Network Traffic Analysis Using Packet Sniffer With Intrusion Prevention System

Renisha A[1], Yogeshwari I[2], Babu M[3]
[1, 2, 3] GKM college of engineering & technology

Abstract- *Traffic analysis using the internet is an activity to record data from user activities in using the Internet. Since user activity is more dominant in finding and downloading sites on the Internet. The method used to get the results of the study is the packet sniffing method. We can filter data packets from the http protocol application. Thus the intrusions through the firewall is being obtained and the IDS alerts the system after the implementation of Intrusion prevention system. This paper focuses on the basics of packet sniffer and its working, development of the tool on Linux platform and its use for Intrusion Detection. Hence the demonstration over particular LAN is performed and prevention system is built around the host.*

Keywords- Network analysis, Packet sniffing, Intrusion detection, Intrusion prevention.

I. INTRODUCTION

Network monitoring software can analyze performance in real-time, meaning that if a failure or issue is detected, you can be immediately alerted. It eliminates the need for a physical system administrator and manual checks. A subspace method usually applied to the flow traffic is used to count the number of feature occurrences for features such as number of packets, byte count of multivariate time series etc. For most organizations packet sniffer is largely an internal threat. Packet sniffers can be operated in both switched and non switched environment. Reports can help you identify patterns and trends in system performance, as well as demonstrating the need for upgrades or replacements.IDS ensures quick and effective detection of known anomalies with a low risk of raising false alarms. It analyzes different types of attacks, identifies patterns of malicious content and help the administrators to tune, organize and implement effective controls.

II. LITERATURE REVIEW

In this study to obtain optimal output research, literature review conducted related previous studies, so that it can be used as a reference in research. There are several research studies that have been carried out by previous researchers, such as [1], they discussed packet analysis and network traffic monitoring over TCP protocol used Wireshark packet sniffer.

A. NETWORK

Networking comprises not only the design, construction and use of a network, but also the management, maintenance and operation of the network infrastructure, software and policies. Computers that are connected—either by cables (wired) or WiFi (wireless)—with the purpose of transmitting, exchanging, or sharing data and resources. Local area network (LAN) consists of a series of computers linked together to form a network in a circumscribed location. Networks enable communication for every business, entertainment, and research purpose. The internet, online search, email, audio and video sharing, online commerce, live-streaming, and social networks all exist because of computer networks.

B. WIRESHARK

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

C. INTRUSION DETECTION

An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system.

Signature-based: Signature-based IDS detects possible threats by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from antivirus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.

Anomaly-based: a newer technology designed to detect and adapt to unknown attacks, primarily due to the explosion of malware. This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behavior against this trust model. While this approach enables the detection of previously unknown attacks, it can suffer from false positives: previously unknown legitimate activity can accidentally be classified as malicious.

III. RESEARCH METHODOLOGY

In the proposed system, The connected networks of system in a small geographical area is kept as a target region where the network traffic monitoring and analysis is being performed.: Focus has also been laid to analyze the bottleneck scenario arising in the network, using this developed packet sniffer. The proposed approach also detects the intrusions and a system is built to prevent those intrusion.

Packet Sniffing :

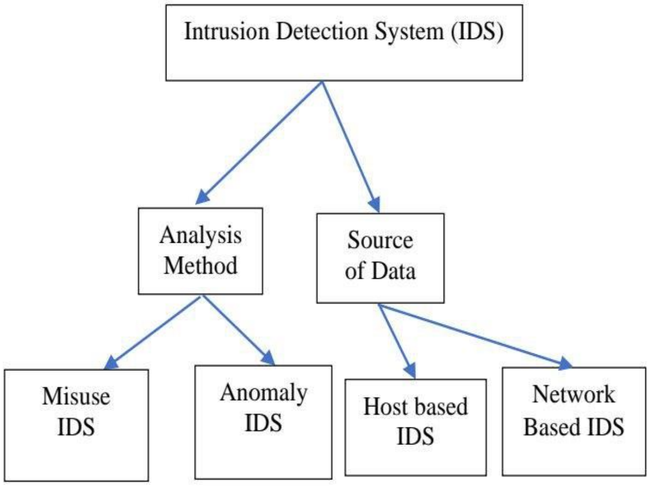
Packet sniffing is tools that are used as monitoring data packet when a packet crosses a network. There are packet sniffing in the form of software, but there are also hardware based devices that are installed directly along the network. Sniffer can handle data sent specifically to them. Sniffer can be used legally on the network by system administrators to monitor and solve traffic problems in their own networks. For example, if a computer has a communication problem with another computer, a administrators can view packet from one machine to another and determine the cause of the problem.

The packet sniffer consists of the following components:

1. **Hardware** : standard network adapters .
2.**Capture Filter** : This is the most important part . It captures the network traffic from the wire, filters it for the particular traffic you want, then stores the data in a buffer.
3. **Buffers :** used to store the frames captured by the capture filter.
4. Real-time analyzer: a module in the packet sniffer program used for traffic analysis and to shift the traffic for intrusion detection.
5. Decoder : Protocol Analysis.

Intrusion prevention:

The threats that enterprise security systems face are growing ever more numerous and sophisticated. The automated capabilities of an IPS are vital in this situation, allowing an enterprise to respond to threats quickly without placing a strain on IT teams. As part of an enterprise's security infrastructure, an IPS is a crucial way to help prevent some of the most serious and sophisticated attacks.IDS based on anomaly detection model can detect symptoms of attacks without specifying model of attacks, but their drawback is that they are very sensitive to false alarms. This should be avoided. Intrusion detection system sits between a set of networked users and firewall and router which connects the users with the outside world through Internet. IDS detect anomaly activities and prevents from attacks from unauthorized or unauthenticated persons.



The checked PC framework can be spoken to as the progress outline of a state that is a realistic portrayal of an intruder's actions to compromise the framework. An interruption is seen as a request for action by an intruder that leads to an objective compromised state from a single state on a PC framework. State progress exam charts perceive the preconditions and off - state trading of the entry. They also list the key actions that need to take place to complete an attack effectively.

IV. CONCLUSION

This intrusion detection system can be enhanced in future by incorporating features like packet sniffer program platform independent, adding report network statistics, intrusion detections integration. However, a user can employ a number of techniques to detection and sniffing on the network as discussed in this paper and protect the data from being sniffed.

REFERENCES

[1] G. Varghese, “Network Algorithmic: An Interdisciplinary Approach toDesigning Fast Networked Devices”, San Francisco, CA: Morgan Kaufmann, 2005.

[2] J. Cleary, S. Donnelly, I. Graham, "Design Principles for Accurate Passive Measurement," in Proc. PAM 2000 Passive and Active Measurement Workshop (Apr. 2000).

[3] 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

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

[5] Daiji Sanai, “Detection of Promiscuous Nodes Using ARP Packet”, http://www.securityfriday.com/

[6] Ryan Spangler , Packet Sniffer Detection with AntiSniff, University of Wisconsin – Whitewater, Department of Computer and Network Administration, May 2003

[7] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, “Malicious Sniffing System Detection Platform”, Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT’04), IEEE Computer Society

[8] Hornig, C., “A Standard for the Transmission of IP Data grams overEthernet Networks”, RFC-894, Symbolic Cambridge Research Center, April 1984.

[9] Wei Wang; Gombault, S.; Guyet, T., "Towards Fast Detecting Intrusions: Using Key Attributes of Network Traffic", Internet
Monitoring and Protection, 2008. ICIMP '08. The Third International Conference on Digital Object Identifier: 10.11 09IICIMP.2008.13 Publication Year: 2008.

[10] Yang Li, Bin-Xing Fang, You Chen, Li Guo, "A LightweightIntrusion Detection Model Based onFeature Selection and Maximum Entropy", Model Communication Technology, 2006. ICCT 06. International Conference on Digital Object Identifier: 10.1 I 09IICCT.2006.341 771 Publication Year: 2006 , Page(s): I - 4.

[11] Panda, Mrutyunjaya; Patra, Manas Ranjan, "Some ClusteringAlgorithms to Enhance the Performance of the Network IntrusionDetection System", Journal of Theoretical & Applied Information Technology;2008, Vol. 4 Issue 8, p7IO

[12] Komviriyavut, T.; Sangkatsanee, P.; Wattanapongsakorn, N. ;Charnsripinyo, C.; "Network intrusion detection and classification with Decision Tree and rule based approaches", Communications and Infonnation Technology, 2009. ISClT 2009. 9th International Symposium on DigitalObjectIdentifier:IO.Il09/ISCIT.2009.534I005 Publication Year: 2009 , Page(s): 1046 - 1050.

[13] Quang Anh Tran; Jiang, F.; Jiankun Hu; "A Real-Time NetFlowbased Intrusion Detection System with Improved BBNN and HighFrequency Field Programmable Gate Arrays", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on Digital Object Identifier:10.1109/TrustCom.2012.51 Publication Year: 2012 , Page(s): 201- 208.

[14] Winpcap library. Available from, http://www.winpcap.org.

[15] Risso, F. ; Degioanni, L.; "An architecture for high perfonnance network analysis" Computers and Communications, 2001.Proceedings. Sixth IEEE Symposium on Digital Object Identifier: 10.1109IISCC.2001.935450 Publication Year: 2001, Page(s): 686 693