Indian Journal of Science and Technology, *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/80108, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Intrusion Detection Systems, Tools and Techniques – An Overview

S. N. Sheela Evangelin Prasad[1]*, M. V. Srinath[2] and Murtaza Saadique Basha[3]

[1]Department of Computer Science and Engineering, Sri Krishna Engineering College, Chennai – 601301, Tamil Nadu, India; samefren@gmail.com
[2]Department of Master of Computer Applications, Sengamala Thayaar Educational Trust Women's College, Thiruvarur – 614001, Tamil Nadu, India; sri_induja@rediffmail.com
[3]Department of Master of Computer Applications, C. Abdul Hakeem College of Engineering and Techology, Melvisharam – 632509, Tamil, Nadu, India; m_s_basha76@yahoo.co.in

Abstract

Organization's crucial data are highly endangered due to several security attacks and threats. Intrusion is one among such type of threat. Intrusions are efforts that attempt to elude normal security mechanisms of computer system. Intrusion detection is the process of monitoring and analyzing the events arising in a computer network to identify security breaches. Intrusion Detection System is the most important tool in maintaining network's security. This paper provides an overview of Intrusion Detection System and helps reader gain some fundamental concepts and methodologies used by IDS. This paper also provides discussion about types of IDS, approaches and types of attacks in the network and intensive literature survey. Finally, comparison of several IDS methods with merits and demerits are also presented in the paper.

Keywords: Attacks, DoS, IDS, Intrusion, Misuse Detection, Network Security

1. Introduction

As network technology is rapidly increasing, internet has become a common means of communication for most of the organizations. Because of this change, there are lot of problems that have been faced by many organizations to secure their valuable resources and vital information in network. A number of attacks have been reportedly observed in many networks. Intrusion is one such attack.

Intrusion is an act of accessing data and using computer resources without privileges, thus causing incidental damage and security breach[1]. Intrusion detection is the process of monitoring and analysing the events occurring in a computer or network and to identify security breaches, i.e. the process of detecting events with intrusive behaviour. Intrusion Detection System (IDS) analyses the network traffic and identifies activities that violates the security policy of computer and network[2]. It also alerts the system or network about the threat it has been detected.

Intrusion Detection System analyses the operations of firewall, routers, servers and crucial files for intrusions. Though the primary objective of IDS is to detect intrusions, it also bound to provide the following services:

- Audit the system configuration and vulnerabilities.
- Evaluating the integrity of network, hardware and files.
- Tracking anomalies.
- Observing and analysing network and system activities.
- Providing user friendly interface for security management.

*Author for correspondence

2. Types of IDS

Intrusion Detection Systems are broadly classified into two main categories: Host based Intrusion Detection Systems and Network based Intrusion Detection Systems. Host based IDS takes care of single system. Agents are used which monitors the system activities like integrity of the system, applications activities, network traffic, file operation, file modification, operating system activities, etc. and a log file is created to record the above actions[3]. Host based IDS analyses the log file for any unauthorized access, change, activity and if found, it alerts the system by sending pop-up messages, blocks the activity and inform to management server. The decision to alert, block and inform about the intrusion is based on the type of security policy imposed by the local system. These types of Intrusion Detection Systems are installed in a single host[3].

Network based Intrusion Detection System monitors the network and protect from unauthorized access. Here also, the activities of the network are recorded in a log file and IDS analyses this file to detect threats and anomalies. Network based IDS detect attacks like DOS attacks, root attacks, etc. Network based IDS is implemented in such a way that all the network traffic enters and leaves via this system[4]. Network based IDS is fixed on the boundary of network or on a network segment to monitor all the network traffic. It examines traffic and checks packet real time or near real time parameter to detect intrusions. The procedure of Network based IDS are called active components whereas for Host based IDS, it is said to be passive components. Combination of Network based IDS and Host based IDS, called hybrid intrusion detection system, is used currently in many network environments. It provides high flexibility and more security[4].

3. Intrusion Detection Approaches

Intrusion Detection System employs variety of techniques to detect intrusions. IDS uses single or combination of techniques to detect intruders. The techniques include anomaly detection, misuse detection, target monitoring and stealth probes.

3.1 Anomaly Detection

This technique stores normal behaviour such as network packet information, software running information, system long events, operating system information, kernel information, etc. Whenever there is a difference in the above parameters, anomaly is detected and alarm is generated. Anomaly detection is useful for fraud detection, network based intrusion and other unusual activities on the system[5]. Anomaly detection, also referred to as behaviour based detection, identifies deviations of the system from normal behaviour. This method is having the ability to detect new and unknown attacks by analyzing audit data. But this method is having high false alarm rate. Sometimes legitimate system behaviours may also be categorized as anomalies and flagged as intrusions.

3.2 Misuse Detection

This technique stores sequence of patterns, attack signatures, intrusion patterns, etc in the database. The system events are matched with stored information. If a match is found, the system generates the alarm. Since this method compares signatures, it is sometimes referred to as signature-based detection. These techniques automatically update their database on different input data to include new type of attacks[6]. Misuse detection techniques have high degree of accuracy in detection known attacks and its variants. But these techniques cannot detect unknown intrusions as they depend on signatures.

3.3 Target Monitoring

This technique searches for modification on specific files and does not detect anomalies. It works like a corrective control that restores file after the file has been modified by the intruder. It uses cryptographic hash computing to restore the modified contents. This technique is easy to implement as constant monitoring of traffic by the administrator is not needed[7]. Sending alarm to the network or to the system is done when there is a data check sum mismatch. Check sum calculation can be computed at different intervals.

3.4 Stealth Probes

This technique detects intruders who stay in the network for a long period of time. Generally attackers check for system vulnerabilities and open ports for a long period and wait for another long period to attack[8]. Stealth probe technique checks for any such methodological attacks by collecting wide variety of data about the entire system. Stealth probe technique requires large amount of

samples – samples collected from different machines and networks to discovery attacks. For this, it combines both anomaly detection and misuse detection.

4. Types of Attacks

Though the common objective of an attacker is to intrude into the system or network and gain access, these intrusions are classified based on the way they are performed. Moreover, intruders can be within the network called inside attackers or from outside the network called outside attackers. These attackers generally use internet as the common means to intrude. Several types of attacks are:

4.1 Denial of Service (DoS) Attack

Making resources like computing, memory, too busy so that legitimate users can be denied for their request is the main objective of DoS attack[9]. DoS attack artificially makes server or network too busy thus making these resources unavailable to users. There are two types of DoS attacks viz. flooding and flaw exploitations. Flooding targets resources using external communication requests. For example, sending PING command many number of times to the network thus overwhelming the network. Another example of flooding attack is sending SYN requests to a server for handshaking process but never sends the ACK. Flaw exploitation attack causes the system or network to crash. Here the attacker sends an input message that takes advantage of bugs in the target machine and crash or destabilizes the system so that it cannot be accessed[9]. Variant of DoS attack is Distributed Denial of Service (DDoS) attack that causes multiple systems to collapse simultaneously.

4.2 User to Root (U2R) Attack

Attacker gets username and password maliciously and gets access to the system as a normal user. After gaining access, the attacker exploits some vulnerability to get root access of the system thereby becoming the administrator[10]. Different types of U2R attacks are available and buffer overflow attack is the most common among them. When a program copies too much of data to predefined buffer, buffer overflow occurs.

4.3 Scan Attack

Ports are little doors through which traffic enters and leaves the system and network. TCP and UDP are the two protocols that uses ports for communication. An attacker scans to check for the open ports with a listening service. Attacker sends the packet to these open ports[11]. The attacker can find services running on that machine, type of operating system running, etc. by using the packet. Port scanning attack also let intruders to know what are the hosts up on a network and various network details such as topological data, IP address, MAC address, router and gateway filtering schemes, firewall rules imposed, etc.

4.4 Eavesdropping Attack

Here the attacker monitors other people's communication in an unauthorized manner. It can be listening telephone calls, viewing emails and messages and other internet services[12]. Eavesdropping attack is hard to detect since it does not affect the normal operation of network. Since it is hard to detect, eavesdropping is generally the biggest problem most of the administrators face in an enterprise. By using strong encryption schemes, the data can be protected from eavesdropper.

4.5 Man-in-the-Middle Attack

Here the attacker maliciously intercepts in a conversation between two parties and impersonates them thereby gaining access to the vital information. The two parties feel that they are directly communicating with each other even though attacker has intercepted in the middle[13]. Man-in-the-middle attack is a greatest threat to online security because it gives the attacker capability to capture and modify sensitive information in real-time transactions. The attacker can also exploit vulnerabilities to the network security configurations. Man-in-the-middle attack takes the form of session hijacking, side jacking, evil twin and sniffing[13].

Oludele Awodele et al.[14] proposed a multi-layered approach to the design of intelligent intrusion detection and prevention system. The proposed method consists of three different layers viz. the file analyzer layer, system resources layer and connection layer. File analyzer layer monitors important files and folders of interest from any type of intrusion. Important files and folders are selected by the administrator and supplied to file analyzer so that it can monitor for only these files. System resources layer periodically scans the system log files for new entries. Values of entries are compared with threshold value set by the administrator. By this way, the proposed method

safeguards the system resources from intrusions. Connection layer allows physical and logical connection between two entities. This layer monitors for any intrusion in connections to the local machine and network. All the three layers are capable of detecting anomalies and misuses. The multi-layered approach prevents and detects intrusions and avoids activities like tampering of important files, unauthorized connection, unauthorized permissions, etc.

Yu Lasheng and Mutimukwe Chantal[15] presented an Agent Based Distributed Intrusion Detection System (ABDIDS). Autonomous and cooperative agents are assigned the duty of detecting intrusions. Three types of agents such as monitory registry agents, monitoring agents and managing agents are used which cooperates with each other in detecting intrusions. Monitory registry agents initialize and identify monitoring agents. It also provides details about current status of each monitoring agent. Monitoring agents collects data pertaining security of nodes and transmit to managing agents. Managing agents process data and detect intrusions.

Jaisankar and Kannan[16] presented hybrid intelligent based Intrusion Detection System. Three different types of agents such as feature selection agent, validation agent and decision making agent are used. Feature selection agent selects required features of IDS using rough sets. Selected features are validated and passed to hybrid model by validation agents. In order to distinguish between normal and abnormal behaviour, decision making agents are used. The final decision is taken by decision manager which identifies the intruders. Three classifiers viz. EC4.5, SVM and hybrid model are used which provides better detection rate.

M. Laureno et al.[17] presented host-based intrusion detection through virtual machines. Virtual machines are more preferable than computing systems because of cost and portability. This method monitors guest actions through Intrusion Detection System which is external to virtual machine. Virtual Machine Monitor sends data to IDS. The detection system is secure and cannot be accessed by intruders. This method also tracks the activities of isolated processes. Response module restricts the execution of isolated process without disturbing genuine users. The system needs additional work to improve the performance of current IDS and response mechanism. Improper interface to interact with kernel to allow, kill and suspend a process is also a drawback of this method.

Garth Crosby et al.[18] presented location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks. The method first develops reputation and trust so that each device in wireless sensor network can determine whether other devices have been compromised or not. If it is compromised, necessary corrective action is initiated using negative information sharing and independent trust-based decision making. The paper also provides simple location verification algorithm that utilizes received signal strength information. Compromised node detection rate is good when 15 or less number of nodes are available. When there is an increase in number of nodes, compromised node detection rate decreases.

Khan et al.[19] proposed new Intrusion Detection System using Support Vector Machines and hierarchical clustering. The proposed method gives more importance to detect anomalies than misuse detection. Support Vector Machine (SVM), one of the most accurate classifier, is used with less training time. If the data is large, Dynamically Growing Self-Organizing Tree (DGSOT) algorithm is used for clustering since DGSOT provides several advantages over traditional clustering algorithm. The method is highly accurate, having less false positive and false negative rates.

Yihua Liao and V. Rao Vemuri[20] presented Intrusion Detection System using k-nearest neighbour classifier. System calls are analyzed to detect intrusion in this method. Separate database for short system calls are built for different programs. The frequency of occurrence of a system call is used to describe program's behaviour. All the system calls are considered as tuples of a database. For an unknown tuple, k-nearest neighbour searches for patterns closest to unknown tuple. Here the tuples are classified by majority votes of its neighbours. With the combination of statistical schemes, intrusions are detected. To perform above tasks, huge computations and storage are required. Efficiency can be achieved by implementing the algorithm in parallel hardware.

Dewan M. Farid et al.[21] presented a paper on adaptive intrusion detection by combining Naïve Bayesian Classifier and decision tree. The problem with traditional learning algorithms in IDS is poor false positive rate. Combination of Naïve Bayesian Classifier and decision tree based learning performs better balance detection and false positive rates. This method also detects various types of attacks and removes duplicate attributes in training set. The method is having higher detection rate with great

accuracy. This method is tested on KDD99 data set and it has detected intrusions with 99% accuracy with minimized false positives.

R. Shanmugavadivu and N. Nagarajan[22] presented paper on Intrusion Detection System using fuzzy logic. Most of the Intrusion Detection Systems rely on broad knowledge of various attacks so that the machine is capable of handling any environment. This dependency is minimized in this paper by using fuzzy-logic which effectively identifies abnormal activities in a network. The accuracy is achieved since the rule base contains set of better and updated rules. Rule base is constructed by mining single length frequent items from attacks and normal data. Then, indistinct rules are selected and supplied to fuzzy system for test data classification.

Emma Ireland et al.[23] presented a paper on intrusion detection using combination of genetic algorithm and fuzzy logic. First the method randomly generates rules and quality of the rules are improved by using fuzzy genetic algorithm during training phase. Each feature in a record is matched with block of rules. Parameters of each block are used to compute attack's degree of certainty by applying trapezoidal fuzzy rule. Sum of certainty of each block are compared with administrator fixed threshold value to categorize an event as attack or normal behaviour. This fuzzy genetic algorithm detects unknown attacks than traditional genetic algorithms. This method is highly effective in detecting denial of service attacks.

5. Comparison of various Intrusion Detection Schemes

Table 1. Comparison of various IDS methods

Title	Authors	Description	Advantages	Disadvantages
A multi-layered approach to the design of Intelligent Intrusion Detection and Prevention System (IIDPS)	Awodele, Oludele, et al.	Signature based intrusion detection scheme with three layers performing different functions	Strong detection and prevention rate	Huge memory and time is required
Agent Based Distributed Intrusion Detection System (ABDIDS)	Lasheng, Yu and Chantal	Autonomous and cooperative agents detect intrusions. Three types of agents are used	Low false alarm rate and performance is better than traditional Intrusion Detection System	No description about security issues of mobile agents
A Self-organized Agent-based architecture for Power-aware Intrusion Detection in wireless ad-hoc networks.	Srinivasan T, Vivek Vijaykumar and R. Chandrasekar	Decision manager is used to take final decision about normal and abnormal behaviour	Using three classifier increases the detection rate. It is better than PROBE and R2L	Time complexity is high as three classifiers are used
Protecting host-based intrusion detectors through virtual machines	Laureano Marcos, Carlos Maziero and Edgard Jamhour	Virtual machine monitors the network traffic and sends data to IDS	IDS is implement with low as virtual machines are cheap	Unable to detect anomalies behaviour
Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks	Crosby Garth V, Lance Hester and Niki Pissinou	Detects and isolates compromised nodes in wireless sensor networks	Uses reputation based monitoring to detect and isolate malicious node Location aware IDS increases integrity	Extension is needed for location verification protocol
A New Intrusion Detection System using Support Vector Machines and hierarchical clustering	Khan Latifur, Mamoun Awad and Bhavani Thuraisingham	Support vector machines and hierarchical clustering is used to detect both anomalies and misuses	Accurate and able to model complex non-linear decision boundaries.	Kernel choice is difficult High algorithmic complexity and excess memory is required Speed of training and testing data is slow

Use of k-nearest neighbor classifier for intrusion detection	Liao Yihua and V. Rao Vemuri	Use of k-nearest neighbour algorithm enhances classification	Highly adaptive behaviour and easy for parallel implementations	Memory requirements are high and susceptible to cure of dimensionality
Combining Naive Bayes and decision tree for adaptive intrusion detection	Farid Dewan Md, Nouria Harbi and Mohammad Zahidur Rahman	Use of naïve bayes classifier minimizes false positive rates with higher accuracy	Method is fast and accurate even on large databases	Assumptions on class conditional independence. Lack of available probability data
Network Intrusion Detection System using fuzzy logic	Shanmugavadivu R and N. Nagarajan	Rule base is constructed by mining single length frequent items from attacks and normal data	Rule base can be easily modified Conflicting objectives can be reconciled	Difficulty in developing fuzzy model from fuzzy system Fine tuning is needed before simulation
Intrusion Detection with Genetic Algorithms and Fuzzy Logic	Emma Ireland et al.	Improved rules are used for detecting anomalies	Various data sets are used and false positive, false negative rates are minimal	No constant optimization of response time

7. Conclusion

Undoubtedly intrusion has become a dangerous threat to many organizations in safeguarding their vital information and resources. Various Intrusion Detection Schemes are surveyed in this paper. All the methods discussed try to detect intrusion in one way or another. But attackers are capable of discovering new techniques and ways to break security policies. From the literature, it is evident that many IDS techniques depend on high time, memory and cost requirements apart from advantages. For example, Network Intrusion Detection System using fuzzy logic[22] detects intrusion using rule base with high accuracy. But designing fuzzy model and fine tuning is a tedious job. Few methods also have higher false alarm rate. Hence any Intrusion Detection System must have high accuracy, low false positive and false negative rates with low computational, time and cost overheads.

8. References

1. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011 Jan; 34(1):1–11.
2. Zhang Y, Lee W, Huang YA. Intrusion detection techniques for mobile wireless networks. Wireless Networks. 2003 Sep; 9(5):545–56.
3. Akyildiz IF, Xie J, Mohanty S. A survey of mobility management in next-generation all-IP-based wireless systems. IEEE Wireless Communications. 2004 Aug; 11(4):16–28.
4. Srinivasan T, Vijaykumar V, Chandrasekar R. A self-organized agent-based architecture for power-aware intrusion detection in wireless ad-hoc networks. International Conference on Computing and Informatics. ICOCI'06. IEEE; 2006. p. 1–6.
5. Garcia-Teodoro P, Diaz-Verdejo J, Marcia-Fernandez G, Vazquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers and Security. 2009 Feb-Mar; 28(1-2):18–28.
6. Wang K, Salvatore J, Stolfo SJ. Anomalous payload-based Network Intrusion Detection. Recent Advances in Intrusion Detection. Springer: Berlin Heidelberg; 2007. p. 203–22
7. Bose A, Hu X, Shin KG. Behavioral detection of malware on mobile handsets. Proceedings of the 6th International Conference on Mobile Systems, Applications and Services. ACM; 2008. p. 225–38
8. Qu Y, Lu Q. Effectively mining network traffic intelligence to detect malicious stealthy port scanning to cloud servers. Journal of Internet Technology. 2014 Sep; 15(5):841–52.
9. Sisalem D, Kuthan J, Ehlert S. Denial of service attacks targeting a SIP VoIP infrastructure: Attack scenarios and prevention mechanisms. IEEE Network. 2006 Sep-Oct; 20(5):26–31.
10. Luo M, Peng T, Leckie C. CPU-based DoS attacks against SIP servers. IEEE Network Operations and Management Symposium, NOMS 2008; Salvador, Bahia. 2008 Apr 7-11. p. 41–8.
11. Kim J, Lee JH. A slow port scan attack detection mechanism based on fuzzy logic and a stepwise policy. 4th International Conference on Intelligence Environments; Seattle, WA. 2008 Jul 21-22. p. 1–5.

12. Zhang Z, Li Y, Man ZX. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. Physics Letters A. 2005 Jun; 341(5-6):385–9.
13. Desmedt Y. Man-in-the-middle attack. Encyclopedia of Cryptography and Security. Springer: US. 2011. p. 759–9.
14. Awodele O, Idowu S. A multi-layered approach to the design of Intelligent Intrusion Detection and Prevention System (IIDPS). Issues in Informing Science and Information Technology. 2009 Jan; 6(1):631–47.
15. Lasheng Y, Chantal M. Agent Based Distributed Intrusion Detection System (ABDIDS). Second Symposium International Computer Science and Computational Technology (ISCSCT'09); 2009 Dec 26-28. p. 134–8.
16. Srinivasan T, Vijaykumar V, Chandrasekar R. A self-organized agent-based architecture for power-aware intrusion detection in wireless ad-hoc networks. International Conference on Computing and Informatics, ICOCI'06; IEEE; Kuala Lumpur. 2006. p. 1–6.
17. Laureano M, Maziero C, Jamhour E. Protecting host-based intrusion detectors through virtual machines. Computer Networks. 2007 Apr; 51(5):1275–83.
18. Crosby GV, Hester L, Pissinou N. Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks. International Journal of Network Security. 2011; 12(2):107–17.
19. Khan L, Awad M, Thuraisingham B. A new Intrusion Detection System using Support Vector Machines and hierarchical clustering. The VLDB Journal - The International Journal on Very Large Data Bases. 2007 Oct; 16(4):507–21.
20. Liao Y, Rao Vemuri V. Use of k-nearest neighbor classifier for intrusion detection. Computers and Security. 2002 Oct; 21(5):439–48.
21. Farid DM, Harbi N, Rahman MZ. Combining Naive Bayes and decision tree for adaptive intrusion detection. International Journal of Network Security and its Applications. 2010; 2(2):12–25.
22. Shanmugavadivu R, Nagarajan N. Network Intrusion Detection System using fuzzy logic. IJCSE. 2001; 2(1):101–11.
23. Ireland E. Intrusion detection with genetic algorithms and fuzzy logic. UMMC Sci Senior Seminar Conference; Morris, MN. 2013. p. 1–30.