Network Monitoring Using Internet Protocol

Gowtham K K[1,] Krishnammal N[2], Anandhan P[3],Deepak S[4]
[1, 2, 3, 4] Dept of Computer Science
[1, 2, 3, 4] Sri Shakthi Institute of Engineering and Technology

Abstract- *The quick and rapid advancement of technologies such as Artificial Intelligence, Machine Learning , Software Application, Data Science etc. helps developers to develop high quality software applications .The standard or traditional way of data analyzing will not help anymore because the data generated daily is very enormous volume. There is also a need for Network Analysis , as they are related to each other. The networking tools started developing at that point and there is a need for each tools. It enhances the security of the application developed. There are large number of network based tools which used for different purposes by different people. The evolution of these tools are also the important cause for improving cyber security and quality assurance. Some of these tools are also used by ethical hackers to find a vulnerability in a particular server and exploit the particular vulnerability and hack the system. These tools are used for different purposes for networking such as website health monitoring using ping, port scanning, IP address tracking, resolving dns details of a website, getting domain information. This application provides more accuracy than the other tools. As it uses some advanced algorithms and methodologies. As like Internet Protocol tracker available in the market provides less location accuracy. This application gives atleast 20% more location accuracy than others with live map location .And also port scanner in this gives more accurate scanning of open ports and fast scanning option available to scan only the most important ports such as FTP, TELNET , HTTP etc.*

Keywords- Handshake Mechanism, Intenet Protocol, Ping Network , Port Scanning

I. INTRODUCTION

The contents of this paper mainly focus on android application for web and networking tools. The tools include Internet Protocol(IP) address tracker, IP logger, Domain Name Services(DNS) resolver, Domain Information, Phone Number Resolver, Website Screenshot, Cloud flare Resolver, Ping ,Port Scanner, Speed Test, HTML extractor, Website Headers Resolver, and Media Access Control address resolver. Each tools have its own functionalities and use cases. These tools are developed for network enthusiasts, network administrators, developers etc. Each tools are used for the unique purposes. An IP tracker records all IP addresses assigned by Internet Service Providers to personal and buisness purposes. So in a particular subnet, the ISP records the details of the IP address and assigned timestamp which is acquired by IP tracking systems. A port scanner is software tool which is used for scanning ports in a remote server or system. The port scanner helps to enhance security which is used by ITs network admins , developers by detecting open ports in the server or cloud system so that the port can be stopped accepting requests from insecure and unreliable sources .The ethical hackers use this to find the running open ports and services. Then they may inject a script to stop the particular service running. For example, if FTP port is open hacker can upload malicious file into the target server and exploit it. Port scanners is able to scan all the ports or popular ports or predefined ports. Scanning all the ports takes much time so scanning predefined ports are very useful and provide the necessary result faster. A port scanning tool can be used for different purposes based on the requirement.

1. All the running ports can be scanned against a particular local system or even a remote server
2. The most popular ports can be scanned which effictively reduces time of port scanning all the thousands of ports available
3. Also scans for open UDP ports
4. Scanning ports on multiple target machines at the same time
5. Scanning on most common ports
6. Scanning on particular ports with the input of port number

The port scanning is developed to help SecOps developer in enhancing security of the system. But ethical hackers use the port scanner tool to find the open ports and services running of a remote server, which is basic step of fingerpring a server and exploiting it. For example, if an open port is found out by the hacker, hacker can using this vulnerability and exploit the server. These networking tools helps network administrators to monitor server and find vulnerabilities in the system.

II. METHODOLOGY

Each tools works on different methodology.IP address trackers gathers the data they need such as isp details from network information centres who is api and record any further movements. A port scanner helps to scan a server or host for open ports(Ranges from 0 to 1023). The internet speed test works in a methodology where when the test is started, first ping is executed between the client and server. Then for download test a small piece of file is downloaded from the test server. Vice versa, the upload test is done by uploading a small piece of file. The bandwidth and speed is measured by calculating the difference in timings and the small file size.

2.1 Ip Tracker

An IP(Internet Protocol) address is a decimal representation of numbers based on several rules,which is helpful for uniquely identifying a device in the local network and also identification of router in public internet. There are two cases of IP address. One is private IP address. This address is used to find the particular device in the same network. This private IP is handled by the router. The another one is public IP. The devices connected to the same network has same public IP address. This IP address helps in communication between two computers in local network and also the internet.

2.2 How Ip Works

How IP works. Internet Protocol is designed to work over both static and dynamic network. So it works without the requirement of central repository of IP address logs. Internet protocol is based on datagram protocol which states that it may be connectionless. So every communication through the internet requires source IP address and destination IP address to transfer data packets between them. So this ensures that the message is succesfully delivered from sorce to destination where the acknowledgement will be sent to source to notify sorce that the data is received successfully.

2.3 IP handshake

Every time when a computing device is connected to a web server or another network or other devices in the internet, there is requirement to provide the IP address of the source with the data with header information .It ensures that the data is transferred between the source and destination. The destination also acknowledge the sorce with the IP address and acknowledgment message .So the communication between devices in the intenet in not at all possible. The communication between two devices in intenet requires both sorce and destinaion IP addresses to be public, transeferring their IP address to each other. This is process where the ISP logs every data transimission between client and server and IP tracker gets the data for tracking the Ip address. This IP address are assigned by Internet Service Provider. It ensures to avoid duplication IP address assigned to particular users.

2.4 Port Scanner

A port in a computer is network socket point through which the data flows from a particular program on one computer or to another computer from the Internet or another computer in the same network to the same program. The simple example is for file transfer the FTP port of one computer communicates with FTP port of another computer with the help of port number assigned to the particular port.Port numbers are numbered according to some standards for using it more efficiently and use them as a standard. Every ports available from 0 to 1023 is used for unique services in the internet such as SMTP service, telnet, http, https, ftp, IMAP etc..The port scanner in our system can scan in faster manner than the other port scanner. Our port scanning system is based nmap scannning system.

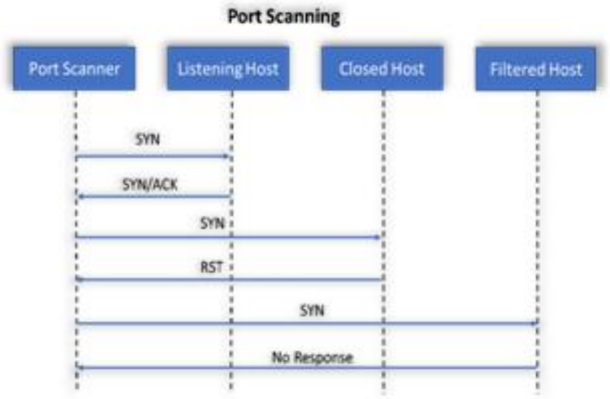
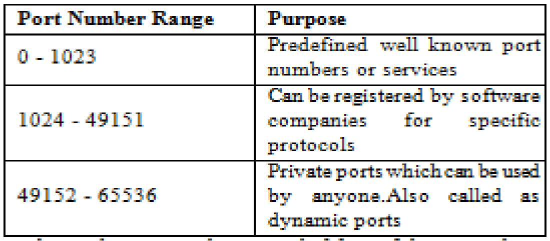


Fig. 1. Port Scanner

The scanning of most commonly used ports is used mostly. Our system also cahces the result of the scan in the server . So for continuous scan instead of scanning the host again it just sends the cached result at a quicker manner.The port scanner nowadays is mostly used by ethical hackers to get the details of the targeting web server and if they find any vulnerable ports they exploit the server using the vulnerable port. This is the reason the open ports are very dangerous to server computers connected in internet.

TABLE I Port Range Groups



Port Number Range	Purpose
0 - 1023	Predefined well known port numbers or services
1024 - 49151	Can be registered by software companies for specific protocols
49152 - 65536	Private ports which can be used by anyone.Also called as dynamic ports

2.5 Port Sweeping

Port sweeping is an advanced method of port scanning of a host. Our port scanning system is helpful for scanning of all ports of a particular host.The port sweeper is able to scan all the open ports in the whole subnet but it takes lot of time to scan because scanning all the Ip address in a subnet for all ports are done in a sequential manner to avoid large traffic on host.

2.6 A Serious Threat

The open ports are always dangerous to any web sevrer.This is also leads to loss of confidential data in the particular web server. The hackers can also use this vulnerability and inject a virus script through open port and it leads to compromising of data to the zhackers. So it is a serious security threat to any websites. So this must be montinored every time. The serious threat is the the server does not logs the IP address of the hacker who scanned the particular host for open port and so it will be difficult to track if the webserver is exploited the hacker. If a new security risk is found it should be solved as soon as possible to avoid any exploits done by the hacker.

2.7 Firewall Protection

The webserver can be stopped blocked for port scanning and port sweeping by configuring the system with the firewall. It acts as an extra layer of security of computer in the intenet. It is used by ISP ,so the data transfer between two devices are made in a more secure manner.So if configured with firewall, even though hacker tries to scan the port he will receive the error message. But sometimes the hacker may use individual scan to get the open port data,which will be difficult to stop. The one of the technique to avoid port scanning is by openning all the available ports at the same time and due to long scanning time required ,the empty result is sent to the hacker.

III. RESULTS AND DISCUSSION

All the computer network based systems may seem to be simple to implement. But the reality is network monitoring tools required more performance than feature.The building of networking system may not seem that much difficult but building a high efficient and fast networking system is required. To put in briefly, these network monitoring tools will be used be used by network administrators, network engineers, networking enthusiasts , developers etc.. to build high quality products.So it is required that the system should be more efficient and effective. So the network administrators can be easily monitor the network. Most of the networking systems are mostly Command Line Interface(CLI) based tools. So it requires some knowledge on using commands . But our network monitoring system is a Graphical User Interface(GUI) based tool so anyone without much networking experience can easily use the app. Each modules in the application are explained clearly. Some of the third party APIs are integrated and also Google Maps is integrating for seeing the live location on the tracked IP address of the user. All the major issues in network monitoring systems are explained in detail in this project. This is a very easy to use system.

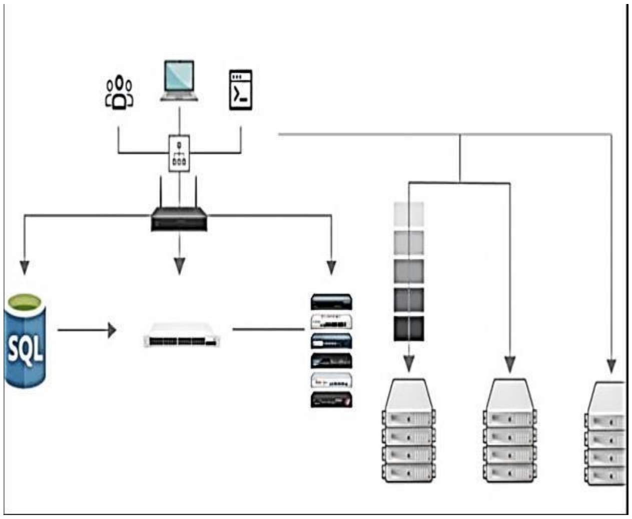
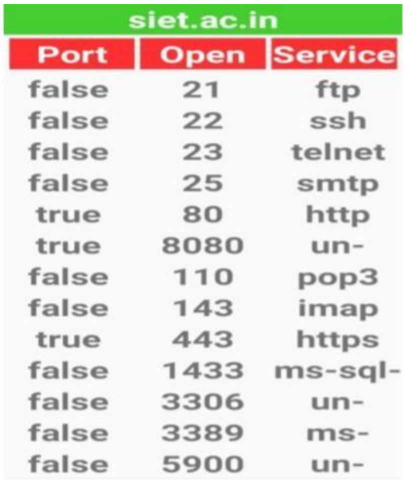


Fig. 2. **Computer Network**

The main objective is to develop a more feasible network tool that will be available in handy mobile devices. As this does not require any special authentication and so the system was entirely tested and proven to be most feasible than other network based tools. So it is required to do some work to find best tool for the user requirement. But our system contains more than thirteen networking tools and will be developed further. Some object were changes during the development process and others took longer than expected to finish , but the all the modules in project works perfectly with more accurate and more efficient than any other network based tools which makes the project a success. The methodology and algorithms will be constantly evolving and based on that our system will be improved by developing more modules based on the new networking based tool requirement.In the end, the product described in this document is a working system that we developed. This system will help network administrators , developers to do their work efficiently and accurately.



siet.ac.in

Port	Open	Service
false	21	ftp
false	22	ssh
false	23	telnet
false	25	smtp
true	80	http
true	8080	un-
false	110	pop3
false	143	imap
true	443	https
false	1433	ms-sql-
false	3306	un-
false	3389	ms-
false	5900	un-

Fig. 3. **Port Scanner Result**

IV. FUTURE SCOPE

The system can be updated and optimized for providing most accurate results than any other tools. The tools like packet level capturing of data through the network can be devloped based on wireshark packet capturing tool or VPN based packet capturing tool. The port scanner will be optimized for scanning the ports more quicker and improcing cahing mechnism by setting expiry time, session id and cookies. Vulnerability detection system will be added such as Cross site scripting detection ,SQL injection detection and some other vunerability detection.system will be improved by developing more modules based on the new networking based tool requirement. In the end, the product described in this document is a working system that we developed. This system will help network administrators , developers to do their work efficiently and accurately.

V. CONCLUSION

Thus this application helps network administrators to monitor health of web server using ping tool, finding vulnerable ports using port scanner, and helps penetration testers to footprint a website by resolving the DNS ,getting the domain information, checking whether it is protected by the Cloudflare network and tracking the IP address of the website to get the location of the server. While the Network Monitoring System is a small cog in the monitoring game it is a complex and versatile cog. It is important to remember that while the Network monitoing system can provide a lot of information and data you must also consider the Legal, Ethical, and Social issues that can arise when implementing the Network monitoing system.

REFERENCES

[1] James F. Kurose, Keith W. Ross, “Computer Networking – A Top-Down Approach Featuring the Internet”, Fifth Edition, Pearson Education, 2009.

[2] Nader. F. Mir, “Computer and Communication Networks”, Pearson Prentice Hall Publishers, 2010.

[3] Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, “Computer Networks: An Open Source Approach”, Mc Graw Hill Publisher, 2011.

[4] Behrouz A. Forouzan, “Data communication and Networking”, Fourth Edition, Tata McGraw – Hill, 2011.

[5] Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Fifth Edition, Morgan Kaufmann Publishers, 2011.

[6] Jay Beale, Renaud Deraison, Haroon Meer, Roel of Temmingh, and Charl Van Der Walt. Service detection. In Nessus Network Auditing, page 248. Syngress Publishing, 2004.

[7] Nagios. The Industry Standard In IT Infrastructure Monitoring. http://www.nagios.org. Accessed June 3, 2015

[8] Information Sciences Institute, University of Southern California. Internet protocol. RFC 791, RFC Editor, http://www.ietf.org/rfc/rfc791.txt,September 1981