ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Intrusion Detection: A Survey

Vani A. Hiremani

Assistant Professor, Dept. of Computer Engineering, Pune Institute of Computer Technology, Pune, Maharashtra, India

ABSTRACT: Data exchange is very essential part in any communication process. Since, from establishing to delivery at desired destiny. The overall process has to be sure about integrity of information being shared across channel for flawless transmission. In computer communication both sender and receiver are expected to sign legal agreement before getting into actual transmission. Throughout the data exchange process they need to abide by this. Agreement generally may include the traffic pattern, data rate, packet format, sequence signature, mode of transmission, preamble and CRC details. Based on this, the two communicating entities authenticate each other. On observing disruption in any of above details indicates presence of the intrusion (unauthenticated third party). Since, from many decades many researches are working towards better identification of intrusion and many are successful. Through this paper I tried to summarize some of recent works focused on intrusion detection with variousapproaches.

KEYWORDS: Types of IDS, Medoid Clustering Algorithm, Snort and EAACK

I. INTRODUCTION

A computer system should provide assurance of confidentiality, integrity and fortification against intrusion. Since, due to increased connectivity on internet, and the evolution of vast spectrum of real time applications, e-commerce, e-business and more and more systems are subject to attack by intruders.Intrusion is defined as, process of intervening as burglar in between two authentic entities and the attempt to compromise the integrity,confidentiality or availability of a resource. And a system which is installed to take care of such ill activities by detecting them and keeps updated both entities. Intrusion detection systems (IDS) can be classified into different ways. The major classifications are Active and passive IDS, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS), Knowledge-based (Signature-based) IDS and behavior-based (Anomaly-based) IDS

1. Active and passive IDS

An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS) which is configured to automatically block suspected attacks without any intervention required by an operator. It has the advantage of providing real-time corrective action in response to an attack.A passive Intrusion Detection Systems (IDS) is a system that is configured to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It is not capable of performing any protective or corrective functions on its own.

2. Network Intrusion detection systems (NIDS)

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate managementinterface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

3. Host Intrusion Detection Systems (HIDS)

HIDS installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. It can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network and are used to monitor any intrusion attempts on critical servers.The drawbacks of Host Intrusion Detection Systems (HIDS) are-

- Difficult to analyze the intrusion attempts on multiple computers.
- Host Intrusion Detection Systems (HIDS) can be very difficult to maintain in large networks with different operating systems and configurations
- Host Intrusion Detection Systems (HIDS) can be disabled by attackers after the system is compromised.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

4. A knowledge-based (Signature-based) Intrusion Detection Systems (IDS)
It references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature, when we talk about Intrusion Detection Systems (IDS) is recorded evidence of an intrusion or attack. Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts.The disadvantages of Signature-based Intrusion Detection Systems (IDS) are signature database must be continually updated and maintained and Signature-based Intrusion Detection Systems (IDS) may fail to identify unique attacks.

5. A Behavior-based (Anomaly-based) Intrusion Detection Systems (IDS)
It references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.Higher false alarms are often related with Behavior-based Intrusion Detection Systems (IDS).

II. LITERATURE SURVEY

The intrusion detection is very vital in security related applications. Recognizing the mode of attack, intense of act and remedy against flawfull activities are genuine in communication applications. In last decade's most of the researchers identified various intrusions and proposed different solutions for detecting intrusion activities. Some of the recent related works are summarized in the following; In 2014, Ravi Ranjan and G. Sahoo [1] presented a new clustering approach for anomaly intrusion detection by using the approach of K-medoids method of clustering and its certain modifications and proposed a algorithm to achieve high detection rate and overcome the disadvantages of K-means algorithm, such as dependence on initial centroids, dependence on number of clusters and degeneracy. The proposed algorithm had used k-medoids algorithm and its modifications. However, the k-medoids algorithm is also a partitioning technique of clusters that clusters the data sets of n objects into k clusters with apriori. It is found as more robust to noise and outliers as compared to K-means since it minimize a sum of pair-wise dissimilarities using a squared Euclideandistance. The New Medoid Clustering Algorithm is described as follows.
Input: D dataset of n object
Output: Desired set of normal and abnormal clusters.
Begin
Step1: Standardize the dataset in order to make the feature value to appropriate range. This is done because features with greater value dominate the features with lesser value.
Step2: Select initial medoids and for that the formula of Euclidean distance for dissimilarity measure has been used. It is given as under:

$$dist_{ij}=\sqrt{\sum_{b=1}^{y}(z_{ib}-z_{jb})^2} \quad \text{, i=1, 2,....x and j=1, 2,...x} \qquad \text{....eq-1}$$

Let x objects having y variables classifies into c clusters.Compute

$$y_{ij}=\text{dist}_{ij} / \sum_{k=1}^{x} dist_{ik} \qquad \text{....eq-2}$$

After finding yij at each object and sorting them in ascending order, c objects are selected as the initial medoids having minimum value.
Step3: Associate each object to its closest medoid and calculate the optimal value as the sum ofdistances from all objects to their medoids.
Step4: Swap the current medoid in each cluster by the object which minimizes total distance toother objects in the cluster.
Step5: Again associate each object to the closest medoids and compute the new value as in step3.
If the new value is same as previous one then stop the algorithm otherwise repeat step4.
End
Cluster formation is obtained from above algorithm, further each cluster undergoes for an empty cluster check, if an empty cluster is found then those are removed by deletion and hence eliminating degeneracy problem. The most

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

commonly used KDD cup99 data set given by Massachusetts Institute of Technology for intrusion detection is used as an input. The dataset has been standardized to be appropriate for proposed algorithm. Standardization is achieved by following steps:

Step 1: The mean of each feature in the dataset is found using the equation

$$\text{Mean}_f = \frac{D_{1f} + D_{2f} + \cdots D_{nf}}{n} \quad \text{....eq-3}$$

where, D 1 f, D 2 f ,.....D n f are n measuring values of each feature f.

Step 2: The standard deviation of the calculated mean is computed using the equation

$$\text{SD}_f = \frac{1}{n}(|D_{1f} - \text{Mean}_f| + |D_{2f} - \text{Mean}_f| + \ldots |D_{nf} - \text{Mean}_f|) \quad \text{...eq-4}$$

where , D 1 f, D 2 f ,.....D n f are n measuring values of each feature f.

Step 3: The standardized values obtained as:

$$S_{if} = \frac{D_{if} - Mean_f}{SD_f} \quad \text{....eq-5}$$

After getting the standardized value the proposed algorithm generatethe desired clusterand further the cluster is chosento label as normal or intrusions. Then based on parameters detection rates, accuracy and false alarm rate, the proposed algorithm is compared with the existing algorithm for performance analysis.In 2014, Robert Mitchell, Ing-Ray Chen [2] carried a survey of intrusion detection in wireless network applications, and put up an approach of classifying existing contemporary wireless intrusion detection system (IDS) techniques based on target wireless network, detection technique, collection process, trust model and analysis technique and summarized pros and cons of same. They developed a classification tree for intrusion detection techniques for wireless networks to find gaps in IDS research and therefore identify research directions, shown below:

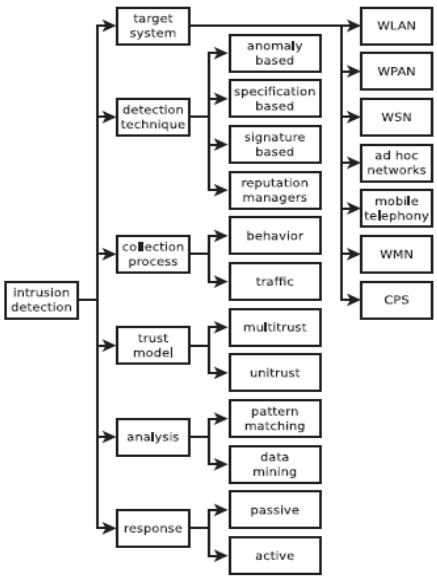

Fig.1. Classification tree

Where, 1.Target system: described the proposed environmentfor the IDS;2. Detection technique: distinguished IDSsbased on their basic approach to analysis;3. Collection process: carried a comparison betweenbehaviour basedIDSs and traffic based IDSs; 4. Trust model: separated IDSs that share rawdata or analysis results from standalone IDSs;5. Analysis technique: for particular implementation simplepattern matching are separated from sophisticated data miningapproaches;meanwhile Detection Technique defined what the IDS looks for and Analysis Technique defined how the IDS looks for it;6. Response Strategy: compared active frompassive response strategies.; further they summarized the pros and cons of specific attributes of targeted wireless networks viz., wireless local area networks (WLANs), wireless personal area networks (WPANs), wireless sensor networks (WSNs), adhoc networks, mobile telephony, wireless mesh networks (WMNs) and cyber physical systems (CPSs) considering approaches

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

like,Signature, Anomaly, Specification, Reputation, Behaviour, Traffic and Multitrust. In 2014, Amrit Pal Singh and Manik Deep Singh[3] focused on two types of intrusion detection systems viz., Network-IDS and Host Based- IDS and their result analysis along with their comparisons.However, Host Based- Intrusion Detection System (OSSEC) is a free open source, performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting and active response. While Network- Intrusion Detection System (Snort) is a lightweight, keep track of packets coming across network and can alert the user regarding ill attacks. A favorable environment is established to test the ability of OSSC (HIDS Tool) and the way it responds to threats by immediate email notification to users,Sending alerts via syslog, sending output to a Database andsending output to prelude. A syscheck and rootcheck is kept on the client machines via the Host machine, to log the results and activity to storage disk. On other side to set up NIDS,a network of four computers via LAN is deployed to exchange ARP, PARP packets. All packets are transmitted between the computers are detected and examined by using Snort in sniffing mode.Snort is made to run from 1 machine to monitor all the packets of the network. While sniffing traffic through snort some packets loss is observed, to keep track of lost packets, successfully delivered packets and possible threats, a pie chart has developed. In fact the packets which were dropped were basically stopped by the snort, as they seem to be threat to the system. Based on pie chart log of successful packets and lost packets, analysis of efficiency of the software is done. On conferring these results and threats, snort generates the alerts by changing the color of the details to the red. In 2014 Pratibha Wage, ChannveerPatil [4], proposed a new Intrusion detection mechanism called EAACK (Enhanced Adaptive ACKnowledgment) an acknowledgement based IDS with the aim of securing Mobile Adhoc Network by detecting threats like false misbehavior report and forge acknowledgement, reducing memory consumption, hardware cost, network overhead when no misbehaviour is detected, safeguarding battery lifetime.Toprevent the attacker from forging acknowledgment packets proposed scheme has adopted the DSA and RSA digital signature algorithms to prevent the nodes from attacks as in EAACK all acknowledgment packets are digitally signed before sending out. EAACK splits into three major parts viz., 1.ACK- an end-to-end acknowledgment schemeassumes malicious acts and switch to S-ACK for detection on not receiving ACK from receiver. 2. S-ACK assures malicious detection; in consecutive node arrangement every third node sends S-ACK to first node. 3.MRA selects an alternate path to the destination if malicious present. Proposed scheme demonstrated positive performance as compared to watchdog and TwoACK schemes. In 2014, Joseph RishSimenthy, AMIE, K. Vijayan[5] introduced an Advanced Intrusion detection System to achieve maximum security against intrusion by adapting Hybrid Intrusion DetectionSystem(HIDS), Energy Prediction based Intrusion DetectionSystem (EPIDS) and Cross layer DetectionSystems. Usingthe Energy Prediction System,the observation made is thatunder attack energyconsumption rate of the sensor nodes is different as compared to the energy consumption rate in normal working condition.This concludes in clear vision that whichever node consuming more power is affected. A notable problem is, even a faulty battery may shows variation in energy consumption which again identified as attack and prone to an alert.So for efficient detection of the intrusion EPS is coupled with HybridIntrusion Detection System. Abnormal sensor nodes are rechecked for the intrusionsusing the Hybrid Intrusion Detection System, fusion of Signature based and Anomaly based intrusion detection Systems. Where, the well-known attacks and the new attack are checked.Ifan attack is detected it is cross checked by the Cross Layer IDS. Up to this level all most all attacks will be detected. In 2015,AbebeTesfahun, D. LalithaBhaskari [6], have presented a hybrid layered intrusion detection system concept for detecting both standalone misuse (anomaly intrusion detection system) and zero-day attacks. Proposed system consists of two layers system that combines misuse and anomaly intrusion detection system. Misusedetector is deployed in first layer to detect and block known attacks anomaly detector is deployed in second layer to detect and block previously unknown attacks.Random forests classifier and bagging technique with ensemble of one-class support vector machine classifiers are adapted to model misuse detector and the anomaly detector respectively. Data pre-processing is done using automatic feature selection and data normalization. Experimental result shows that the proposed intrusion detection system outperforms other well-known intrusion detection systems in detecting both previously known and zero-day attacks. In proposed system,each attributes information are collected and optimal subset of features are selected for classifier. Using some threshold value, selected features are compared with the original feature. On obtaining the relevant features, are forwarded to the misuse intrusion detectorimplemented using random forests classifier. Thisclassifier model consists of training data containing both normal and known attack patterns. It excludes well-known attacks from being reprocessed by the subsequent one-class SVM based anomaly detector. Rest normal patterns are forwarded to anomaly detector module for final decision. Incoming data is preprocessed to enhance the performance of one-class SVM. At the end decisions of each classifier are aggregated to reach final decision on voting. Further, the anomaly detector is adapted to block detected attacks which were considered as normal traffic by the misuse detector. In 2015, S.Yamunarani, D.Sathya, S.Pradeepa[7],had used decision

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

tree technique to improve existing IDS. Further, to detect cross layer attacks they deployed intelligent IDS methods like Back Propagation Network,Bayesian Classification,Support VectorMachines. The main goal is to detect anomaly andmisuse to improve detection rates and accuracy and reduce false positive rate. The proposed method succeeded in detecting sinkholes and sleep deprivation attacks. In 2015, DipaliSuhalalPatil and AtulDusane[8] proposed a system to detect intrusion using anomaly based detection approach able to detect novel or newly generated and unknown attacks by observing a significant deviation in normal behaviour of legitimate user. Proposed IDSused HIDS that integrates misuse detection and anomaly detection techniques to enhance the performance of the intrusion detection as false intrusion alert generation on even internal physical failure is observed by anomaly.

III. CONCLUSION

On surveying few papers focusing on Intrusion Detection I can conclude myself in knowing intelligent IDS methods likeCluster algorithm, classification tree, Network –IDS (Snort), HIDS, EAACK, one class SVM, Back Propagation Network and Bayesian classifier. All methods work towards better detection of Misuse and anomaly behaviours with different approach and aggregation of one or two methods lead to improved performance.

ACKNOWLEDGEMENT

I lend my gratitude to all the respective authors for giving me immense motivation to survey different methods of intrusion detection by retrieving related information from their valuable work. And I extend my gratitude to all those helped me directly or indirectly.

REFERENCES

1. Ravi Ranjan and G. Sahoo, A New Clustering Approach ForAnomaly Intrusion Detection, International Journal of Data Mining & Knowledge Management Process (IJDKP) Vol.4, No.2, March 2014.
2. Robert Mitchell, Ing-Ray Chen, A survey of intrusion detection in wireless network applications, Computer Communications journal,Elsevier, 2014
3. Amrit Pal Singh, Manik Deep Singh, Analysis of Host-Based and Network-Based Intrusion Detection System, I.J. Computer Network and Information Security, 2014, 8, 41-47,2014.
4. Pratibha Wage, ChannveerPatil, "Intrusion-Detection System for Manets: A Secure Eaack", International Journal of Research in Engineering and Technology, eISSN: 2319-1163, pISSN: 2321-7308, 2014.
5. Joseph RishSimenthyCEng , AMIE, K. Vijayan, "Advanced Intrusion Detection System for Wireless Sensor Networks",International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,Vol. 3, Special Issue 3, April 2014.
6. AbebeTesfahun, D. LalithaBhaskari, Effective Hybrid Intrusion Detection System: A Layered Approach, I. J. Computer Network and Information Security, 2015, 3, 35-41, 2015.
7. S.Yamunarani, D.Sathya, S.Pradeepa, "Intelligent Intrusion Detection System In Wireless Sensor Networks", IJARSE, Vol. No.4, Special Issue (01), March 2015.
8. DipaliSuhalalPatil and AtulDusane, "Semantic Host Based Intrusion Detection",International Journal of Current Engineering and Technology, E-ISSN 2277 – 4106, P-ISSN 2347 – 5161, 2015.