. *Average Scan Time*

Scan Tool	Average Scan Time in minutes
Nmap	2.3
Net Crunch	2.9
SoftPerfect Network Scanner	2.3
Angry IP Scanner	13
Advanced Port Scanner	2.09

Table 2 shows the average scan time taken to complete the scan. Angry IP Scanner took 13 minutes for completing the scan as it probes 5000 ports to discover services on each active host. Other scanners took around 2 to 3 minutes for completing the scan.

TARGETED SERVICES BY SCANNING TOOL

Table 3. *Percentage Of Targeted Services Detected By Scanning Tool.*

Service	Nmap	NetCrunch	Soft Perfect Network Scanner	Angry IP Scanner	Advanced Port Scanner
http	66.67%	0%	100%	100%	0%
ms-wbt-server	100%	0%	100%	66.67%	100%
mysql	100%	0%	100%	100%	0%
microsoft-ds	100%	0%	0%	66.67%	100%
netbios-ssn	100%	0%	0%	66.67%	100%
msrpc	100%	0%	0%	66.67%	100%
upnp	66.67%	0%	0%	0%	0%
tcpwrapped	100%	0%	100%	100%	100%
Ping	100%	100%	100%	100%	100%
CIFS/SMB	0%	100%	0%	0%	0%

Table 3 shows the percentage of targeted services discovered by the network scanning tools. If number of services discovered by the scanner is more, then, the machine is more vulnerable.

It is observed that, Nmap discovered most of the targeted services and they were discovered in all the scans. Angry IP scanner discovered most of them but not as efficient as Nmap. SoftPerfect Network Scanner and Advanced Port Scanner discovered some of the targeted services and those services were discovered in all the scans. Net Crunch discovered only two targeted services and they were found in all the scans.

CONCLUSION

In this paper we studied few scanning tools and analyzed the results of the experiment performed to identify which among the scanning tools discovers more services. This result helps the system administrator to identify the breaches in the system and take an appropriate action.

REFERENCES

1. Nabanita Mandal and Sonali Jadhav, "A Survey on Network Security Tools

for Open Source", IEEE, 2016.
2. Sun-young Im, Seung-Hun-Shin, Ki Yeol Ryu, and Byeong-hee Roh, "Performance Evaluation of Network Scanning Tools with Operation of Firewall", IEEE, 2016.
3. Suriya Begum, Sujeeth Kumar, Ashhar, "A Comprehensive Study on Ethical Hacking", International Journal of Engineering Sciences and Research Technology, August 2016.
4. Ashiqur Rahman, Kantibhusan Roy Kawshik, Atik Ahmed Sourav, and Al-Amin Gaji, "Advanced Network Scanning", American Journal of Engineering Research, Volume-6, 2016.
5. Linda Markowsky and George Markowsky, "Scanning for Vulnerable Devices in the Internet of Things", IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, September 2015.
6. Rajwinder Kaur and Gurjot Singh, "Analysing Port Scanning Tools and Security Techniques", International Journal of Electrical Electronics and Computer Science Engineering Volume 1, October 2014.
7. Marco de Vivo, Le Ke, Germinal Isern, and GabrielaO. de Vivo, "A review of port scanning techniques", ACM SIGCOMM Computer Communication Rev., 29(2: 41-48), April 1999.
8. Nmap.org, "Nmap Network Scanning", 2011. [Online]. Available: https://nmap.org/book/toc.html. [Accessed: 28-Mar.-2018].
9. Soft Perfect Network Scanner, 2018. [Online]. Available: https://www.softperfect.com/products/networkscanner. [Accessed: 14-April.-2018]
10. NETCRUNCH 10, "Smart Monitoring for Modern IT", 2018. [Online]. Available: https://www.adremsoft.com. [Accessed: 28-Mar.-2018].
11. Angry IP Scanner, 2017. [Online]. Available: https://angryip.org. [Accessed: 28-Mar.-2018].
12. Advanced Port Scanner, 2018. [Online]. Available: https://www/advanced-port-scanner.com. [Accessed: 28-Mar.-2018].
13. Port Scanning Techniques, 2011. [Online]. Available: https://nmap.org/book/man-port-scanning-techniques.html. [Accessed: 16-Aug.-2017]