Review on Network Intrusion Detection Framework

Dr. Siddhartha Choubey[1], Parmanand Sahu[1], Abha Choubey[1]
[1] Department of CSE, Shri Shankaracharya Group of Institutions, Bhilai

Abstract— In the present situation the greater part of the organization and companies relies upon the web for their correspondence, storage and security of their valuable information and other internal assets from the unauthorized access as the significance of web is expanding quickly the odds of assaults additionally increments in the proportion. Intrusion Detection System assumes a critical part in organization security. Its primary part in the system is to assist PC framework with creating and managing malicious activity. An IDS goes about as a key segment to guaranteeing the security of any system or framework on which it runs. IDS deals with the idea of researching all the approaching bundles for the discovery of any malicious action. This is a study paper on the different upgrades throughout the decades on IDS.

Keywords— *Intrusion Detection System, Network, Malicious Packets, Data Security.*

*****

I. Introduction

Network intrusion detection systems (NIDS) are most efficient way of defending against network-based attacks aimed at computer systems [1, 2]. These systems are used in almost all large-scale IT infrastructures [4]. Fundamentally, there are two primary sorts of intrusion identification frameworks: signature-based (SBS) and anomaly-based (ABS). SBS frameworks (e.g. Snort [3, 5]) depend on design acknowledgment systems where they keep up the database of signature of beforehand known attacks and contrast them and broke down information. An alert is raised when the signature are coordinated. Whereas ABS frameworks (e.g. PAYL [6]) manufacture a measurable model portraying the typical system movement, and any strange conduct that digresses from themodel is distinguished. Rather than signature-based frameworks, anomaly-based based frameworks have the preferred standpoint that they can distinguish zero-day attacks., hence novel attack can be recognized when they occur. While ABS (dissimilar to SBS) requires a preparation stage to build up the database of general attacks and a watchful setting of edge level of location makes it complex.

Anomaly Based Detection

The anomaly construct recognition is based with respect to characterizing the system conduct. The system conduct is as per the predefined conduct, at that point it is acknowledged or else it triggers the occasion in the anomaly location. The acknowledged system conduct is arranged or learned by the determinations of the system directors. The essential stage in characterizing the system conduct is the IDS motor ability to slice through the different conventions at all levels. The Engine must have the capacity to process the conventions and comprehend its objective. In spite of the fact that this convention investigation is computationally costly, the advantages it creates like expanding the manage set aides in less false positive alerts.

The major disadvantage of anomaly based detection is that it requires collecting and learning of rules and after that implementing those rules to IDS.

Signature Based Detection

Signature based detection includes searching system network for a progression of malicious sequences. The primary advantage of this strategy is that signatures are easy to develop but difficult to create and comprehend on the off chance that we realize what arrange conduct we are attempting to distinguish. For example, we may utilize a signature that searches for specific strings inside adventure specific buffer overflow weakness. The occasions created by signature based IDS can impart the reason for the alarm. As example coordinating should be possible all the more productively on present day frameworks so the measure of energy expected to play out this coordinating is insignificant for a lead set. For instance if the framework that will be ensured just convey by means of DNS, ICMP and SMTP, every single other signature can be disregarded.

The major disadvantage of this technique is that the signature must be present beforehand.

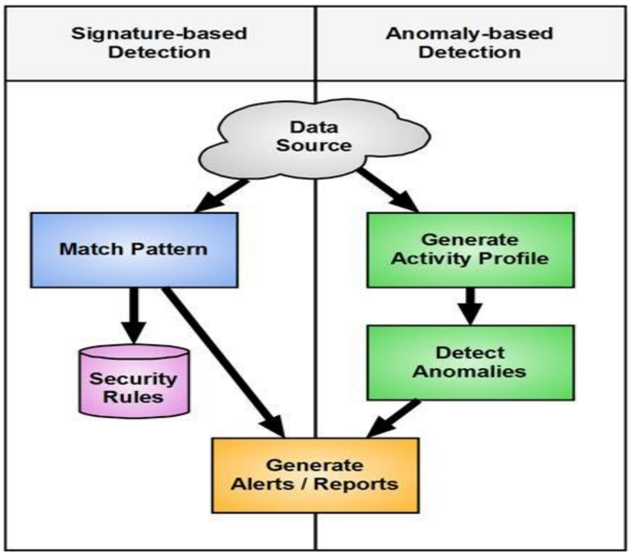


Fig.1. Flow chart of Signature and Anomaly based detection technique

Classification of anomaly Based Detection

There are various types of anomaly based intrusion detection. Some of them are described below.

Statistical Based
Markov Process
Operational
Multivariate
Time Series
Cognition Based
Finite State Machine
Expert Systems
Machine Learning
Bayesian Network
Genetic Algorithm
Neural Network
Fuzzy Logic

Statistical Based Model

Statistical based model includes Markov process model, time series model etc. These model are depend upon some statistical historic data which are processed by some formulas. These formulas are standard and are very accurate while producing results.

Cognition Model

This model is also known as expert system model. It require knowledge base for processing the information. The huge knowledge base is required for framework to predict the malicious flow of the network.

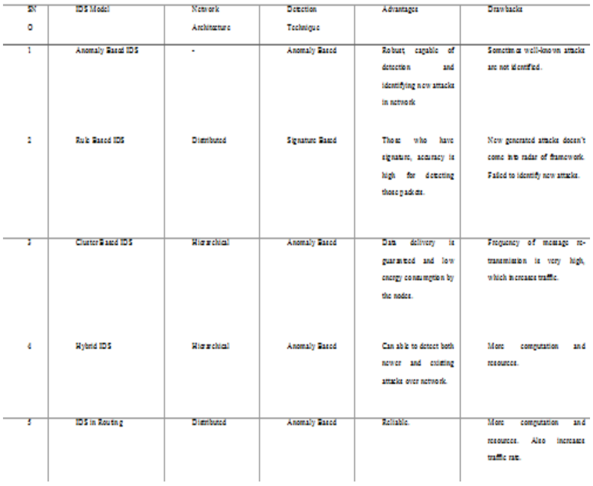
Machine Learning

This model is very popular among researches. There are lots of machine learning techniques are present which can be used for detection of malicious flow in network. The technique includes Bayesian Network simulation, neural network, fuzzy logic etc.

I. Shows the comparison of various techniques used in various layers of network for malicious network detection.

TABLE I. Protocol and its Overhead in Various Layers for Malicious Network Detection System

Layer	Protocol	Overhead
Physical	RSSI Value	Calibration RSSI value for neighbor nodes
MAC	TDMA	Keeping track of TDMA for other nodes
Network	Checks neighbor and expected packet info matches matches	Updating of hops in the packets
Application	RTT	Calibration of RTT for each node



SN O	IDS Model	Network Architecture	Detection Technique	Advantages	Drawbacks
1	Anomaly Based IDS	-	Anomaly Based	Robust, capable of detection and identifying new attacks in network	Sometimes well-known attacks are not identified.
2	Rule Based IDS	Distributed	Signature Based	Those who have signature, accuracy is high for detecting those packets.	New generated attacks doesn't come into radar of framework. Failed to identify new attacks.
3	Cluster Based IDS	Hierarchical	Anomaly Based	Data delivery is guaranteed and low energy consumption by the nodes.	Frequency of message re-transmission is very high, which increase traffic.
4	Hybrid IDS	Hierarchical	Anomaly Based	Can able to detect both newer and existing attacks over network.	More computation and resources.
5	IDS in Routing	Distributed	Anomaly Based	Reliable.	More computation and resources. Also increase traffic rate.

TABLE II. Comparisons of various techniques and method used in existing system

Challenges in IDS

Intrusion detection systems in theory looks like a defense tool which every reorganization needs. However there are some challenges the organizations face while deploying an intrusion detection system. Some of them are:

Lack of infrastructure.
Dynamic change in topology of networks.
Difficult routing protocols.
Recourses consumption.

II. Literature Survey

Yi S et al. [7], presents the algorithm for information mining of intrusion discovery framework has been enhanced and streamlined to accomplish smart location of system information. Winsock2 SPI is utilized amid the outline to catch information in the system, and the strategy for "session sifting" is embraced to channel arrange bundles. The framework comprises of modules of control rules and wise discovery, and so on. As per real location, the framework is equipped for showing system association status consistently, adequately controlling application programs and shrewdly recognizing system information.

Jiankun Hu and Xinghuo Yu et al [8] attempts to improve the host-based anomaly intrusion identification, concentrating on framework call based HMM. This was again later improved with the consideration of information pre-handling for perceiving and dispensing with excess sub-groupings of framework calls, coming about in less number of HMM sub models. Exploratory outcomes on three open databases showed that preparation cost can be decreased by half without influencing the intrusion identification execution. False caution rate is higher yet sensible contrasted with the group preparing technique with a 58% information decrease.

R. Nakkeeran et al [9] proposed an anomaly discovery framework involving identification modules for identifying anomalies in each layer. The anomaly identification aftereffect of the neighbor node(s) is taken by the present hub and its outcome thusly is sent to the neighbor node(s).Experimental comes about uncovered expanded location rate and diminished false caution positives, contrasted with different strategies.

Jiong Zhang et al [10] proposed another structure of unsupervised anomaly NIDS in light of the exception location system in random forests calculation. The system manufactures the examples of system benefits over datasets marked by the administrations. With the fabricated examples, the system identifies attacks in the datasets utilizing the modified anomaly identification algorithm, decreasing the complexity. This approach is autonomous of free attack training datasets, however accept that each system benefit has its own particular example for ordinary activities.

TY. Zhao [11] develops a system intrusion identification display in light of information mining innovation, which can distinguish known intrusion adequately and has a decent ability to perceive obscure information diagram which can't be recognized successfully in customary IDS. The paper mostly does the accompanying work: by examining the intrusion profoundly, extricate the properties which can reflect intrusion attributes viably; consolidate abuse discovery, anomaly location and human mediation, build up rule library in view of C.45 decision tree calculation and utilize the ideal example coordinating in order to enhance identification rate.

Jabez Ja, et al. [12]. Proposes intrusion detection framework to recognize the attacks productively. Besides, it is similarly vital to identify attacks at a starting stage with a specific end goal to diminish their effects. This exploration work proposed another approach called exception identification where, the anomaly dataset is estimated by the Neighborhood Outlier Factor (NOF). Here, prepared model comprises of huge datasets with dispersed capacity condition for enhancing the execution of Intrusion Detection framework. The test comes about demonstrated that the proposed approach recognizes the anomalies adequately than some other methodologies.

TABLE IV. Comparisons of various attacks and energy consumption in existing system

SNO	IDS Model	Handled Attacks	Energy Computation
1	Anomaly Based IDS	Routing attack Sink Hole Black Hole	Low
2	Rule Based IDS	Black Hole Selective Forwarding	Low
3	Cluster Based IDS	Black Hole	Very Low
4	Hybrid IDS	Worm Hole Selective Forwarding	Medium
5			High

III. Conclusion

This paper reviews the establishments of the primary anomaly based system intrusion recognition advances alongside their operational designs and furthermore exhibits an classification and detection techniques of various IDS Systems. This investigation moreover depicts the primary highlights of a few IDS frameworks/stages that are right now accessible in a compact way.

The most huge open issues with respect to Anomaly based Network Intrusion Detection frameworks are distinguished, among which evaluation is given specific accentuation. The displayed information in Table II and III, constitutes a critical point to begin for tending to further more Research and Development in the field of IDS.

References

[1]. Hazem M. El-Bakry, Nikos mastorakisa, "Real-Time Intrusion Detection Algorithm for Network Security,WSEAS Transactions on communications, Issue 12, Volume 7, December 2008

[2]. Debar.H, Dacier.M and Wespi.A, "A Revised Taxonomy of Intrusion-Detection Systems" Annales des Telecommunications 55(7–8) (2000) 361–378

[3]. Roesch.M, "Snort - Lightweight Intrusion Detection for Networks" 13th USENIX Conference on System Administration, USENIX Association (1999) 229–238

[4]. Allen.J, Christie.A, Fithen.W, mchugh.J, Pickel.J, Stoner.E, "State of the practice of intrusion detection technologies" Technical Report CMU/SEI-99TR- 028, Carnegie-Mellon University - Software Engineering Institute (2000).

[5]. Hossein M. Shirazi,"Anomaly Intrusion Detection System Using Information Theory, K-NN and KMC Algorithms", Australian Journal of Basic and Applied Sciences, 3(3): 2581-2597, 2009

[6]. Wang. K and Stolfo.S.J, "Anomalous Payload-Based Network Intrusion Detection" 7th Symposium on Recent Advances in Intrusion Detection, Volume 3224 of LNCS., Springer-Verlag (2004) 203–222

[7]. Yi S., Deng F. (2012) Research of Network Intrusion-Detection System Based on Data Mining. In: Gaol F. (eds) Recent Progress in Data Engineering and Internet Technology. Lecture Notes in Electrical Engineering, vol 157. Springer, Berlin, Heidelberg.

[8]. Jiankun Hu and Xinghuo Yu, "A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection" IEEE Network Journal, Volume 23 Issue 1, January/February 2009.

[9]. R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad-hoc networks" IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[10]. Jiong Zhang and Mohammad Zulkernine, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection" IEEE International Conference on Communications, 2006.

[11]. Y. Zhao, "Network intrusion detection system model based on data mining," 2016 17th IEEE/ACIS International Conference on Software Engineering,Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Shanghai, 2016, pp. 155-160.

[12]. Jabez Ja, Dr B.Muthu Kumar, "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach", International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)