Hybrid Intrusion Detection System: Technology and Development

Megha Gupta
Assistant Professor CSE-Department,
Advanced Institute of Technology and Management,
Palwal, India

ABSTRACT

In current scenario most of the intrusion detection systems (IDS) use one of the two detection methods, misused detection or Anomaly detection, both of them have their own limitations. Technology has developed the technique that combines misuse detection system with anomaly detection system (ADS) or network intrusion detection system and host-based intrusion detection system is known as hybrid intrusion detection .The aim is to increase the detection rate and decrease the false positive rate by the use of misuse detection and anomaly detection. A review on the hybrid IDS is shown in this paper. It shows several main aspects of hybrid Ids and also reviewed some major research in IDS using hybrid approach. A comparative study of performance criterions of different research is also shown in this paper.

Keywords

IDS, HIDS, NIDS, K-Means, Naive –Bayes.

1. INTRODUCTION

With the rapid growth of network technology, a cybercrime has also grown. Today, a wide range of risks and threats against uncontrolled and undefended assets such as database and web server as well as entire network system become the general concern for intruders. Gaining unauthorized access to files, network and any other serious security threat can be detected by use of Intrusion Detection System. IDS identify any activity that breaks the security policy from various areas within computer and network environment. IDS can send early alarm upon risk exposure caused by any attack. It is used to alert the system administrators to execute corresponding result measurements, and to reduce the possibility of bigger losses. A computer-implemented intrusion detection system is a method which is used to monitor a computer system in real-time for actual access by unauthorized persons or computers the system detects unauthorized users attempting to enter into a computer system by comparing user behaviour to a user profile and detects events which indicates an unauthorized entry into the computer system, notifies a control function about the unauthorized users and events that indicate unauthorized entry into the computer system and has a control function that automatically takes action in result to the event. The user profiles are dynamically constructed for each computer user when computer user first try to log into the computer system, the user's profile are dynamically updated. By comparing user behaviour to the dynamically built user profile, false alarms are reduced. An IDS often performs following tasks:

- It will Monitor and analyse user and system activities.
- It can Audit of system structure and fault.
- Recognition activity model mapping known attacks and alert.
- Statistic analysis of abnormal behaviour model.
- It can evaluate the integrity of systems and data files.
- It can Audit tracing management of operating system and recognition of user behaviours disobeyed security policy.

Following are the Performance criterions of measurement of IDS:

- False positives-It is an event which is incorrectly identified as being an intrusion by the IDS when none has occurred.
- False negatives- It is an event that IDS fails to identify as an intrusion when it has in fact occurred.
- Performance impact- It is throughput delay or CPU usage.

2. CATEGORIES OF IDS

There are two types of intrusion detection system

- Host based intrusion system(HIDS)
- Network based intrusion system(NIDS)

2.1 Host- based Intrusion Detection System

A host-based intrusion detection system (HIDS) is an intrusion detection system which is used to monitor and analyse the internals of a computing system .This was the first type of intrusion detection software to have been designed, with the original target system being the mainframe computer where outside interaction was infrequent. A host-based IDS monitors all or parts of the dynamic behaviour and the state of a computer system. A HIDS can detect which program accesses what resources and discover that, for example, a word-spreadsheet has suddenly started modifying the system password database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.

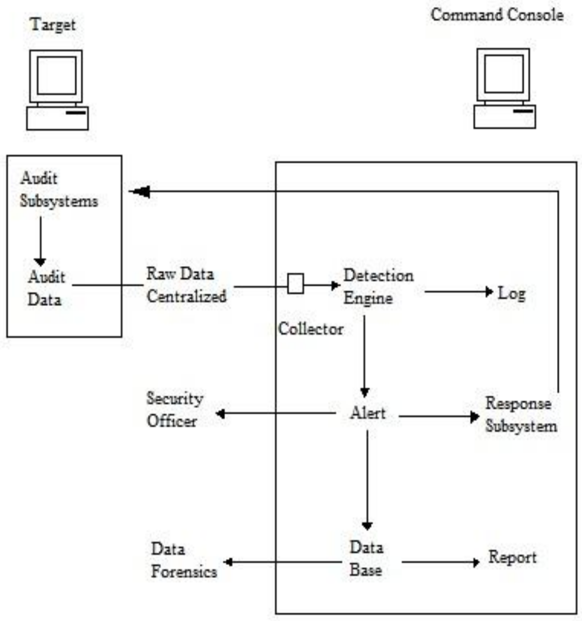

Figure 1: A centralized host based intrusion detection architecture

2.2 Network Intrusion Detection System (NIDS)

A Network Intrusion Detection System (NIDS) is an intrusion detection system that attempts to discover unauthorized access to a computer network by analysing traffic on the network for signs of malicious activity. It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems detect network traffic by connecting to a network hub, network switch configured for port mirroring. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders.

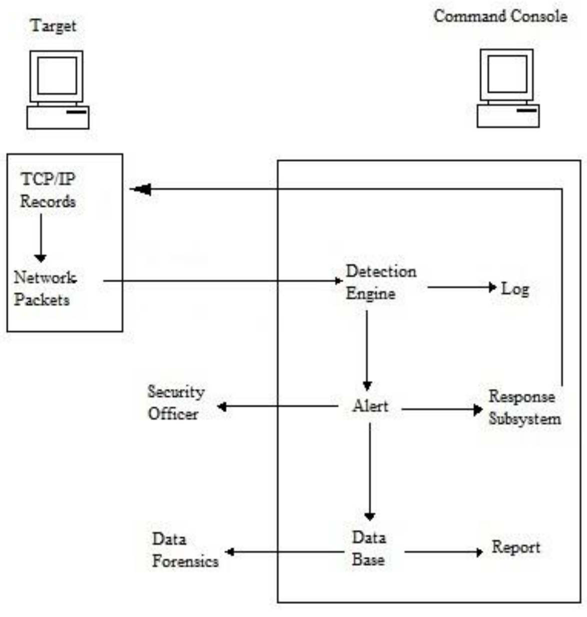

Figure 2: A standard network intrusion detection system architecture

3. INTRUSION DETECTION TECHNIQUES

The techniques of intrusion detection system divide in two categories

- Anomaly intrusion detection
- Misuse intrusion detection

3.1 Anomaly Intrusion Detection

An Anomaly-Based Intrusion Detection System is a system for detecting computer intrusions and classifying it as either normal or anomalous. The classification is done by heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that different from normal system operation [8]. It is unlike from signature based systems which can only detect attacks for which a signature has previously been created. In order to determine what attack traffic is, the system must be learned to recognize normal system activity .one can use another method to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection. Anomaly-based Intrusion Detection does have some disadvantage, namely a high false positive rate and the ability to be fooled by a correctly delivered attack, but it is good technique for known attacks.

3.1.1 Drawbacks

Like every IDS, anomaly detection systems also suffer from several drawbacks

- The first drawback is that the system should be trained to create the appropriate user profiles.
- Another drawback of anomaly detection is complexity of the system and the difficulty of associating an alarm with the specific event that triggered the alarm.
- The last drawback makes it difficult for you to know which attacks will set off alarms unless you actually test the attacks against your network using various user-profiles.

3.2 Misuse Intrusion Detection

Another major technique of IDS is known as *misuse detection*. It is also sometimes known to as *signature-based detection* because alarms are generated based on specific attack signatures [8]. These attack signatures passes specific traffic or activity that is based on known intrusive activity.

3.2.1 Drawbacks

Instead of numerous benefits, misuse detection systems also have some limitations.

- The first drawback is the problem of maintaining state information for signatures in which the intrusive activity encompasses multiple discrete events
- The second drawback is that your misuse detection system must have a signature defined for all of the possible attacks that an attacker may launch against your network.
- Last drawback with misuse detection systems is that someone may set up the misuse detection system in their lab and intentionally try to find ways to launch attacks that bypass detection by the misuse detection system.

4. SOME MAJOR DEVELOPMENTS IN HYBRID IDS

4.1 Hybrid intrusion detection system

Some of the most current intrusion detection system only uses one of the two detection methods, misused detection or anomaly detection both of them have their own limitations, this is the technique which combines misuse detection system and anomaly detection system is known as hybrid intrusion detection system or we can say that the technique [7] which combines the network intrusion detection system and host intrusion detection system is known as hybrid intrusion detection system.

4.2 Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification

A hybrid learning approach is the combination of K-Means clustering and Naïve Bayes classifier [4]. The proposed approach was compared and evaluated using KDD Cup '99 benchmark dataset. The fundamental solution is to separate instances between the potential attacks and the normal instances during a starting stage into different clusters. Therefore, the clusters are further classified into more specific categories, for example Probe, R2L, U2R, DoS and Normal. Hybrid learning approach achieved much reduced false alarm rate with an average below than 0.5%, while keeping the accuracy and the detection rate on average higher than 99%. This approach can classify all data correctly except for attack type U2R and R2L

4.3 Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network

HIDS is used to detect intrusion by CH of CWSN [2]. The proposed HIDS contain both anomaly detection module and a misuse detection module. It is used to filter out a large number of packet records using the anomaly detection module, and second detection can perform with the misuse detection module if the packet is determined to intrusion. Hence, it efficiently detects intrusion and merges the outputs of the misuse detection modules and anomaly detection with a decision making module. HIDS find out intrusion, and tells the type of attack. The output of the decision making module is then send to an administrator for follow-up . it is not only reduces the threat of attack in the system, but also helps user to handle and correct the system further with hybrid detection. In HIDS, the performance of the misuse detection module is evaluated.

4.4 Research and implementation of Snort-based hybrid intrusion detection system

It is used to detect attacks from all the network connection events by combining misuse-based detection method with anomaly-based detection method [1]. The HIDS given in figure 4 contains three sub-modules, anomaly detection module, misuse-based module, and signature generation module. Misuse-based Detection system uses snort as its basis. ADS module is constructed with the help of frequent episode rule mining algorithm. a variation of a priori algorithm is used to design signature generation module. It is implemented under platform known as DebianGNU/Linux. The HIDS performs well in the offline detection and because of this the FER mechanism has good performance in making the relationships between connection events.

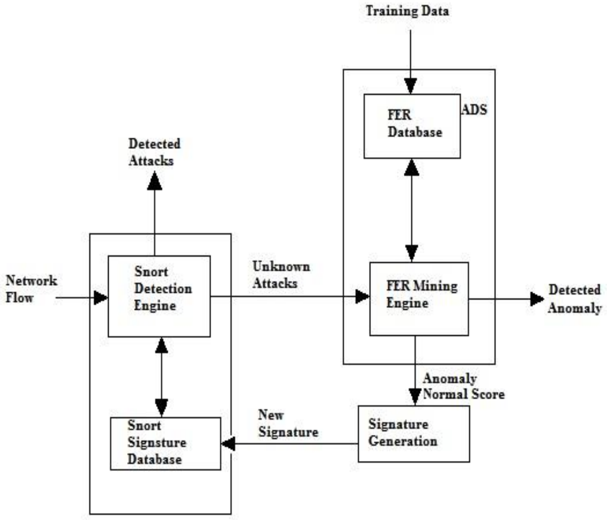

Figure 3: The architecture of snort-based IDS

4.5 Hybrid Network Intrusion Detection

A hybrid intrusion detection system is used to provide increased detection capabilities [6]. HNID integrates a neural network Detection component with a basic pattern matching engine to detect anomalies in the network traffic. This approach efficiently detects known classes of attacks, and also the unknown ones. Since both of the detection solutions run simultaneously so that one can provide a method to filter and group the security alerts to reduce the number of alerts which will be sent to the network administrator.

4.6 Adaptive Network Intrusion Detection System using a Hybrid Approach

Adaptive network intrusion detection is another hybrid approach [5]. In this technique HMM is used for network intrusion detection which performs good empirically on DARPA data set. In this approach HMM based model is combined with Naive Bayesian (NB) based approach to address the issues. Hybrid model include NB model that uses online learning and HMM model for offline learning. The NB model monitor incoming traffic and suspicious flag traffic blocks. The HMM model would be filled with the traffic marked by NB model. Then HMM model would perform source separation for the connections present in the marked traffic and categorized the connections as attack or normal. The HMM model is added to NB model which narrow down the attacking IPs present in flagged traffic instead of improving the attack detection performance. Naturally, the chances of errors can increase when two classifiers are cascaded.

Table 1. Comparison of different hybrid approaches

Approaches	**AC**	**DR**	**FP**	**FA**
KM+NB(K.Means+NaiveBayes)	99.6	99.8	0.09	0.5
CSWN(Cluster Based wireless Sensor Network)	99.75	99.81	N/A	0.57
Snort-Based Hybrid Intrusion Detection Sytsem	N/A	99.3	0.03	N/A

Hybrid Network Intrusion Detection System using netpy	N/A	94.07	N/A	N/A

5. CONCLUSION

In this paper ,we presented an overview of hybrid IDS.we conclude that if we are working on the anamoly based ids then it will generate a large no of false positive and false negative although it can detect unknown attacks but its performance is decreases due to large no of false positive and if we are woking on misuse based ids then it this is impossible to detect unkown attacks.so,to overcome this problem a hybrid ids is developed which uses both anamoly and misuse based ids to find out the unknown attacks and to raise the detection rate and lower false positive and false negative.In this paper we have also presented review of some major research in hybrid ids and the comparison between performance criterion of different hybrid approaches.

6. REFRENCES

[1] YU-XINDING, MINXIAO, AI-wuliu“research and implementation on snort- based hybrid intrusion detection” Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009

[2] K.Q. Yan, S.C. Wang, S.S. Wang and C.W. Liu “Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor” 978-1-4244-5540-9/10/$26.00 ©2010 IEEE.

[3] Yubeinbai, hidestunekobayashi“intrusion detection systems: technology and development “proceedings of 17th international conference on advance information networking and applications (AINA’03)2003IEEE

[4] Z. Muda, W. Yassin, M.N. Suleiman, N.I. Udzir “Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification” 2011 7th International Conference on IT in Asia (CITA)

[5] Rangadurai Karthick, Vipul P. Hattiwale ,BalaramanRavindran“Adaptive Network Intrusion Detection System using a Hybrid Approach” 978-1-4673-0298-2/12/$31.00 �c 2012 IEEE

[6] Cristina Amza, C˘at˘alinLeordeanu, ValentinCristea “Hybrid Network Intrusion Detection” 978-1-4577-1481-8/11/$26.00 ©2011 IEEE

[7] Harley Kozushko “Intrusion Detection: Host-Based andNetwork-Based IntrusionDetectionSystems”DuanyangZhao,QingXiangXu,Zhilinfeng“analysis and design for intrusion detection system based on data mining”978-0-7695-3987-4/10$26.002010IEE

[8] Earl Carter“intrusion detection system”article by cisco press.

[9] Vijayasarathy, R., Ravindran, B.andRaghavan, S.V., A system approach tonetworkmodeling for DDoS detection using a Naive Bayesian classifier,COMSNETS, 2011.