HOST BASED INTRUSION DETECTION SYSTEM FOR VARIOUS NETWORK ACTIVE ATTACKS

[1]Rekha P, [2]Dr. Amutha S
[1]Student, [2]Professor
[1]Department of Computer Science and Engineering,
Dayananda Sagar College of Engineering, Bangalore, India

Abstract : Network intrusion detection system (NIDSs) plays a important role in securing computer systems against various network attacks There are two types of network intrusion detection systems and they are network based intrusion detection system (NIDS) and host-based intrusion detection system (HIDS). Here the main concern is about defending the system against various attacks. There are many works done in the field of intrusion detection till now. In this paper we introduce Intrusion Detection System for various Network Attacks which uses the standard datasets such as KDD Cup datasets and NSL_KDD datasets to compare the data files sent by users. This paper mainly concentrate on four layer such as Prob Layer, Dos layer, R2L layer and U2R Layer to detect the infected file were both normal files and virus files are passed through and data files passes from source to destination through all four layers using layer selection algorithm. Were data is begin checked in each layer and only normal data is allowed to flow in and reach the destination and infected data are dropped immediately. Promising results have been obtained from our proposed system over the existing system.

***IndexTerms* - KDD Cup datasets and NSL_KDD datasets, layer selection algorithm, network security.**

I. INTRODUCTION

An intrusion detection system monitors(IDS) network traffic for suspicious activity and alerts the system and network administrator. In some cases, the intrusion detection system may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. Intrusion detection system come in a variety of flavour's and approach the goal of detecting suspicious traffic in different ways. There are two types of network intrusion detection systems and they are network based intrusion detection system (NIDS) and host-based intrusion detection system (HIDS) . There are some intrusion detection system that detect malicious activities based on looking at particular signatures of known threats that are similar to the way antivirus software typically detects protects against malicious software that detect based on comparing traffic patterns against a baseline and looking for deviation.

There are intrusion detection systems that simply monitor and alert and there are intrusion detection systems that perform an action or actions in response. Network Intrusion Detection Systems are placed at strategic points or points within the network to monitor traffic that flows to and from all devices in the network .alternatively, you would scan all inbound and outbound traffic, however doing so might create a barrier that would damage the overall speed of the network.

Host Intrusion Detection Systems(HIDS) are those which run on single hosts or devices in the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected
A signature-based intrusion detection system will monitor packets in the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a large between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time, your IDS would be unable to detect the new threat.

An intrusion detection system which is anomaly based will monitor network traffic and compare it against an well-established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is abnormal, or significantly different than the baseline .A passive intrusion detection system simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is left up to them whether to take action to block the activity or respond in some way.

The goal of intrusion detection systems is to automatically detect attack from the continuous stream of network data traffic and generate alarm for administrator. With the growth of hacking and exploiting tools and invention of new ways of intrusion, intrusion detection and prevention is becoming the major challenge in the world of network security. The increasing network traffic and data on Internet is making this task more popular. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. The false positive rates make it extremely hard to analyze and react to attacks.

Network Intrusion Detection System (NIDS). Despite the significant advances in NIDS technology, the majority of solutions still operate using less-capable signature-based techniques, as opposed to anomaly detection techniques. There are several reasons for this reluctance to switch, including the high false error rate (and associated costs), difficulty in obtaining reliable training data, longevity of training data and behavioral dynamics of the system. The current situation will reach a point whereby reliance on such techniques leads to ineffective and inaccurate detection. The specifics of this challenge are to create a widely-accepted anomaly detection technique capable of overcoming limitations induced by the ongoing changes occurring in modern networks.

A passive intrusion detection system simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is left up to them whether to take action to block the activity or respond in some way.

A reactive intrusion detection system will not only detect suspicious or malicious traffic and alert the administrator but will take pre-defined proactive actions to respond to the threat. Typically this means blocking any further network traffic from the source IP address or user.

One of the most well known and widely used intrusion detection systems is the open source, freely available is Snort. It is available for a number of platforms and operating systems including both Linux and Windows. Snort has a large and loyal following and there are many resources available on the Internet where you can get signatures to implement and to detect the latest threats.

There is a fine line between a firewall and an intrusion detection system. There is also a technology called intrusion Prevention System (IPS). An IPS is essentially a firewall which combines network-level and application-level filtering with a reactive intrusion detection system to proactively protect network. It seems that as time goes on firewalls, intrusion detection system and intrusion Prevention System take on more attributes from each other and dim the line even more.
That is where your intrusion detection system would come in. Whether you implement a network intrusion detection system across the entire network or a host intrusion detection system on your specific device, the intrusion detection system will monitor the inbound and outbound traffic and identify suspicious or malicious traffic which may have some how bypassed your firewall or it could possibly be started from inside your network as well.

An intrusion detection system can be a great tool for proactively monitoring and protecting your network from malicious activity, however, they are also vulnerable to false alarms. With just about any intrusion detection system solution implement you will need to start it once it is first installed. You need the intrusion detection system to be correctly configured to recognize what is normal traffic on your network versus. what might be malicious traffic and you, or the administrators responsible for responding to intrusion detection system alerts, need to understand what the alerts mean and how effectively it can be responded.
Historically, intrusion detection systems were categorized as passive or active; A passive , intrusion detection systems that detected malicious activity would generate alert or log entries, but would take no actions. An active , intrusion detection systems, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

II. RELATED WORK

Multiple learning based classifiers using layered approach and Feature Selection for attack detection says that One of the major shares of the current security infrastructure is formed by the Intrusion Detection Systems (IDS). The attack launched towards the security systems are increasing in a fast way providing network security for intrusion detection system [1].

“Multi-layer hybrid machine learning techniques for anomalies detection and classification approach Describes that Intrusion detection systems (IDS) are well-known research area for the detection of anomalous activities in a system from both insider and outsider intruders[2].

A novel hybrid anomaly based intrusion detection method a novel technique which tell why existing network systems and intrusion detection methods are often not sufficient in determining zero-days attacks[3].

“Intrusion detection system combining misuse detection and anomaly detection using Genetic Network Programming” The paper, is a class association rule mining approach based on Genetic Network Programming (GNP) for detecting network intrusion combining misuse detection and anomaly detection is proposed[4].
A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS) Intrusion detection technology is a new generation of security technology that can monitor system to avoid malicious activities[5].

Multi-agent Intrusion Detection System Using Feature Selection Approach As the result of the increased connectivity to Internet and corporate network, industrial control system is no longer resistant to network attacks[6].

Intrusion detection systems vulnerability on adversarial examples Intrusion detection systems define an important and dynamic research area for cybersecurity. The role of Intrusion Detection System within security architecture is to improve a security level by identifying of all malicious and also suspicious events that could be observed in computer or network system[7].

MANET security: An intrusion detection system based on the combination of Negative Selection and danger theory concepts” Many researches have been using artificial immune systems AIS to solve intrusion detection problems due to several reasons[8].

General study of intrusion detection system and survey of agent based intrusion detection system In today's world one of the most serious threat to computer security is the illicit intrusion into a computer system[9].

Multi-agent Intrusion Detection System Using Feature Selection Approach As the result of the increased connectivity to Internet and corporate network, industrial control system is no longer resistant to network attacks[10].

Intrusion detection system based on classification With the network security issues being more outstanding, the safety of system and network resources develop more and more important problem[11].

Intrusion Detection System using Self Organizing Maps With the rapid expansion of computer usage and computer network the security of the computer system has became very important. Every day new kind of attacks are being faced by industries[12].

A Model of Collaborative Intrusion Detection System Based on Multi-agents With the rapid development of computer network and applications, attacks are becoming more and more complicated and ambiguous[13].

Study on network intrusion detection system of Snort Network security is a complex and systematic approach. The intrusion detection system is the first line of defence against network security. Snort is a important intrusion detection system in the field of open source software[14].

Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation Intrusion detection system (IDS) is used to find malicious connections and protect networks from external or internal attacks.[15].

Increasing the reliability of distribution systems by the use of intrusion detection system based on rick flows In this paper presented research methods of intrusion detection in the cloud systems[16].

III. PROPOSED WORK

Here, we represent a model for intrusion detection system which uses attack rules to identify the data affected by virus at each layer using the rules sets. Data is passed from source to destination through four layers i.e Attacks fall into four main categories DOS: denial-of-service, e.g. syn flood; R2L: unauthorized access from a remote machine, e.g. guessing password U2R: unauthorized access to local superuser privileges, e.g., various buffer overflow attacks probing: surveillance and other probing, e.g., port scanning. Each of these layers have some attributes . Data which is virus free and matches all four layer attributes reaches the destination without any problem. Data that is affected by virus is scanned and is dropped immediately by one of the four layer were in the data fails to match the attributes of that layer.

This shows that the modified layer selection algorithm is capable of detecting attacks in network intrusions detection system. The KDDCUP 99 dataset which is freely available online is used for our experimentation and result compression Our intrusion detection system using layer selection algorithm is able to generate attack rules that will detect the attacks in network audit data using anomaly detection, while maintaining a low false positive rate.

There are four important layers in this in the architecture
1)Probe Layer
2)Dos Layer
3)R2L Layer
4)U2R Layer

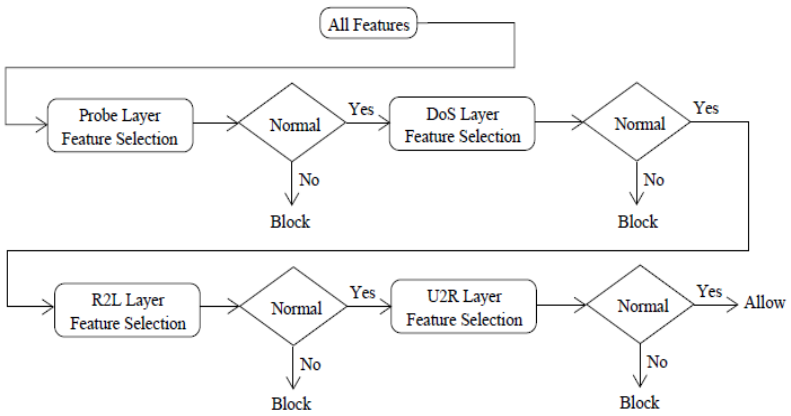

Fig 1 :system architecture

Probe Layer is a program or other device inserted at a key junction in a network for the purpose of monitoring or collecting data about network activities. The probe attacks are planned at achieving information about the target network from a source that is often foreign to the network. Hence, essential connection level features such as the span of connection and source bytes are important while features like" number of files creations" and "number of files accessed" are not expected to provide information for identifying probes.

DoS layer traffic features such as the percentage of connections having similar destination host and similar service and packet level features such as the source bytes and percentage of packets with errors are important. To detect DoS attacks, it may not be important to know whether a user is logged in or not.

The U2R attacks involve the semantic details which are very problematic to identify at an initial stage. Such attacks are often content based and target based on an application. Hence, for U2R attacks, we select features such as "number of file creations" and "number of shell prompts invoked," while we ignore features such as "protocol" and "source bytes."

The R2L attacks are one of the most problematic to detect as they affect the network level features and the host level features. We there fore select both the network level features such as the "duration of connection" and "service requested" and the host level features such as the "number of failed login attempts" among others for detecting R2L attack.

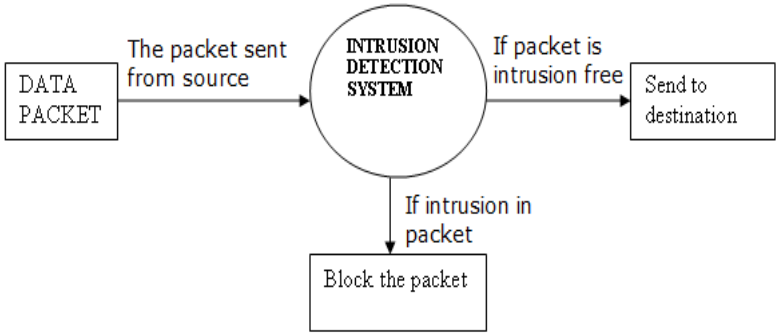

Fig 2: Flowchart for Intrusion Detection

Figure above shows data is collected from source module which has to be passed from source to destination through four layers i.e Probe Layer DOS Layer R2L Layer and U2R Layer data files reaches destination if it is virus free else the data file is dropped immediately by any of the layer if data files are affected by virus.

IV. RESULTS AND ANALYSIS

A result is the final consequence of actions or events expressed qualitatively or quantitatively. Performance analysis is an operational analysis, is a set of basic quantitative relationship between the performance quantities. user can login using login credentials provided by the admin. once the user is authenticated user can upload their respective files. Files are passed from source to destination via probe , DOS, R2L and U2R layers. Files which are virus free reaches destination. Virus files are dropped immediately by any one of the layer.

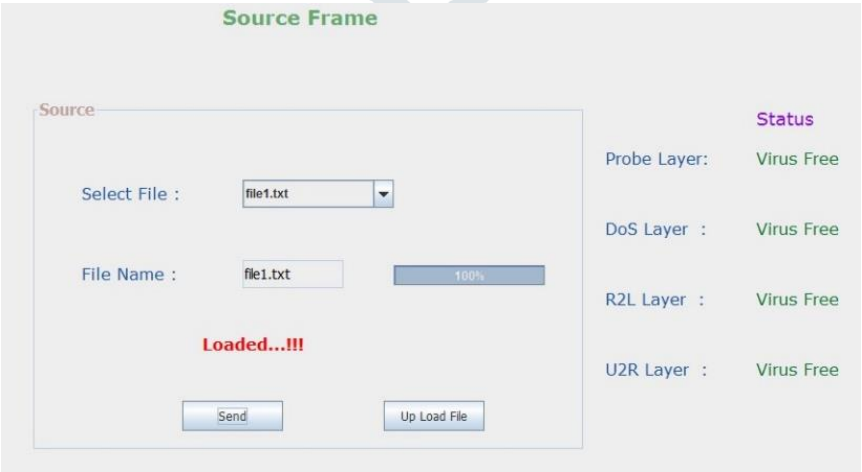

Fig 3: virus free source frame

Figure above shows how user files are uploaded and send to all four layers . we can see that file uploaded is virus free and reaches destination without any interrupts.

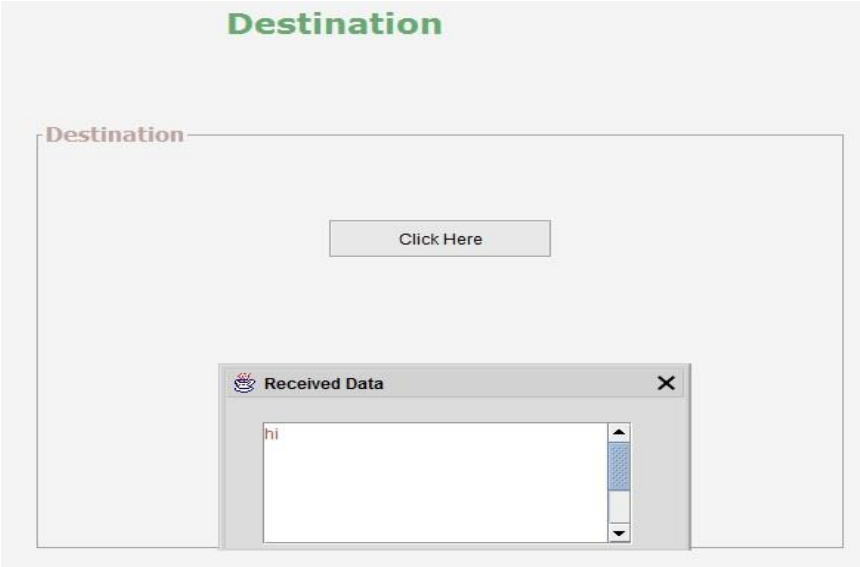

Fig 4: virus free Destination frame.

Figure above shows destination frame were data file after passing successfully through probe, DOS, R2L and U2R layer reaches destination without any interruptions.

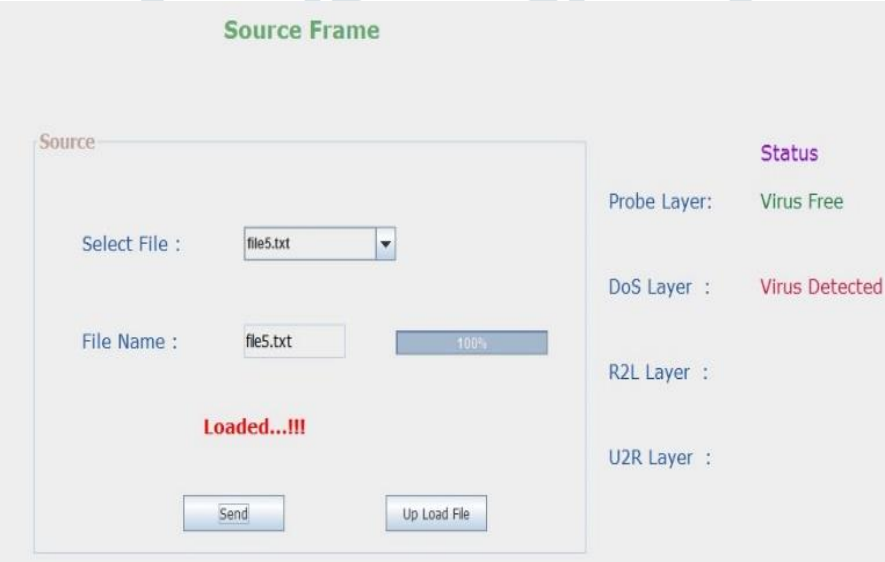

Fig 5 : virus detected source frame

Figure above shows how user files are uploaded and send to all four layers . we can see that file uploaded is affected by virus and is detected in DOS layer.

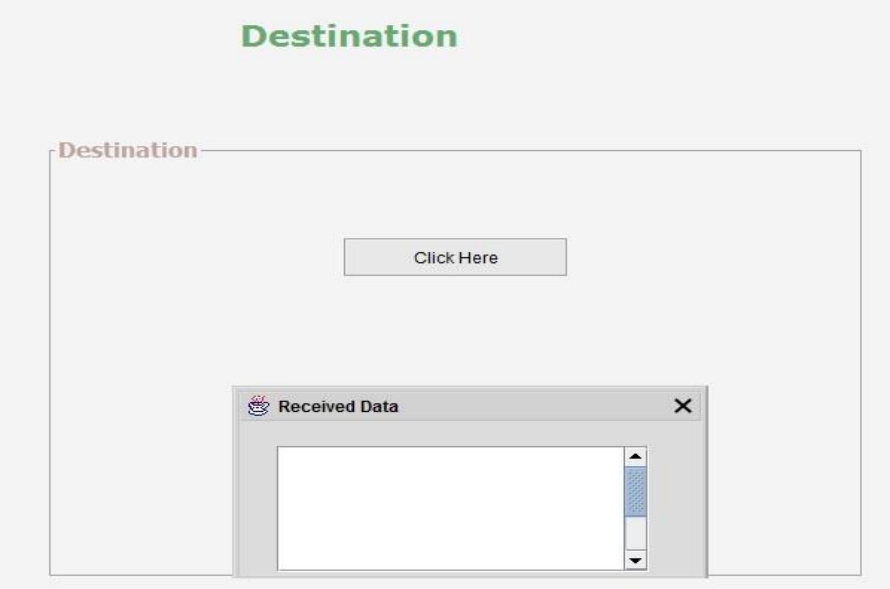

Fig 6: virus free Destination frame.

Figure above shows destination frame were data file are affected by virus and fail to reach destination .

V. CONCLUSION

In this paper, we have discussed the problems faced by existing intrusion detection system. Existing system uses KDDCUP 99 data sets for result analysis 40 parameters were used. In proposed system we are using less than 40 parameters for Probe, DOS, R2L and U2R layers. The proposed system can helps us in identifying an attack very quickly once it is detected at a particular layer data file are dropped immediately by same layer. If data files uploaded by user is virus free then it successfully passes through all four layers and reaches destination without any interruption, therefore time required to process the data files is optimized and detection is faster compared to the existing system

VI. REFERENCES

[1] Layered Approach Using Conditional Random Fields for Intrusion Detection Kapil Kumar Gupta, Baikunth Nath, Senior Member, IEEE, andRamamohanarao Kotagiri, Member, IEEE.

[2] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.

[3] Y. Chang, W. Li, and Z. Yang, "Network intrusion detection based on random forest and support vectormachine," in *Proc. IEEE Int. Conf. Comput. Sci. Eng./IEEE Int. Conf. Embedded Ubiquitous Comput.*, Jul. 2017, pp. 635–638.

[4] KDD Cup 1999 Intrusion Detection Data, http://kdd.ics.uci.edu/ databases/kddcup99/kddcup99.html, 2010.

[5] Y. Y. Aung and M. M. Min, "An analysis of random forest algorithm based network intrusion detection system," in *Proc. 18th IEEE/ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput.*, Jun. 2017, pp. 127–132.

[6] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in *Proc. 2nd Int. Conf. Adv. Cloud Big Data*, Nov. 2014, pp. 247–252.

[7] SANS Institute—Intrusion Detection FAQ, http://www.sans.org/ resources/idfaq/, 2010.

[8] T. Abraham, IDDM: Intrusion Detection Using Data Mining Techniques, http://www.dsto.defence./gov.au/publications/ 2345/DSTO-GD-0286.pdf, 2008.

[9] R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases," Proc. ACM SIGMOD, vol. 22, no. 2, pp. 207-216, 1993.

[10] N.B. Amor, S. Benferhat, and Z. Elouedi, "Naive Bayes vs. Decision Trees in Intrusion Detection Systems," Proc. ACM Symp. Applied Computing (SAC '04), pp. 420-424, 2004.

[11] J.P. Anderson, Computer Security Threat Monitoring and Surveillance,http://csrc.nist.gov/publications/history/ande80.pdf, 2010.

[12] R. Bace and P. Mell, Intrusion Detection Systems, Computer Security Division, Information Technology Laboratory, Nat'l Inst. of Standards and Technology, 2001.

[13] D. Boughaci, H. Drias, A. Bendib, Y. Bouznit, and B. Benhamou, "Distributed Intrusion Detection Framework Based on Mobile Agents," Proc. Int'l Conf. Dependability of Computer Systems (DepCoS-RELCOMEX '06), pp. 248-255, 2006.

[14] Y. Bouzida and S. Gombault, "Eigenconnections to Intrusion Detection," Security and Protection in Information Processing Systems, pp. 241-258, 2004.

[15] H. Debar, M. Becke, and D. Siboni, "A Neural Network Component for an Intrusion Detection System," Proc. IEEE Symp. Research in Security and Privacy (RSP '92), pp. 240-250, 1992.

[16] T.G. Dietterich, "Machine Learning for Sequential Data: A Review," Proc. Joint IAPR Int'l Workshop Structural, Syntactic, and Statistical Pattern Recognition (SSPR/SPR '02), LNCS 2396, pp. 15-30, 2002.