ISSN:0975-9646

NIDS Designed Using Two Stages Monitoring

Rahul B. Adhao, Avinash R. Kshirsagar,Dr. Vinod K. Pachghare

Department of Computer Engineering and IT
College of Engineering Pune
Shivajinagar Pune, India.

***Abstract*—Introduction of high speed network technologies like 3G and 4G and ever increasing network users are giving rise to increased traffic at Network Intrusion Detection System (NIDS). In old NIDS, each captured packet is inspected using database to detect intrusion. But this is not suitable for today`s increased traffic. The new concept of flow inspection, is suffering from scarcity of data. So by combining both inspection methods i.e. flow and packet, two stages monitoring NIDS can be designed which is explained in this paper**

Keywords—Network Intrusion Detection System, IP flow , Netflow, Packet Inspection.

I. INTRODUCTION

The ongoing research in network technology causes wireless network to be seen everywhere and day by day the speed with which it can be accessed has increased. Along with laptop and Desktop computers, one can access this network even with his hand held devices like PDAs, cell phones at same speed. But introduction of such new technology along with a variety of user friendly applications has resulted in fluctuation of volume and types of traffic in the network. Though the network speed has increased, the security of such networks continues to be a thing of concern. To deal with such speedy network, packet based approach of NIDS can never be suited. So there is need for faster security approach.

In this paper, we are interested in emphasizing how two stage monitoring NIDS better suits for today's high speed network.

II. INTRUSION DETECTION SYSTEM

The rapid expansion of computer network has changed the prospect of network security. Unfortunately the risk and chances of malicious intrusion still continues [1]. An intrusion can be defined as the act of gaining unauthorized access to a system so as to cause loss or harm. So IDS`s are becoming integral part of network monitoring. According to Krugel et al. [2], "intrusion detection is the process of identifying and responding to malicious activity targeted at computing and network resources". So IDS does not usually takes preventive measures when attack is detected, it is reactive rather than proactive agent.

An Intrusion detection system (IDS) is a tool (software or hardware or both) designed to discover undesirable attempts at having access to, manipulating, and/or disabling of systems. It additionally watches for attack that originates from inside network system [4]. An IDS supplies similar functionality as burglar alarm devices put in houses.

IDS Classification:

IDS can be classified in various ways based on various parameters like types of data processing, the type of analysis or the source of the data. However we can classify IDS into two widely known classifications, signature versus anomaly-based and host versus network-based [1].

Signature-based intrusion detection works by identifying specific pattern of events or behaviors that accompany an attack. Each such pattern is called a signature. A signature-based IDS maintains a database of known signatures. It attempts to obtain match between the currently observed behavior of the system and an entry in this database. A real world signature based IDS will have thousands of attack signatures against which to compare. An example of an attack signature is a specific bit sequence in a worm payload. Anomaly based IDS involves making a determination whether the behavior of the system is statistically significant departure from normal. The IDS will have to learn, over time, what constitute normal activity, usage and behavior. Moreover, the definition of what is normal may vary as a function of the time of the day or the day of week. What is normal may also vary from one host to another [3].

In Host based system, the IDS examines at the activity of on each individual computer or host. It is designed to run as software on host computer system. Its main job is to monitor the internal behavior of the host such as the sequence of system calls made, the file accessed etc. For this purpose, its make use of system log, application logs, and operating system audit trails to identify events related to an intrusion. In a network based system the individual packets flowing through a network are monitored and report on all network traffic. The NIDS can detect malicious packets that are designed to be firewall`s simplistic filtering rules [4].

Desirable features of IDS

The two desirable features of IDS are Speed and Accuracy [3].

- **Speed**: Speed is especially important in fast spreading Internet worms, for example. Early worm detection and early response mechanism such as automated system shutdown can help reduce the number of

infected machines.IDS should be able to detect every instance of an intrusion.

- **Accuracy**: The two aspect of accuracy are sensitivity and selectivity- high sensitivity implies a low false negative rate, while high selectivity implies a low false positive.

III. IP FLOWS (CISCO NETFLOW)

Capturing IP flows have many significant benefits hence today`s all vendor provides their routers with flow monitoring measuring facilities. IP flow is captured and stored in flow records which can be used for traffic characterization [5]. It also helps IDS for purpose of intrusion detection which is topic of our paper.

The definition of IP flow given by IPFIX (IP Flow Information Export) is

"A flow is defined as a set of an IP packets passing through an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties".

According to IPFIX documentation, a flow is identified by parameters like source and destination addresses, source and destination port numbers and IP protocols:

(ip_src, ip_dst, port-src, port_dst, proto)

These elements are called as flow keys or common properties. These flow keys are very important for getting behavior of network like:

- Source address gives who are producer of traffic
- Destination address gives who are consumer of traffic
- Port address gives application using these traffic
- Protocol gives which Layer 3 protocol is used for transporting IP packets.
- Matched packets and bytes gives total traffic in network.

Change in network behavior is reflected by above flow keys, so from security perspective it is necessary to monitor packets flowing in network [6].

The monitoring of network can be Active or Passive. In case of active, artificial traffic is injected to get reaction of network. Parameter like Round Trip Time (RTT) and one way delay measurement plays important role in active monitoring. The passive monitoring uses actual traffic passing through observation point. This uses Management Information Base (MIB) of Simple Network Management Protocol (SNMP) or by exporting flow information [7]. Exporting flow information system helps in characterization of traffic from users and applications, analyzing traffic pattern, performance monitoring etc which are not provided by MIB-SNMP system.

Architecture of IP Flow

A Metering Process is responsible for collecting packets at an Observation Points, filtering them out (optionally) and aggregating information about these packets. An Exporter sends this information to a Collector using the IPFIX protocol as shown in following figure [8].

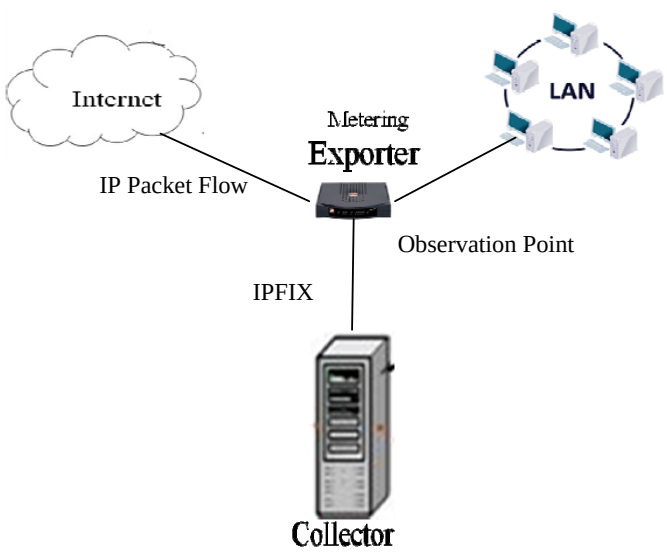

Figure 1 Architecture of IP Flow [8]

IV. NIDS DESIGNED USING PACKET-BASED APPROACH

As stated above in IP flow, each packet is captured at observation point and necessary information is extracted to get behavior of network. This is done through Deep Packet Inspection associated with mirror port (monitoring port) of observation point (Switch / Router) [9].

For each packet following operation need to be performed:

- Capture every packet in network traffic
- Each packet is time stamped (with nanosecond precision)
- Read the flow keys in the packet
- Duplicating and Filtering
- Processing
- Storing to Disk

In case of NIDS designed using packet based approach, header and payload of each incoming packet is checked for detecting intrusion. Packet-based approach is mostly suited for Misuse/Signature detection method. In case of signature, data from each packet is compared with entire signature database. Without disturbing this procedure, the database is continuously updated [4]. So day by day database size is growing to be increased so number of comparison also goes on increasing, which result in time and resources consumption. So NIDS performance degraded. Also it detects only previously known attack, it cannot detect unknown attack since it does not match with predefined and already known signature.

In case of high speed network number of packets captured at an observation point is much more; e.g. a link running with full saturation of 1 Gbps produces traffic of 6 Terabytes in a single day [10]. So NIDS running at such

network need to be fast to handle such large number of packets (Speed). Loss of packets may result in entry of intrusion in network (Accuracy) that is supposed to be catch by NIDS. As already stated for any IDS desirable features are Speed and Accuracy, which is not guaranteed in this case. Thus for high speed network packet based approach is not good options.

So it is clear from above discussion, there is difference in speed of packet capturing tool and packet analyzing application and is very hard to bridge. As network`s bandwidth is doubled after every six months; To deal with such ever increasing network speed there need of technique for monitoring and analyzing network traffic at high speed with accuracy.

V. NIDS DESIGNED USING FLOW BASED APPROACH

The Nowadays we are aware of how computer network are being used widely as a mean of communications. Along with this, this network can be accessed by using hand held devices like PDA`s, android cell phones. There is also introduction of high speed network technology like 3G and 4G. There is also increase in network user day by day, this all results in increase in network traffic across network. So packet analyzing to be very fast to cope up such huge traffic, otherwise there could be chance of losing packet. In such case our NIDS will be such decorative thing. To deal with all this issue better approach is to focus on flow rather than individual packets. As stated in flow concept that the changes in flow keys can be used for traffic analysis and security purposes i.e. detecting attack [11]. Anna Sperotto and Aiko Pras have shown in their dissertation digest how flow can be used to detect attack like DoS, Botnets, Scan and worm [6].

Actually flow offers aggregated view of network traffic by inspecting group of packets flowing in network. So drastically reduces amount of data need to compared. The flow monitoring process consists of two steps flow exporting and flow collection. After packet is captured by flow exporter it is given to flow collector. The information given from exporter to collector usually called as flow records [8]. It is duty of flow collector to get flow records from flow exporter and stored them in the form of suitable for analysis. Thus by aggregating packets of identical flow, we can inspect for abnormal traffic pattern observed in case of attacks [12].

In this case we are getting speed but questions is does the flow provide enough information i.e. reduction in information should not result in negligence of any single attack. Thus accuracy is in question, as we stated above speed and accuracy are the desirable feature of IDS. As flow is aggregated form of information it cannot provide accuracy like packet based inspection.

VI. NIDS DESIGNED USING TWO STAGES MONITORING APPROACH

As we have seen that packet based approach cannot deal with ever increasing network traffic (Speed). The flow based approach can be able to handle this increased traffic but suffer from accuracy problem. So packet based and flow based approaches are not alternative to each other rather than they are supportive to each other i.e. two stage monitoring.

In case of two stages monitoring approach first stage is flow based approach. In first stage incoming traffic is analyzed using flow based approach and try to detect intrusion and also for suspicious packets. If packets are identified as suspicious then that packet is given to second stage. This packet is examined using packet based approach. All this depicted in following figure. In this case we are getting both, speed and accuracy, desirable features of IDS.

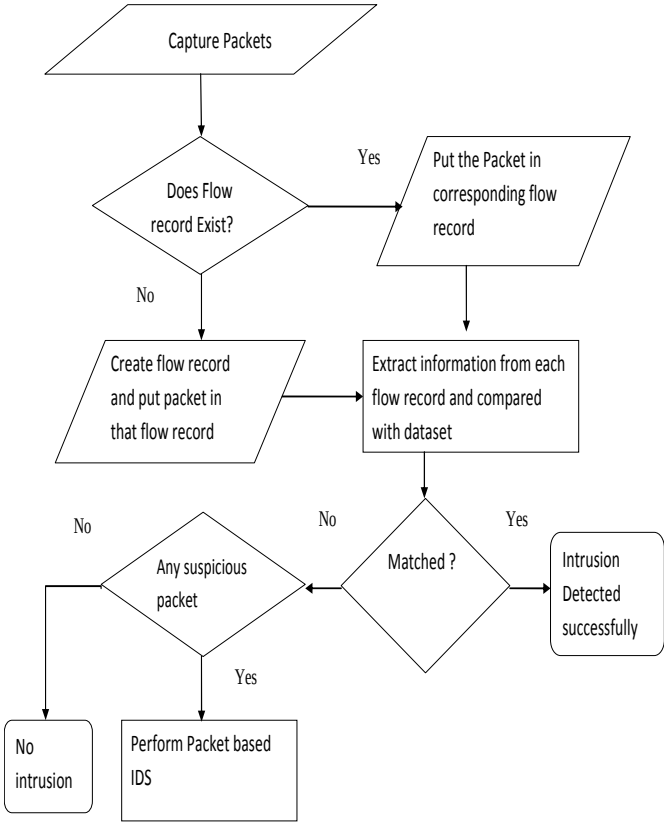

FIGURE 2 TWO STAGES MONITORING NIDS FLOW CHART.

VII. CONCLUSION

As already stated network traffic is increasing and old packet based approach cannot able to handle such ever increasing traffic. The new concept i.e. flow based approach can handle this increased traffic but faces accuracy problem. Thus NIDS are becoming just decorative things if they are not able to handle such situations.

To avoid this better is to use two stage monitoring, first flow based approach to identify suspicious flow and later use packet based approach on suspicious flow to detect intrusion.

REFERENCES

1. F. Sabahi and A. Movaghar, “Intrusion Detection: Survey”, The Third International Conference on System and Network Communications (2008), pp. 23-26.
2. C. Kruegel, F. Valeur and G. Vigna, “Intrusion Detection and Correlation: Challenges and Solutions”, Springer- Verlag Telos (2004),.
3. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning , pp. 235-237.
4. Dr. V K Pachghare , “Cryptography and Information Security”, PHI publication .
5. Anna Sperotto, Georor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller, “ An Overview of IP Flow- Based Intrusion Detection”, IEEE Communication Survey & Tutorials, Vol. 12, No. 3, Third Quarter 2010, pp. 343-355.
6. Anna Sperotto and Aiko Pras, “Flow Based Intrusion Detection System”, 12th IFIP/IEEE 2011: Dissertation Digest (2011), pp. 958-963.
7. Brad Hale, “NetFlow v9 Datagram”, SolarWinds Whitepaper (2012).
8. G. Sadasivan, N. Brownlee, B. Claise, “Network Working Group” RFC 5470, http://www.ietf.org/rfc/rfc5470.txt (2009).
9. Darragh Delaney, “Comparing packet and Flow Capture”, User and Network Forensics, http://blogs.computerworld.com/networking/21078/comparing-packet-and-flow-capture (2012).
10. Derek Banks, “Custom Full Packet Capture System”, SANS Institute Reading Room (2013).
11. Morin B. “Intrusion Detection and Virology: an analysis of differences, similarities and complementariness”, Journal in Computer Virology (2007), pp 39-49.
12. Myung S., Hunk K., Seung C., James H. “A Flow Based Method for Abnormal Network Traffic Detection”, IEEE/IFIP Network Operations and Management Symposium (2004), pp. 599-612.