Review on Implementation of Intrusion Detection in Physical Network

Chinmay Karadkar[1], Ketan Thuturkar[2],
Ketan Ghatole[3], Harsh Patel[4], Roshan Thakur[5]

[1]*Student, CSE, DBACER, RTMNU, India*
[2]*Student, CSE, DBACER, RTMNU, India*
[3]*Student, CSE, DBACER, RTMNU, India*
[4]*Student, CSE, DBACER, RTMNU, India*
[5]*Assistant Professor, CSE, DBACER, RTMNU, India*

***Abstract* – Network infrastructure security have become a major concern with the extensively growing computing environment. A malicious activity made with an intension to disrupt the functioning of the network is termed as intrusion. Intrusion can have its root effects varying in a wide range, including individual host, resources and the network infrastructure itself. HIDS functions at the primary stage where it prevents unauthorized access to the host. NIDS ensures secure communication within the network and entail misuse of resources. NIDS may fail in switching environments hence HIDS should be incorporated to enable additional security. A Hybrid IDS is a mechanism which functions to examine activities such as login attempts, system files integrity, monitoring and analysis of individual packet from host and network domain respectively. It significance comes to fore when others preventive measure such as firewall, etc. fails. This paper describes the implementation of such a hybrid system with an objective to ensure network integrity by taking effective measures to provide reluctance to the attacks.**

***Keywords* – HIDS, IDS, Intrusion, NIDS, Network Security, Packet.**

I. INTRODUCTION

Computers were introduced to the world in the late 19th century. Foundation of the internet was laid by ARPNET which encouraged sharing over networks and availability of a wide range of services to distant users. Technological advancements aided spread of Internet across the globe reaching various domains as a result a vast number of organizations got connected.

Sensitive information is shared amongst organizations for expanding their functional areas. Intruders work with an objective to gain access to such sensitive information. Network security always has been a major concern and

Preventive measures have been undertaken so that it cannot be compromised under the influence of intentional attacks. Consistent attacks on network called the need for systems, which will defend these fictitious activities. Therefore network defender system, firewall, etc. came into existence. Security issues were not restricted to networks itself and hence the need of security at system level arose ultimately. Firewalls, Antiviral software sound promising yet some attacks and intrusions can go undetected. To tackle such intrusions an IDS that is Intrusion Detection System was introduced.

An IDS is a software application that detects any intrusion in the defined network limits. IDS are differentiated into two types:

1. Host intrusion detection system (HIDS)
2 .Network intrusion detection system (NIDS)

Host intrusion detection system, as the name suggests resides on single host. It examines the activities on an individual host on which it is installed. Login attempts, system log files, resource utilization are analysed for detection of an intrusion. HIDS may depend on the host's operating system.

Network intrusion detection system collects information from the network traffic stream. This information is compared with signatures to detect sign of an attack. Attack signatures are predefined rules on which will constitute attack. NIDS monitor traffic over a specified network segment and are independent of operating system. Hybrid intrusion detection systems are the one which possess capabilities of both the Host intrusion detection system as well as Network intrusion detection system. In the year 1998, Martin Roesch launched a IDS named "SNORT".

II. LITERATURE SURVEY

[1] A two layered architecture forms the core of the Hybrid system. The first stage focuses upon the detection of anomalies in the network traffic, while the second stage which is based on the Hidden Markov Model (HMM) narrows down the potential attacks over the IP address. The

HMM works to profile the TCP based communication channel for intrusion detection. The HMM model separates the traffic for formation of profiles to detect intrusion. High detection rate of intrusion can be considered as the virtue of the HMM, but it fails to raise alarms against liable attacks by identifying the traffic. False positive rate endangers the flow of legal incoming packets. This fact can raise questions against the rigidity of the system hence a new model i.e. the Naive model needs to be collaborated with the existing model to increase the efficiency of the IDS. The IDS is termed 'Hybrid' because of this combination of the two models. The NB model performs the monitoring of online traffic with the probability of window of intrusion while the HMM monitors the offline traffic and alerts the firewall to block IP addresses. IP spoofing can heavily affect the functioning of the proposed Hybrid system. The resources in such cases can fall into hands of an intruder thus causing misuse of these resources. The fact that the end to end communication exists between the server and client endlessly and acquaintance of the complete knowledge about computations might not be available in real time. Buffers for storage of packets at servers may exhaust, as they may be used frequently to store the information about these computations.

[2] The categorization of IDS is based upon the its residence in the system , which may be Host (HIDS) or Network (NIDS).The CIDF architecture is the basis for the proposed IDS. The architecture provides for components: Event generators, Event analysers, Event databases and Event Responses. The generator component collects filters and makes it worthy of utility in the event, the analysis component scrutinizes the event data to detect attacks ,the database component is used for storage of event data and the response component specifies a set of commands as actions against attacks. The proposed IDS have modules corresponding to the CIDF architecture. The collection module monitors packets from the network traffic, captures the intended one and decodes it for analysis. The attack rule library contains the predefined attack patterns of known attacks. The analysis module matches the packets information with the attacks patterns for intrusion detection. On confirmation of an attack, the response module triggers a set of actions to handle the attack. The IDS can be made more effective and efficient by combining the existing system with anomaly detection techniques.

[3] The paper describes an intrusion detection system whose operational ability is derived in correspondence to a human immune system. The IDS presents features such as intrusion evidence gathering, attack signature extraction and automated response against any intrusive activity. Automated response reduces the human effort in ensuring the security of the network. The framework for the prototype IDS ADENOIDS possess components such as Evidence based detector, Knowledge base detector, Adaptive response generator, Signature extractor, Forensic support repository and Innate response generator. The Evidence based detector gathers proofs about the existence of loop holes in the network which becomes a potential privilege to an attacker. The Adaptive response generator takes a set of counter measures to prevent the resultant damage of an attack. Forensic support repository stores information about a positive attack so that the network can be made immune to similar attacks in mere future. New tests can be performed to identify other vulnerable applications so that the framework can be equipped with components responsible for handling intrusion.

[4] The paper describes functioning of a Network Intrusion Detection System embedded in a smart sensor. The key issues which are addressed and considered for the development of such a NIDS are the number of alerts generated by a traditional IDS and the complexity involved in managing these alerts. As a solution to afore specified issues, a Distributed Intrusion Detection System proves to be a prominent in reducing the involved complexity. The proposed system establishes logical relation between alerts so as to handle them unanimously increases the detection rate, reduces the impact of intrusion upon the network. Smart sensors in the SSN (Smart Sensor Network) are considered as autonomous entities. These sensors work not only to capture the network traffic but also to filter and process a set of packets for analysis. To alert the administrator about intrusion, Intrusion Detection Message Exchange Format (IDMEF) is used whose response can be continuous as well as on demand. The sensor which is formed by the network adapter for connection to LAN supports promiscuous mode of operation. Two individual interfaces for monitoring and communication in the IDS enable proper functioning even in resource starving environment. The prototype based on the specified proposal yields stable detection results by using anomaly detection to identify behaviour different from the normal ones.

[5] The paper describes about An Anomalous based Network Intrusion Detection System that comprises of two parts. The first is an unsupervised anomaly detection technique. This approach determines the extent to which a network connection can be anomalous. This is determined with the help of statistical data that is gathered on the basis of outlier detection algorithm. The algorithm detects the deviation from the normal behaviour. Parameters for extraction include features like count of packets, packet contents like various flags, source and destination addresses etc. The second part is an association pattern analysis based module. It stores information about network connections that are considered to be anomalous by former module and creates profiles to distinguish between normal and anomalous connections. These profiles will be used for future reference.

III. METHODOLOGY

A stand-alone system developed detect malicious activities is referred to as an Intrusion Detection System. The IDS can adopt any of the following techniques to form its functional core:

A. Unauthorized access detection

Violation of standard access procedure can be detected and prevented by implementation of this technique. It maintains access policies for each host known as Access Control List (ACL). User's login credentials are compared with ACL for detection of any unauthorized access.

B. Anomaly based detection

In this detection technique, behaviour of client is monitored to create a baseline for consistent parameters, which is termed as a profile. Any behavioural deviation from the one in the profile is considered as an anomaly.

C. Signature based detection

Signatures are known patterns of attacks which have been exploited by intruders in the past. Signature based detection technique monitors network traffic in search of signature patterns. Countermeasures can be taken as a response when a signature matches successfully. An unsuccessful attempt leaves traces in the form of partial signatures. These signatures can signify an intrusion attempt whose count can be maintained through monitoring.

IV. PROPOSED PLAN OF WORK

Intrusion Detection Systems can be classified into HIDS and NIDS depending upon where they reside and the orientation of their monitoring. Traditional Intrusion Detection Systems were solely based on a single intrusion detection technique which narrowed down the operability. Alarming vulnerabilities of the networks have signified the need to combine various detection techniques. We propose to integrate these systems to make Hybrid Intrusion Detection System. The Hybrid Intrusion Detection System will have two modules - HIDS and NIDS.

A. Host Intrusion Detection Module

This Module will be based on Client-Server architecture. A machine on which IDS is installed will act as server whose responsibility will be to accept connection requests from clients to provide access to system and monitor client activities. The authenticity of a client will be verified during the phase of connection establishment.

While implementing this module the following criteria should be considered. Client credentials such as User Id, Password, MAC address will be stored in the Database. The administrator will have the authority to carry out changes over the Database. The administrator will store above client credentials into the Database. These parameters will form the basis for intrusion detection.

A particular MAC address will be assigned to a client to gain access to the network. User ID and Password are the parameters accountable for a user's authorized access to the assigned MAC address. To provide a two layer security, it is mandatory for a user to provide security question along with its answer at the time of his first login. The security question in combination with User ID and Password will allow a user to gain access to the network through a MAC address different from his assigned one. On providing wrong credentials, the client will be asked to enter the correct credentials. On three unsuccessful login attempts the user will be blocked for a time span of 60 minutes. The blocking mechanism makes use of UNIX Epoch time to calculate finish time of respective client. MAC addresses will be considered, the identifying attribute instead of an IP address as IP address can be spoofed easily.

B. Network Intrusion Detection Module

This module will work as a Stand-Alone system which will monitor the incoming network traffic on the network adapter. This module operates with an intension to detect TCP SYN FLOOD attack. This attack is amongst the variety of attacks under the Denial of Service domain which hampers the network functionality.

A network stream carries a variety of data elements of which TCP packets will be of prime importance. TCP packets consists of headers which contain information such as source IP and sink IP addresses, Flag information etc. which helps this module in detection of attack. TCP SYN attack exploits the limitation of TCP's half open connection. This module will capture and queue the TCP packets from the network traffic immediately for analysis. It will check for IP address from which SYN requests are forwarded successively. If incoming requests are greater than predefined threshold value, then blocking mechanism will block the IP address. [9]WinPCap will be used to capture packets on the network adapter. WinPCap is an open source library for Windows Platform which provides functions to deal with the network.

V. CONLUSION AND FUTURE SCOPE

The study showed that intrusions vary between domains of relevance ranging from host to network. Neither Host Intrusion Detection System nor Network Intrusion Detection System alone can ensure complete immunity to intrusion. A hybrid approach can prove to be a feasible solution to encounter intrusion with devastating effects upon the network infrastructure. The collaboration of two detection systems facilitates enhanced ability of the network to tackle attacks.

The basic definition of network describes openness in communication as the root of their existence. Any restrictions imposed on this nature of networks will hinder their functionality and performance. The perpetual advancements in intrusion and attacks will always continue to persist, thereby encouraging the need for new intrusion detection techniques. Ability of Hybrid Intrusion Detection System can be improvised with the introduction of new techniques that will facilitate keen surveillance over the system. HIDS module can be implemented with encryption techniques for sophisticated communication. Log analysis can be included in the module to observe frequent activity of the user. NIDS module can be made more immune to attacks by incorporating better algorithms for monitoring and processing of packets.

Neural networks are amongst the most flourishing domains today, which are adaptive enough to imitate a secure model. These networks can learn and improve their immunity against attacks. A new approach can be used to develop a IDS which can work efficiently along with neural networks to enhance detection and security.

REFERENCES

[1] R Rangadurai Karthick, Vipuk P. Hattiwale, Balaraman Ravindran, "*Adaptive Network Intrusion Detection System Using a Hybrid Approach*", IEEE 2012

[2] Zhou hunyue, Lie Yun and Zhang Hongke, "*A Pattern matching based Network Intrusion Detection System*", ICARCV, IEEE 2006.

[3] Fabricio Sergie de Paula, Leandro Nunes de Castro,and Paulo LIcio de Geus, "*A Intrusion Detection System Using Ideas from the Immune System* ", IEEE 2004.

[4] Francisco Macia -Perez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera, Juan Antonio Gil-Martinez-Abarca, Hector Ramos-Morillo and Iren Lorenzo-Fonseca, "*Network Intrusion Detection System Embedded on a Smart Sensor*", Transactions on industrial Electronics IEEE, Vol.58, No.3, March-2011.

[5] Bane Raman Raghunath, Shivsharan Nitin mahadeo, "*Network Intrusion Detection System (NIDS)*", First International Conference on Emerging Trends in Engineering and Technology, IEEE 2008.

[6] Eigene C. Ezin, Herve Akakpo Djihountry, "*Java-Based Intrusion Detection System in a Wired Network*", International Journal of Computer Science and Information Security, Vol. 9. No. 11, November 2011.

[7] Prof.D.P.Gailwad, Pooja Pabshettiwar, Priyanka Musale, Pooja Paranjape and Ashwini S. Pawar, "*A Proposal for Implemenation of Signature Based Intrusion Detection System Using Multithreading Technique*", International Journal of Computational Engineering Research, Vol. 2, Issue. 7, November 2012.

[8] Chetan R and Ashoka D.V., "*Data Mining Based Network Intrusion Detection System: A Database Centric Approach*", 201 International Conference on Computer Communication and Informatics IEEE, Jan.10-12, 2012.

[9] Archana D. Wankhede and Dr. P.N. Chatur, "*Implementation of Intrusion Detection and Prevention System Using JPCAP/WINPCAP*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue. 5, May-2014.