DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4771

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY ON ATTACKS AND APPROACHES OF INTRUSION DETECTION SYSTEMS

Gaurav Agrawal
Research Scholar in CSE Department
Radharaman Institute of Technology and Science,
Bhopal, INDIA

Shivank Kumar Soni
Assistant Professor in CSE Department
Radharaman Institute of Technology and Science,
Bhopal, INDIA

Chetan Agrawal
Head of CSE Department
Radharaman Institute of Technology and Science,
Bhopal, INDIA

Abstract- Now a day's information of an organization floating over the internet that increases the traffic on the network, heavily uses of the internet give rise in traffic on the network as well as made the network data vulnerable. All this happened because of easy to access the data on the internet. So we needed a security mechanism to protect the sensitive data over the network. For protecting that information Intrusion Detection System (IDS) is placed in the system. IDS is a software or hardware device that deals with attacks by collecting information from a variety of system and network sources, then analyzing the symptoms of security problems. Network Intrusion Detection (NID) is an Intrusion Detection mechanism that attempts to discover unauthorized access to a computer network by analyzing traffic on the network. Host based Intrusion Detection (HID) analyses the user activities and decides that the user is authorized or not. There are lots of ways to implement an IDS system, and it depends on the usage of the systems or the requirements of an organization. This paper describes some or all of the main techniques to implement IDS. This paper aims towards the proper survey of intrusion detection system, the attacks and techniques to implement IDS, so that researchers can make use of it and can find the new techniques or ways to efficient implementation of IDS.

Keywords- Intrusion Detection System, Data Mining, Pattern Matching, Anomaly detection & Misuse detection, Machine Learning

I. INTRODUCTION

In our daily life we do some work on the internet like making payment of bills, do the shopping etc. All of these types of activities include money exchange, transferring of critical information over the network. And the networks are vulnerable to attacks, so we must need a security mechanism that can protect our system from threats or intrusions. Intrusions are the activities that violate the security policy of the system or intrusions are the set of rules that meant to compromise the system's integrity, confidentiality and availability of any resources in a computing platform [1]. Intrusion Detection System (IDS) is a device or software application that monitors the network or system for malicious activities, or policy violation and produce reports to management station where it is analyzed for further prevention and detection. The objective of IDS is to monitor network assets in order to detect misuse or anomalous behavior [2]. IDS system deals with the fast detection of an intrusion by comparing or matching the attack patterns from a normal to abnormal behavior. An IDS dynamically monitors the system events and decide whether the use of the system is legitimate or symptomatic of an attack. It also maintains the historical records of a user activity and attack signatures. Based on these records IDS will detect the threats in the future and can prevent the system from them.

Generally, IDSs do not act or take operative action when an intrusion detected, IDSs usually do report the system administrator about the intrusion. An IDS is a watchdog that alerts the administrator whenever any suspicious activity detected. Usually it is the system administrator who takes an action on the intrusions that is raised by IDS.

This paper consists of 7 sections. Section 1 describes the intrusion detection system. Its techniques and its very basic architectural model are described in Section 2. Section 3 describes the target of IDS, types of IDS approaches, security functions and measures of IDS. Various types of attacks to the network are described in section 4. Section 5 describes different approaches to IDS. Section 6 having a comparative analysis of different IDS approaches, and section 7 has concluded remarks.

II. GENERIC MODEL OF IDS

A generic model of IDS is shown in Figure 1. Typically, IDS uses the information available in system configuration data, audit storage and previously known attacks (reference data). The IDS can be placed in the system. It can be located in target system or external to it. In former case if the target system is compromised the IDS can also be invaded, in the latter case it IDS can be safe. IDS may use actionable information that is running in the system for reducing the detection time. On detecting anomalous IDS sends alarm to Site Security Officer (SSO) [1]. For detection of anomaly we set the baseline for normal behavior in IDS. For detection of true intrusion it is crucial to set the baseline of normal behavior in IDS, because if it not so system may generate false alarms.

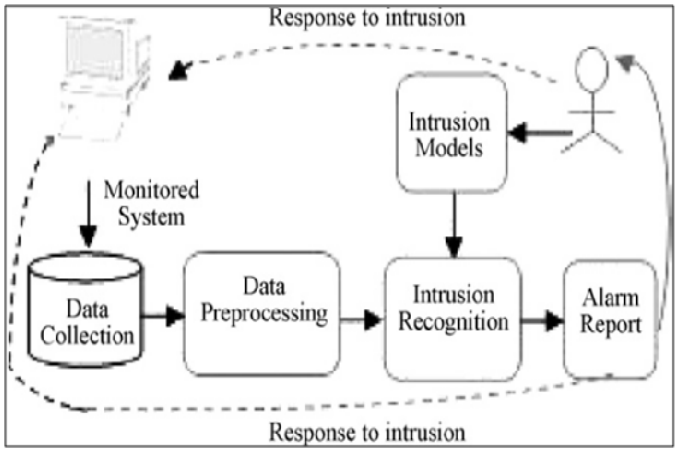

Figure 1. Generic Model of an Intrusion Detection System

III. TRADITIONAL INTRUSION DETECTION SYSTEM

Intrusion detection system is a prime area in the field of network security and research area also. Many researchers have proposed their methods to protect the system from the attacks. In this section we will see the typical types of intrusion detection systems based on audit information and its place in the system (host or network).

A. Target of IDS

There are basically two places where we can put our IDS, and also we can classify IDS based on source of audit information in two types as well [3]. There is another (third) type of IDS which is made by merging both of the techniques.

Host based Intrusion Detection System (HIDS)

It refers to intrusion that take place on a single host system. This type of IDS gets it audit data from host audit trails and monitors activities such as file changes, integrity of system, system logs and host based network traffic. When any suspicious activity found by IDS, it alerts the system administrator or alert the central management server. Server or user or both can block the user request, this judgment is based on the mechanism installed in the local host system.

Network based Intrusion Detection System (NIDS)

It is used to monitor the network traffic to protect the system from network based threats. It gets its data from monitoring the network traffic by using sensors and keeps the records in its defined format in the system log. It tries to detect malicious activity like Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS).

Hybrid based Intrusion Detection System

In this type of IDS we merge both of the techniques to provide better detection of intrusive activity wherever held in the system or on the network. It overcomes the drawbacks of both of the techniques as well as provides better security to both hosts and networks. Apart from that it is sometimes difficult to make both techniques to interpolate with each other and do both functions efficiently, so it is a difficult task to manage both the detection activities in a single IDS system.

B. Detection Approaches

There are basically two ways by which we can find the intrusion or intrusive activity performed by any unauthorized user [4]. First, we can track the activity of a user and decide whether his/her operations or activities are normal or abnormal and second we can provide known normal activities (signatures) to the system so that IDS can compare and decide that the user is authorized or not.

Anomaly Detection

It refers to the technique which is used to detect the malicious activities based on deviation from normal behavior. These activities are considered as an attack on the system. It can also detect the unknown intrusions. All this can happen because we can train this type of IDS for unknown abnormal behavior. For training set we can use the system logs of past activities, database of normal and abnormal behavior, and system configuration files. The detection rate of anomaly based IDS are high, but it also generates false alarms proportionally.

Misuse Detection (or Signature-based Detection)

Misuse detection or Signature-based detection mainly depends on identifying known signatures. It means in this system we first need to determine the normal behavior of the user, based on that IDS can define an activity as a normal or a threat to the system. So, this IDS system is used only for detecting known attacks (intrusions). The drawback of this system is that, a slight modification in activity can lead the system to not to generate the alarm, it can or cannot be a malicious activity. The detection rate of these IDS is low, but it generates very low false alarms.

C. Security Functions provided by IDS

IDS provide a lot of security functions, but there are three basic and most security functions that have to be provided by every IDS [3], and they are:

Data Confidentiality

It checks whether data/information stored in the system is secure or vulnerable to attack. It is the required security function because sometime system uses the sensitive information.

Data Availability

It checks whether the information is available to the authorized user or not. Sometimes the valid user cannot access the system information because of a DOS attack, so IDS should be tough against the DoS attacks. Again, this is a very required security check.

Data Integrity

It ensures that data is consistent and correct throughout the life cycle of an event. The data should not be changed in between of an event and also a valid/authorized user can have rights to change the data.

D. Alert Types

There are four types of alerts that are generated by IDS in terms of alarm generation and its trueness [5].

- True Positive (TP): It signals an alert when an attack has taken place.

- False Positive (FP): It signals an alert when there is no attack on the system.
- False Negative (FN): It does not produce a signal when an attack has taken place.
- True Negative (TN): It signals, no alert and no attack on the system.

E. Measures of IDS

Measures of IDS define how much a system is efficient and strong against intrusive activities [5]. There are lots of points which measure the IDS efficiency, but we brief three main measures, and they are:

Accuracy

Accuracy is measured by the ratio between the correctly classified instances to the total number of samples present in the dataset. It defines that how much an IDS is accurate against the intrusion detection and capable of generating true alarms when a genuine attack has taken place.

Attack Detection Rate

The attack detection rate is the ratio between the total attacks detected by the IDS to the total attacks present in the dataset. The detection rate shows that how many an IDS is efficient in detecting intrusions.

False Alarm Rate

It is the ratio between incorrect instances of the total number of normal instances present in the dataset. False alarm is the alert when there is no attack on the system, so the false alarm rate should be as low as possible because it reduces the IDS's efficiency and may also confuse the administrator.

IV. TYPES OF ATTACKS

The attacks on the computer system or computer network is done to steal confidential information, gain unauthorized access, and destroy system activities and to learn some patterns that compromises the system integrity, confidentiality and availability. There are two types of attack on the computer system or network, Active attack and Passive attack. An active attack attempts to affect the operation of the system and also affect the system resources. Passive attack meant to learn the patterns of the system, but not affecting the system resources and services [3]. Here are some of the attacks described:

A. DoS Attack

Denial-of-Service (DoS) attack is the type of attack in which computer resources become unavailable to its intended or authorized users. The services of user can be temporarily or indefinitely interrupted or suspended. Distributed Denial-of-Service (DDoS) attack is happening when the attack to the machine is done by more than one or usually thousands of unique IP addresses. These attacks slow down the system or deny the services of valid user. Due to this attack a lot of network traffic occurs.

B. User to Root Attack (U2R)

In this attack, the attacker starts his activity as a user and takes down the password, next do the dictionary attack and finally attacker gain access as a root user. The U2R attacks lead to several vulnerabilities such as a dictionary attack, password sniffing and social engineering attacks.

C. Remote to User Attack (R2U)

In this attack, an attacker sends the packets to a machine over the network, but does not have an account on the local machine, by using the vulnerabilities of the system attacker gain local access to the system as a user.

D. Probing

A probe is a program or a network device that is inserted at a key juncture in a network for the purpose of constantly monitoring or collecting data about network activity. Based on information attacker searches for the weak points and vulnerabilities in the system, from that point he attempts to enter into the system.

E. Eavesdropping Attack

It is a network layer attack, in which an attacker captures the packets from the network that are transmitted from a host of others. An attacker can read sensitive and confidential information that is transmitted.

F. Man-in-the-Middle Attack

In this type of attack the attacker situated himself in the middle of two persons in communication, and both persons in communication think that they both communicating with each other but all the conversation is compromised.

G. Smurf Attack

It is a type of distributed denial of service attack in which victim's system is flooded with spoofed ping messages. To create a lot of ping messages attacker broadcast the Internet Control Message Protocol (ICMP) packets in the network intended to victim's IP address. Most of the network devices will respond to these messages by default and if the number of these types of packets is very large then the victim's computer will be flooded with traffic.

V. INTRUSION DETECTION APPROACHES

In recent incident and activities the traditional model of intrusion detection is not feasible, in traditional model we manually analyze the network or give some fixed, abnormal patterns in the system and decide whether the system or network is under attack or not. In present scenario the use of internet enhances the traffic on the network as well as threats from attacking because of easy to access policy, so these activities enhance the data for the network analyst and it is difficult for him to detect the intrusions. So we needed strong methods to automate this process of intrusion detection and also made them dynamic, so that the system can learn from him and can detect new types of intrusions. In this way many researchers do their work in finding the intrusion detection techniques that are dynamic, adaptive and can work on the huge amount of network traffic and data.

Intrusion detection approaches involve mainly three steps for finding an intrusion:

- Define and extract the features: In this way the analyst decides for his method, which parameters (features) to select to categorize the data, so that the data can be partitioned according to features selected and then analyst can find the common rules present in the data set.
- Define and extract the rules: The categorized data, then analyzed to find the common rules in the data set by applying appropriate method.
- Apply rules to detect intrusions: After defining the rules in the dataset, which activity or data going out of rule is considered as an intrusion.

We hereby are describing some of the methods that were developed according to the need of the systems and networks. There are four main categories of intrusion detection:

A. Pattern Matching

Pattern matching is a simple intrusion detection technique in which intrusions are detected by comparing with the known attack signatures. Using this technique we can generate the signatures from the audit records and compare them with the current activities to detect intrusions. The attack signatures specifically having some common binary patterns through which we can find the abnormal activity. The rules for pattern matching are easy to write and also can easily be generated from the audit records [1] [6].

The limitation of pattern matching is that it can only recognize the known attacks; it cannot find the new activities. In recognition of new attack patterns it needed constantly updating in signature records. Pattern matching technique is appropriate for misuse detection only.

B. Data Mining Method

Data mining techniques are used to extract interesting facts or knowledge that is hidden in the database. The knowledge can be in the form of patterns, relationships, groups or classes, etc. The data mining methods are usually applied to process the bulk amount of data at once [1] [7].

This capability of processing bulk amount of data in quick time we use this for intrusion detection systems, where the audit/transaction data are in huge amount. By applying different data mining techniques we can extract known attack behavior from the database of audit/transaction records.

- Association Rule/Frequent patterns: Association rule consider each item pair as an entity. Collections of item that are frequent in the database are extracted by the algorithm. The algorithm searches those frequent patterns based upon two parameters Support and Confidence. The aim of association rule in finding intrusion in terms of finding the relationships between attributes that constitutes an attack. Because intrusive activities have some common patterns, by finding these patterns by using association rule we can find intrusions.
- Clustering: Clustering is used to form the groups of unlabeled data and labeling of those groups. Each group have similar object but having different object from each other, means each group's object having some commonalities but have differences with other group's objects. Clustering can be used to find the intrusions over a time period. The objects or patterns that are far away or not in any cluster can be identified as an intrusions or we can make some specific clusters so that the object lies in that will be automatically classified as an intrusion. The objects that don't lie in any cluster can be a new type of attack, so the clustering is unsupervised machine learning method used for both anomaly and misuse detection [4].
- Classification: Classification is a task of assigning a particular class label by grouping the data set according to some defined rules. Since, the class label is already known, so this type of classification is known as supervised learning. For intrusion detection, classification technique is used for classification of network traffic into normal or abnormal. Based on user activity, it can also classify a user as an authorized user or an unauthorized user. For doing this it follows two step procedure, learning and classification. In learning phase it trains himself from the training data set about the intrusive activities and in classification phase it applies it trained set of rules of the network data for the classification.

C. Machine Learning Method

We have seen the techniques that rely on human intervention for detection of intrusions. It sometimes takes many days or weeks to detect new signatures of intrusions. In present scenario where the network traffic increasing day by day it is infeasible to spend days or weeks in the process of finding an intrusion. To overcome this problem a human independent solution developed, i.e. anomaly based intrusion detection system with machine learning capabilities.

The machine learning techniques are adaptive to learn from training dataset and then it applies the learnt rules on the network data to find the deficiency or intrusions. Some of Machine learning techniques are as follows for anomaly based intrusion detection [8] [9] [10].

- Neural networks: Neural network approach for intrusion detection is to learn the behavior of users. Neural network predicts the next step of user based on the past sequences of user activities. It is a three step process to implement a neural network in intrusion detection system and the processes are- Collecting training data, Training, and implementation [5].
- Genetic algorithms: Genetic algorithms are a programming technique which mimics the biological evolution as a problem solving strategy. The Genetic Algorithms use an evolution and natural selection that uses a chromosome like data structure and evolve the chromosome using selection, recombination and mutation operators. GAs can be used in intrusion detection systems for artificially selecting the different features and detecting intrusions. The flexibility of selecting different features makes GAs different from available approaches.
- Support Vector Machine: Support vector machine is a supervised machine learning model that is used to analyze and classify the data. It is trained by the training data to model a hyper plane between the data set so that the data set can be separated into two classes. There may be many hyper plane exists in the data set but we choose the best hyper plane that represents the largest separation or margin between two classes. We use this concept of the intrusion detection system for the classification of data as normal or malicious. When a new activity takes place in the system we SVM model, classify the activity as normal or malicious based on its activity pattern. If it is malicious activity, then the system will generate an alarm.

VI. COMPARISON OF IDS APPROACHES

We can detect intrusions by various available techniques. The question is obvious is which technique is best to implement for efficient detection of intrusions. The answer is every technique has advantages and disadvantages/limitations, to choose the best technique we have to look at various parameters like what type of intrusions we need to detect, how large is the data set, where to place IDS, network requirements, how many resources we have to implement an IDS, etc. According to the need we can choose the specific techniques for our IDS. For making all this stuff easier, we hereby done the comparative study of various IDS approaches.

TABLE I. Comparison of different IDS Techniques

S. N.	Method/ Technique	Concept	Advantage	Limitation
1	Pattern Matching	Used to detect intrusions based on matching the existing patterns with the incoming traffic patterns.	Simple to implement and used to detect simple misuse detection. Not very complex and resource consuming.	Limited to misuse detection, it cannot find the new intrusions means anomaly detection is not possible.
2	Data Mining	Used to detect intrusions where the data set is very large to process. We can extract different type of knowledge by applying various methods of data mining.	It is used to detect both misuse and anomaly detection. It can classify the data according to the analysts need.	On huge databases it is time consuming.
3	Machine Learning	These methods are adaptive to learn from it. Training phase is used for learning and implementatio n phase is used to detect the intrusions based on those learnt rules.	It is an automated process of detecting both misuse and anomalous intrusions. It hardly needs human intervention.	It is a very complex procedure to implement and also resource consuming.

Table 1 shows the comparative analysis of different intrusion detection techniques. The comparative analysis shows the different perspective of using the method. Different approaches have their advantages and disadvantages. We chose the specific method for our IDS based on different parameters. If we want to detect the intrusions that are anomalous in behavior and also we know the specific patterns of attacks, we choose pattern matching algorithms. Likewise, if we have a huge amount of data we chose data mining methods. In spite of the two methods we have a machine learning method that adapts to self learning and used in those IDS where we needed new attack patterns to be recognized frequently.

Overall analysis shows that every method has their usage in different situations. All we need to do to collect the need of the Intrusion Detection System and according to the needs and target we place appropriate method.

VII. OBJECTIVE AND RESEARCH SCOPE

Intrusion detection systems are nowadays recognized as fundamental tools for the security of computer systems. IDSs aim at identifying violations of security policies and perform automatic counteractions to protect computer systems and information. As soon as IDSs are deployed, they may become target of attacks that may severely undermine or mislead their capabilities. To the best of our knowledge, this paper is the first survey on adversarial attacks against IDSs, a relevant topic especially for safety–critical environments. In this synopsis we provided the following contributions:

(1) We provided a general taxonomy of attack tactics against intrusion detection systems;

(2) We subdivided the IDS task into three different phases,

Moreover, throughout the paper we identified a number of challenging issues that should be addressed by future research activities on intrusion detection. We focus our attention on a few of them:

- Strengthening the measurement mechanisms by relying on both host and network sensors, and exploiting the concept of redundancy as performed by data reconciliation techniques in process control. In addition, in-VM monitoring showed to be a very promising way to strengthen measurements at the host level.
- Enhancement of the description of alerts in anomaly based systems through automatic attack inference mechanisms. This may definitely cope with the lack of informative output in anomaly based systems that may allow for the detection of variants of known, or never-before- seen intrusions. Moreover, exploiting contextual information about the systems being monitored (e.g., for performing alert verification) seems the natural way to deal with over stimulation attacks, as well as false alarms in general.
- Responses against intrusions based on cost-sensitive models, game theory and proactive techniques should be further investigated. Human expertise will always play a central role, but these methods can be helpful to automate the response process and make it effective against an adversary.
- IDS solutions are expected to increasingly implement machine learning mechanism s, to deal with the complexity of the intrusion detection task. Consequently, techniques based on adversarial machine learning are worth being further investigated.

VIII. CONCLUSION

The paper describes different types of intrusion detection system and highlights techniques of intrusion detection approaches. We draw attention to Pattern Matching, Data Mining method, Machine Learning techniques, which are used to implement Intrusion Detection System (IDS). We also describe different types of attack from which we need to take precautions in IDS. We make the comparative analysis of various Intrusions detection approaches so that researchers can categorize the methods and use according to the need.

The aim of this paper is to describe as many as possible terminologies related to intrusions and its detection system. All the terminologies and the very basic intrusion detection system architecture help anyone understanding the IDS. We sure this brief survey is useful for all researchers that want to investigate more efficient methods against intrusions.

REFERENCES

[1] A Murali M Rao, “A Survey on Intrusion Detection Approaches”, IEEE, P.P. 0-7803-9421-6, 2005.

[2] K. Asif, Talha A. Khan, Sufyan Yakoob, “Network Intrusion Detection And Its Strategic Importance”, Ieee Beiac, P.P 978-1-4673, September 2013.

[3] Subaira.A.S, Anitha.P, “Efficient Classification Mechanism for Network Intrusion Detection System Based on Data Mining Techniques:a Survey” International conference on

Intelligent System and Control(ISCO), IEEE, P.P. 978-1-4799-3837, July 2014.

[4] F.Sabahi, A.Movaghar, "Intrusion Detection: A Survey", The Third International Conference on Systems and Networks Communications, IEEE, P.P. 23-26, ISBN 978--7695-3371-1, October 2008.

[5] Adriana-Christina Enache, Victor Valeriu Patriciu, "Intrusions Detection Based on Support Vector Machine Optimized with Swarm Intelligence", 9th IEEE international symposium on Applied Computational Intelligence and Informatics", P.P. 978-1-4799-4694-5/14, May 2014.

[6] Zhou Chunyue,Liu yun:Zang Hongke, "A Pattern matching based Network Intrusion Detection System", ICARCV '06. 9th International Conference on Control, Automation, Robotics and Vision, 2006", IEEE, P.P. 1-4, E-ISBN 1-4214-042-1.

[7] Deepthy K Denatious, Anita John, "Survey on Data Mining Techniques to Enhance Intrusion Detection", International Conference on Computer Communication and Informatics (ICCCI - 2012), IEEE, P.P. 1-5, ISBN: 978-1-4577-1580-8, January 2012.

[8] Ming Xue,Changjun Zhu. "Applied Research On Data Mining Algorithm In Network Intrusion Detection", International Joint Conference On Artificial Intelligence, IEEE, P.P. 275-277, ISBN 978-0-7695-3615-6, April 2009.

[9] W. Feng, Q. Zhng, G. Hu, J Xiangji Huang, "Mining Network Data For Intrusion Detection Through Combining SVMs With Ant Colony Networks" Future Generation Computer Systems, 2013.

[10] Uzair Bashir, Manzoor Chachoo, "Intrusion Detection and Prevention System: Challenges and Opportunities", International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, P.P. 806-809, ISBN: 978-93-80544-10-6, March 2014.

