Capturing, Monitoring and Visualizing the packets in a Network

Anshuman Agarwal, Aditya Varshney, Arnav Bansal

Abstract—This paper presents a new and a modern methodology to build a tool for an in-depth analysis of all the packets flowing through a computer network. We use modern technologies like pyshark and tshark to capture the packets from the device.

Index Terms—packet sniffer, packet capture, network sniffing, tshark, network monitor

1 INTRODUCTION

THERE is a rapid development in computer network technology in this internet era, people are getting more and more network resources and services day by day. This has significantly increased network traffic; along with increasing number of packets of network services, websites and servers are more prone to network vulnerabilities causing unexpected behavior to some services resulting in user's displeasure. Therefore, efficient and more importantly automatic network monitoring has become a need for a website to work properly. Addressing this key issue in network management, network administrators should have the capability to analyze statistical information of network traffic and intrusion detection for improving security measures and maintaining user's privacy. Monitoring network packets can help them understand their visitors better and hence improve their content based on this data and contribute to better use of the network. There are two ways to monitor networks: (1) packet sniffing, capturing all the network packets, analyzing the data and providing statistical conclusions. (2) log analysis technology, analyzing the logs from built-in firewall combing gateway devices.

Packet sniffing is basically a technique of sniffing data belonging to other users on the network. Packet sniffers are utilities that can be efficiently used for network administration. At the same time, it can also be used for nefarious activities.

Packet sniffing requires technical skills and resources which might not be available to all users. Hence we propose a user friendly implementation of a network monitoring and analysis software. Our proposed idea captures packets flowing through a network and provides deep insights such as type of protocol being used, number of packets being sent, source ip address, destination ip address, type of request and also details about the various layers inside the packet.

2 LITERATURE REVIEW/ RELATED WORK

Monitoring of networks is not a new field of research, there are many good tools both free and paid available on the internet which can be customized according to the needs of a website. "The network system monitoring software market is so packed full of tools that it can be difficult to choose", says Tim Keary in his article titled as 10 Best Network Monitoring Tools & Software of 2020 [12]. In his brief study he includes a list of free, paid and open source software for windows, Mac, and Linux. Going by that article *SolarWinds* Network Performance Monitor' [13] seems to be the choice. SolarWinds is a top-tier producer of IT management software. NPM (Network Performance Monitor) is one of its key products. The NPM comes with a dashboard, it has comprehensive controls that can be customized according to your network data and also filter the events reported by the system. This is a very flexible system that is suitable for any size of network. Many other monitoring tools are available like PAESSLER, the choice of tool depends on needs, PRTG Network Monitor is worth taking a look at if you need less than 100 sensors.

Article An Efficient Network Monitoring and Management System [15] presents a network monitoring scheme which uses the smart interaction of Request Tracker (RT) and Nagios software to obtain an intelligent and automatic network monitoring system. The role of networking is performed by nagios software. RT is greatly used globally and is customizable and configurable according to the organization needs.

A lot of work has been done on packet sniffing for LAN or WAN monitoring [16]. There are again many tools available for network monitoring but comparing them is not the objective of this paper. Briefly, Wireshark is used for network troubleshooting, analysis but it does not provide any intrusion detection [17]. Tcpdump, a common packet analyzer uses command line programming allowing users to capture and display TCP/IP and other packets being transmitted or received over a network.

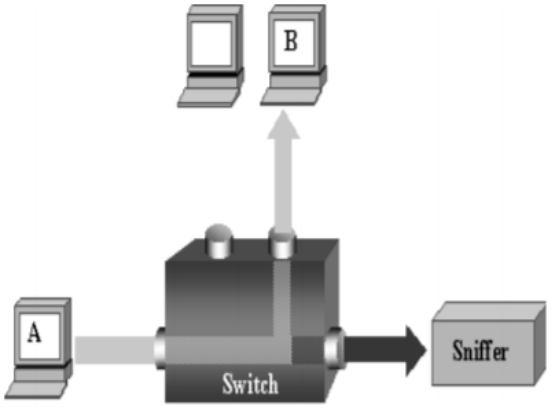
3 DATA RESOURCES

We monitor, capture and analyze live packets flowing through the network.we capture packets using a python module called pyShark. It processes the packets and provides us with all the insights of each packet. Through our platform we do an in-depth analysis and display our findings via informative graphs and a user-friendly environment.The technologies we have used to develop our monitoring system are Flask, HTML, CSS, tshark and pyshark.

4 METHODOLOGIES

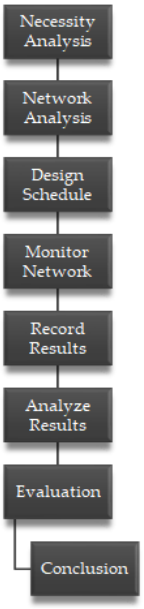
We have developed a web application which provides a user friendly environment to monitor the live packets. The packets are captured using tshark and pyShark modules. pyShark sends the packet data to a custom built flask server which interacts with a SQLite Database. the captured data is stored in this database. This stored data is then used as inputs to various charts such as to display the various sizes of packets and types of protocols . We look at the various layers the packet consists of such as IP layer, TCP/IP Layer.

Through packet sniffing, the information transmitted across networks can be captured. Network administrator, using packet sniffing in network management can analyze networks easily to monitor and troubleshoot network traffic. When a packet transfers from source to destination, it passes through several intermediate devices. A node whose NIC (Network Interface Card) is set in the promiscuous mode which receives all information travelling in the network. The physical address of every NIC is different from another and network. A packet arriving at NIC is copied to driver memory and then it is passed to the kernel and the kernel passes it to user application [18].



NDLC (Network Development Life Cycle) is a process approach in the field of data communication describing a cycle which has no beginning and end in observing the network. It has following stages;

1. Analyze the need to conduct research, focus on existing problems and network analysis.
2. Design a schedule to monitor the network on a specific time scale.
3. Monitor the network, implementation and analysis, capture and record the results.
4. Analyse results by focusing on information you need.
5. Evaluation of result monitoring management advice and conclusion.



5 RESULTS

Main goal of any monitoring system is to improve performance and security.

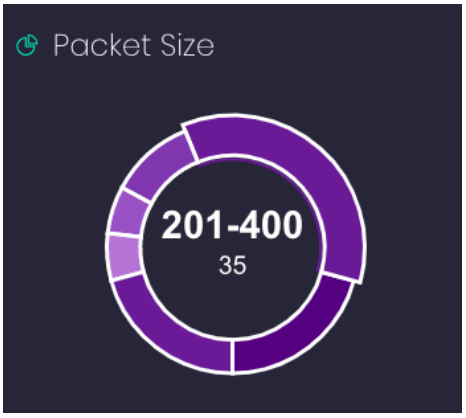
Network Monitoring refers to a system that is capable of monitoring the whole network topology continuously for jamming, slowing down or component failure, it includes notifying network responsible persons, normally the network administrator in case of any problem. Network monitoring is usually associated with the functions involved in network management. Management of the network is required to ensure that network is up and running [15]. For this paper, we were just focused on packet sniffing, a part of network monitoring which sniffs data belonging to other users on the network. Packet sniffers are utilities that can be efficiently used for network administration. At the same time, it can also be used for nefarious activities.

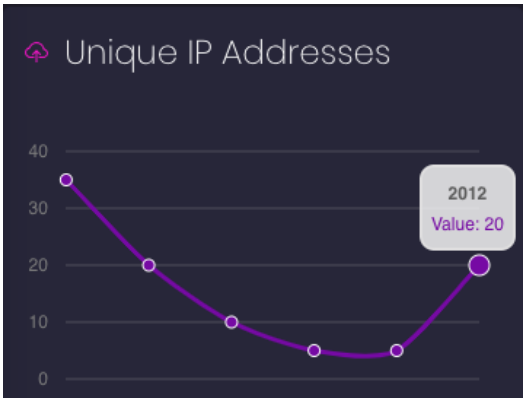
6 PERFORMANCE EVALUATION/ VALIDATION

This hypothesis has been validated and actuated into an actual product using the technologies mentioned. Herein is a figure depicting the actual frontend of the prototype built.

7 CONCLUSION

Computers transmitting packets over networks normally just see the traffic specific to them. Although network cards (NICs) have the power to listen to all network traffic by entering the promiscuous mode, this gives them the ability to see the whole all the packets in the network whether it is directed to or from them. Packet sniffing is basically used by hackers but more importantly it can be used for network traffic analysis, packet analysis,

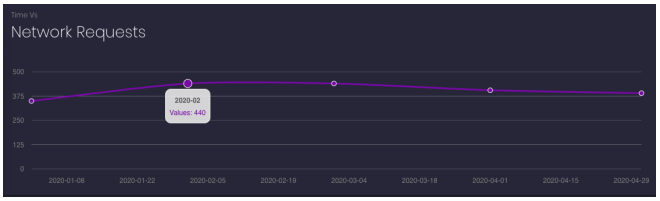


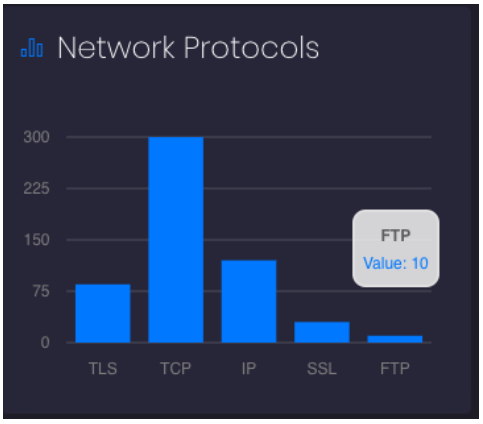


troubleshooting and other useful purposes. A Packet sniffer is designed to capture packets information. Packet sniffing is a very controversial subject, people having malicious intentions take advantage of it to 'sniff' out your password. These so called hackers invade your privacy by getting your personal information.. Sniffing can be done on both switched and non switched networks. Many organizations are not at all aware of the threat of sniffing packets by hackers, various tools can and should be used to capture this network traffic for intrusion detection.

8 ACKNOWLEDGMENTS

This work was part of our End Term Examination for Computer Networks Course. We would like to thank Dr. Kuldeep Chaurasia and Dr. Vijay Kumar Bohat for their continuous guidance and expertise in the subject and giving us motivation and perseverance to write the





research article.

REFERENCES

[1] A. Gupta, R. Birkner, M. Canini, N. Feamster, C. MacStoker, and W. Willinger, Network monitoring as a streaming analytics problem, in Proceedings of the 15th ACM Workshop on Hot Topics in Networks, Atlanta, USA, 2016, pp. 106-112

[2] N. I. Visual, Forecast and methodology, 2016-2021, white paper, San Jose, CA, USA: Cisco, 2016.

[3] Y. Lee, W. Kang, and H. Son, An internet traffic analysis method with mapreduce, in Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, Osaka, Japan, 2010, pp. 357-361.

[4] C. Sanders, Practical Analysis Using Wireshark to Solve RealWorld Network Problems, 2nd ed., W. Pollock, USA, 2007.

[5] Nedhal A. Ben-Eid,"Ethical Network Monitoring Using Wireshark and Colasoft Capsa as Sniffing Tools",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015

[6] W. B. Pottner, L. Wolf, "IEEE 802.15.4 Packet Analysis with Wireshark and off-the-Shelf Hardware", in Proc. SICNSS, 2010.

[7] P. Asrodia, H. Patel, "Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis", in IJEECE, 2012, paper 2277- 2626, p. 55-58

[8] T. Dean, Network+ Guide to Networks, 6 th ed., D. Garza, S. Helba, Nelson Education, Canada, 2013.

[9] A. Orebaugh, Wireshark and Ethereal: Network Protocol Analyzer Toolkit, A. Williams, Canada, Syngress, 2007

[10] Vanparia, Pradip & Ghodasara, Yogesh & Donga, Mr. (2015). Network Protocol Analyzer with Wireshark. developeriq.in.

[11] K. Hassan, A. Ahsan, and M. Rahman, "IEEE 802.11b Packet Analysis to Improve Network Performance", in JUJIT, 2012, Vol.1, p. 27-34.

[12] Tim Keary, *10 Best Network Monitoring Tools & Software of 2020*, June 6, 2020 (Comparative Study)

[13] Stephen Cooper, SolarWinds Network Performance Monitor (NPM) Review, December 19, 2018 (@VPN_News)

[14] Khan, R., Khan, S. U., Zaheer, R., & Babar, M. I. (2013). *An Efficient Network Monitoring and Management System*, (International Journal of Information and Electronics Engineering), 3(1), 122-126. https://doi.org/10.7763/IJIEE.2013.V3.280

[15] X. Jiang and F. Peng, “Network Management Capability Model and its Application of Self-Management Capability Analysis,” in International Symposium on Computer Network and Multimedia Technology, CNMT-09, Wuhan, China, January 2010.

[16] S. Ansari, Rajeev S.G. and Chandrasekhar H.S, “Packet Sniffing: A Brief Introduction”, IEEE Potentials, Dec 2002- Jan 2003, Volume: 21 Issue: 5, pp: 17 – 19

[17] A. Dabir, A. Matrawy, “Bottleneck Analysis of Traffic Monitoring Using Wireshark”, 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov 2007, Page(s):158 – 162

[18] Liqiang Zhang, Huanguo Zhang “An Introduction to Data Capturing” International Symposium on Electronic Commerce and Security.

[19] Daniel Magers “Packet Sniffing: An Integral Part of Network Defense”, May 09, 2002 SANS Institute 2000 – 2002.