ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

Importance of Intrusion Detection System with its Different approaches

Mr. Suresh kashyap[1], Ms. Pooja Agrawal[2], Mr.Vikas Chandra Pandey[3], Mr. Suraj Prasad Keshri[4]

Research Scholar (M.Tech.), Dr.C.V.RamanUniversity, Kargi Road Kota, Bilaspur, India[1]

Research Scholar (Ph.D.), Dr.C.V.RamanUniversity, Kargi Road Kota, Bilaspur, India[2]

Research Scholar (Ph.D.), Dr.C.V.RamanUniversity, Kargi Road Kota, Bilaspur, India[3]

Research Scholar (M.Tech.), Dr.C.V.RamanUniversity, Kargi Road Kota, Bilaspur, India[4]

Abstract: Nowadays it is very important to maintain a high level security to ensure safe and trusted communication of information between various organizations. Intrusion Detection System is a new safeguard technology for system security after traditional technologies, such as firewall, message encryption and so on. An intrusion detection system (IDS) is a device or software application that monitors network system activities for malicious activities or policy violations and produces reports to a Management Station. In this paper, we will look importance of IDS with different approaches. We have presented two types of AI system, both supervised and unsupervised.

Keywords: Firewall, IDS, AI, anomaly & misuse, NID.

I.INTRODUCTION

An IDS (Intrusion Detection System) is a device or application used to inspect all network traffic and alert the user or administrator when there has been unauthorized attempts or access. The two primary methods of monitoring are signature-based and anomaly-based. Depending on the device or application used, the IDS can either simply alert the user or administrator or it could be set up to block specific traffic or automatically respond in some way. The intrusion detection systems didn't have the ability to stop such attacks rather than detecting and reporting to the network personnel.

Signature-based detection relies on comparison of traffic to a database containing signatures of known attack methods. Anomaly-based detection compares current network traffic to a known-good baseline to look for anything out of the ordinary. The IDS can be placed strategically on the network as a NIDS (network-based intrusion detection) which will inspect all network traffic or it can be installed on each individual system as a HIDS (host-based intrusion detection) which inspects traffic to and from that specific device only.

Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them.It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where intrusions detection systems (IDSs) are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyze the security problems so that they are not repeated.IDSs collect information from a computer or a computer network in order to detect attacks and misuses of the system.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

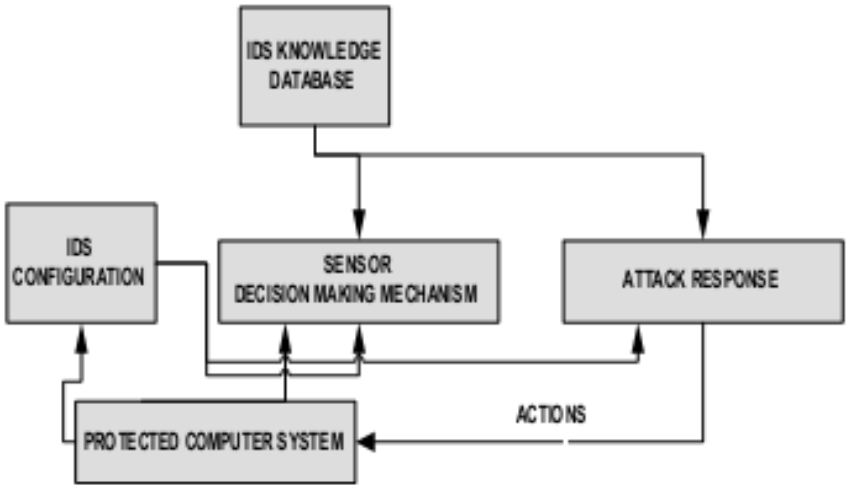

Fig. 1 Intrusion detection system

II.BACKGROUND ON INTRUSION DETECTION

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions. It is very important that the security mechanisms of a system are designed so as to *prevent* unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called **Intrusion Detection**

A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant). The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the "signatures" of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks is further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

Intrusion detection techniques while often regarded as grossly experimental, the field of intrusion detection has matured a great deal to the point where it has secured a space in the network defense landscape alongside firewalls and virus protection systems. While the actual implementations tend to be fairly complex, and often proprietary, the concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack.

III.TYPES OF INTRUSION DETECTION SYSTEM

Intrusion detection system are classified into three types

1. Host based IDS: A host-based intrusion detection system (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse. A host-based IDS analyzes several areas to determine misuse (malicious or abusive activity inside the network) or intrusion (breaches from the outside). Host-based IDSes consult several types of log files (kernel, system, server, network, firewall, and more), and compare the logs against an internal database of common signatures for known attacks. Host-based IDS can also verify the data integrity of important files and executables.

2. Network based IDS: Network-based intrusion detection systems operate differently from host-based IDSes. The design philosophy of network-based IDS is to scan network packets at the router or host-level, auditing packet information, and

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

logging any suspicious packets into a special log file with extended information. Based on these suspicious packets, network-based IDS can scan its own database of known network attack signatures and assign a severity level for each packet.

3. Hybrid based IDS: Hybrid intrusion detection systems offer management of and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide the logical complement to NID and HID - central intrusion detection management.

IV. DIFFERENT APPROACHES OF IDS

In this paper, we will look at four intrusion detection approaches these are

- Artificial Neural Network-IDS
- SOM-IDS
- Fuzzy Logic -IDS
- SVM -IDS

ANN-IDS: -

ANN is one of the oldest systems that have been used for Intrusion Detection System (IDS), ANN is one of the most used techniques and has been successfully applied to intrusion detection (Horeis, 2003; Joo et al., 2003; Kevin, Rhonda, & Jona-than, 1990; Tan, 1995). According to different types of ANN, these techniques can be classified into the following three categories: supervised ANN-based intrusion detection, unsupervised ANN-based intrusion detection, and hybrid ANN-based intrusion detection. Supervised ANN applied to IDS mainly includes multi-layer feed-forward (MLFF) neural networks and recurrent neural net-works .However, the main drawbacks of ANN-based IDS exist in two aspects: (1) lower detection precision, especially for low-frequent attacks, e.g., Remote to Local (R2L), User to Root (U2R), and (2) weaker detection stability (Beghdad, 2008). For the above two as-pects, the main reason is that the distribution of different types of attacks is imbalanced. For low-frequent attacks, the leaning sample size is too small compared to high-frequent attacks. It makes ANN not easy to learn the characters of these attacks and therefore detection precision is much lower.

SOM IDS:-

Purely based on a hierarchy of self-organizing feature maps (SOMs), an approach to network intrusion detection is investigated. Our principle interest is to establish just how far such an approach can be taken in practice. To do so, the KDD benchmark data set from the International Knowledge Discovery and Data Mining Tools Competition is employed. Extensive analysis is conducted in order to assess the significance of the features employed, the partitioning of training data and the complexity of the architecture. Contributions that follow from such a holistic evaluation of the SOM include recognizing that (1) best performance is achieved using a two-layer SOM hierarchy, based on all 41-features from the KDD data set. (2) Only 40% of the original training data is sufficient for training purposes. (3) The 'Protocol' feature provides the basis for a switching parameter, thus supporting modular solutions to the detection problem. The ensuing detector provides false positive and detection rates of 1.38% and 90.4% under test conditions; where this represents the best performance to date of a detector based on an unsupervised learning algorithm.

The Self-Organizing Map is a neural network model for analyzing and visualizing high dimensional data. It belongs to the category of competitive learning network. The SOM Fig. 1 defines a mapping from high dimensional input data space onto a regular two-dimensional array of neurons.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

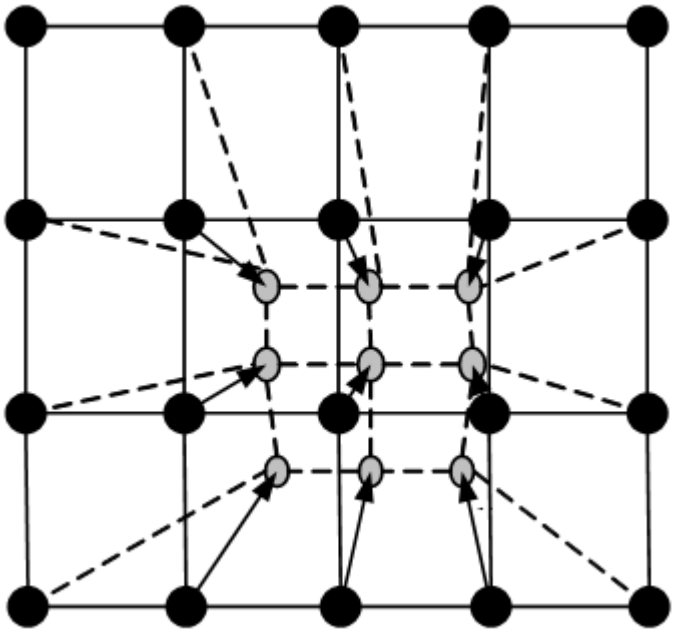

Fig. 2 General SOM topology

Self-Organizing Map has been successfully applied in complex application areas where traditional method has failed. Due to their inherently non-linear nature, they can handle much more complex situations than the traditional methods. One of those problems represents intrusion detection by intrusion detection systems. These systems deal with high dimension data on the input, which is needed to map to 2-dimension space. Designed architecture of the intrusion detection system is application of neural network SOM in IDS systems.

Fuzzy logic IDS:-

Fuzzy systems have demonstrated their ability to solve different kinds of problems in various applications domains. Fuzzy systems based on fuzzy if-rules have been successfully used in many applications areas. Fuzzy if-then rules were traditionally gained from human experts. Recently, various methods have been suggested for automatically generating and adjusting fuzzy if-then rules without using the aid of human experts. Genetic algorithms have been used as rule generation and optimization tools in the design of fuzzy rule-based systems. There are two main reasons to introduce fuzzy logic for intrusion detection. First, many quantitative features, both ordinal and categorical, are involved in intrusion detection and can potentially be viewed as fuzzy variables.

SVM IDS:-

Support Vector Machines (SVM) is the classifiers which were originally designed for binary classification. The classification applications can solve multi-class problems. Decision-tree-based support vector machine which combines support vector machines and decision tree can be an effective way for solving multi-class problems.SVM are learning systems that use a hypothesis space of linear functions in a high dimensional feature space, trained with a learning algorithm from optimization theory. SVM is based on the idea of a hyper-plane classifier, or linearly separability. The SVM is one of the most successful classification algorithms in the data mining area, but it's long training time limits its use. Many applications, such as Data Mining and Bio-Informatics, require the processing of huge data sets. The training time of SVM is a serious obstacle in the processing of such data sets. According to, it would take years to train SVM on a data set consisting of one million records. Many proposals have been submitted to enhance SVM in order to increase its training performance, either through random selection or approximation of the marginal classifier. However, such approaches are still not feasible with large data sets where even multiple scans of entire data set are too expensive to perform, or result in the loss through over-simplification of any benefit to be gained through the use of SVM. Self-organizing maps (SOM) and support vector machine have also been used as anomaly intrusion detectors.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

There are two main reasons for our experimentation with SVMs for intrusion detection. The first is speed because real time performance is of key importance to intrusion detection systems, and any classifier that can potentially outrun neural networks is worth considering. The second reason is scalability: SVMs are relatively insensitive to the number of data points and the classification complexity does not depend on the dimensionality of the feature space.

V.COMPONENTS OF INTRUSION DETECTION SYSTEM

An intrusion detection system normally consists of three functional components.

- EVENT GENERATOR: - It is a data source. Data sources can be categorized into four categories namely Host-based monitors, Network-based monitors, Application-based monitors and Target-based monitors.
- ANALYSIS ENGINE:- This component takes information from the data source and examines the data for symptoms of attacks or other policy violations.
- RESPONSE MANAGER:- In basic terms, the response manager will only act when inaccuracies (possible intrusion attacks) are found on the system, by informing someone or something in the form of a response.

The analysis engine can use one or both of the following analysis approaches:

Misuse/Signature-Based Detection: This type of detection engine detects intrusions that follow well known patterns of attacks (or signatures). Misuse detectors analyze system activities and try to find a match between these activities and known attacks having definitions or signatures introduced to the system beforehand.

Advantages of Misuse-based IDSs:-

- Misuse detectors are very efficient in detecting attacks without signaling false alarms (FA).
- Misuse detectors can quickly detect specially designed intrusion tools and techniques.
- Misuse detectors provide systems administrators an easy to use tool to monitor their systems even if they are not security experts.

Disadvantages of Misuse-based IDSs:-

- Misuse detectors can only detect attacks known beforehand. For this reason the systems must be updated with newly
  discovered attack signatures.
- Misuse detectors are designed to detect attacks that have signatures introduced to the system only. When a well-known attack is changed slightly and a variant of that attack is obtained, the detector is unable to detect this variant of the same attack.
- Misuse-based IDS used in our hybrid IDS is the open-source project Snort. It only looks for the known weaknesses and may not care about detecting unknown future intrusions.

Anomaly/Statistical Detection: An anomaly based detection engine will search for something rare or unusual [26]. They analyses system event streams, using statistical techniques to find patterns of activity that appear to be abnormal. Anomaly detectors detect behaviors on a computer or computer network that are not normal. According to this approach, behaviors deviating from behaviors assumed as ‘‘normal” are thought to be attacks and anomaly detectors compute the deviation in order to detect these attacks. Anomaly detectors construct profiles of users, servers and network connections using their normal behaviors. These profiles are produced using the data that is accepted as normal. After the profile construction, detectors monitor new event data, compare the new data with obtained profile and try to detect deviations. These deviations from normal behaviors are flagged as attacks. Pros and cons of anomaly-based approach are as follows:-

Advantages of Anomaly-based intrusion detection systems

- Anomaly based IDSs, superior to signature-based ones, are able to detect attacks even when detailed information of the attack does not exist.
- Anomaly-based detectors can be used to obtain signature information used by misuse-based IDS.

Disadvantages of Anomaly-based intrusion detection systems

- Anomaly-based IDSs generally flag many false alarms (FA) just because user and network behavior are not always known beforehand.
- Anomaly-based approach requires a large set of training data that consist of system event log in order to construct normal behavior profile.
- This system is that they are highly expensive and they can recognize an intrusive behavior as normal behavior.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

VI. IMPORTANT BENEFITS OF INTRUSION DETECTION DEVICE

Did you know that in Japan the total number of crimes involving the Internet was almost 60% higher in the first half of 2001 than in 2000? Furthermore, Internet fraud has increased by 94%! According to a report mentioned in the Computer Crime and Intellectual Property section, in from 1995 – 2000, Hong Kong witnessed a 26 times increase in cybercrime cases. In 1995, the number of crimes totaled to 14 and in 2000, the crimes had increased to 368. The most popular social media networks see as many as 20 million probes per week! These probes are generally caused due to reasons; such as unauthorized access gained by attackers, malware and authorized users try to get additional privileges. The answer to this is an intrusion detection device.

Intrusion detection device is like a burglar alarm for a computer network. It monitors the flow of traffic and facilitates information systems to deal with the attacks. This system protects your enterprise setup by identifying, logging, reporting and sending alarm whenever there is a probe. The main task of intrusion detection software is to detect attacks and possibly repel them. This article will offer an insight into some of the primary benefits of intrusion detection device.

VII.CONCLUSION

An IDS is a device which is used to inspect all network traffic and alert the user when there has been unauthorized access. There are two primary methods of monitoring these are signature-based and anomaly-based.

This Paper Describe three types of Intrusion detection system. The main goal of this paper is to present different approaches of IDS.ANN and SVM approach belongs to supervised method and SOM and Fuzzy Logic approach belongs to unsupervised method. After study of these approaches we find that hybrid based approaches can overcome the problems which are present in Previous approaches.

REFERENCES

1. S. Northcutt, Intrusion Signatures and Analysis, New Riders, Indianapolis, Indiana, 2001, pp 189-211.
2. Joachims T. “Estimating the Generalization Performance of a SVM Efficiently.” Proceedings of the International Conference on Machine Learning, Morgan Kaufman, 2000.
3. D. Zamboni, “Using Internal Sensors For Computer Intrusion Detection”. Center for Education and Research in Information Assurance and Security, Purdue University. August 2001.
4. R. Graham, “FAQ: Network Intrusion Detection Systems”. March 21, 2000.
5. S. Peddabachigari, Ajith Abraham, C. Grosan, J. Thomas, “Modeling intrusion detection system using hybrid intelligent systems”, Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 114–132
6. M. Saniee Abadeh, J. Habibi, C. Lucas, “Intrusion detection using a fuzzy genetics-based learning algorithm”, Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007,Pages 414-428.
7. Paul Innella Tetrad, “The Evolution of Intrusion Detection Systems”, Digital Integrity,LLC on November 16, 2001.
8. Harley Kozushko, “Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems”, on September 11, 2003.
9. Abraham, A., & Thomas, J. (2005). Distributed Intrusion Detection Systems: A Computational Intelligence
10. Joachims T. “Making Large-Scale SVM Learning Practical.” LS8-Report, University of Dortmund, LS VIIIReport, 1998.

BIOGRAPHY

Ms. Pooja Agrawal received her Master Degree in Computer Science from Guru Ghasi Das University, Bilaspur(C.G.).She Completed her M.Phil In computer science from Dr. C. V. Raman University, Kargi Road Kota,Bilaspur. She is currently pursuing Ph.D. in Computer Science in Dr. C. V. Raman University, Kargi Road Kota, Bilaspur. She is having 10 years of teaching experience. Her Research interest area in Data mining & Software Engineering.

Mr. Suresh Kashyap received his Master Degree in Master Diploma in Computer Science and application from Guru Ghasi Das University, Bilaspur (C.G.).He Completed his M.Phil In Information Technology from Dr. C. V. Raman University, Kargi Road Kota, Bilaspur. He is currently pursuing M.Tech. in Computer Science in Dr. C. V. Raman University, Kargi Road Kota,Bilaspur. He is having 5 years of teaching experience. His Research interest area in Software Engineering.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 5, May 2013

Mr. Vikas Chandra Pandey received his Master Degree in Information Technology from Dr. C. V. Raman University, Kargi Road kota ,Bilaspur(C.G.).He Completed his M.Phil In computer science from Dr. C. V. Raman University, Kargi Road Kota,Bilaspur. He is currently pursuing Ph.D. in Computer Science in Dr. C. V. Raman University, Kargi Road Kota, Bilaspur. He is having 5 years of teaching experience. His Research interest area in Data mining and Networking.

Mr. Suraj Prasad Kesari received his Master Degree in Master Diploma in Computer Science and application from CSVTU Bhilai Raipur(C.G.).He Completed his M.Phil In Information Technology from Dr. C. V. Raman University, Kargi Road Kota,Bilaspur. He is currently pursuing M.Tech. in Computer Science in Dr. C. V. Raman University, Kargi Road Kota,Bilaspur. He is having 5 years of teaching experience. His Research interest area in Software Engineering.