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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Review of Anomaly Detection Techniques in Network Intrusion Detection System

Dr.D.V.S.S.Subrahmanyam

Professor, Dept. of CSE, Sreyas Institute of Engineering & Technology, Hyderabad, India

ABSTRACT: In network security Intrusion detection systems (IDS) are an important element in a network's defenses to help protect against increasingly sophisticated cyber attacks. Intrusions are nothing but attacks. IDS that rely solely on a database of stored known attacks are no longer sufficient for effectively detecting modern day threats. This paper is basically a research paper on network intrusion detection techniques. And also describes what kind of attack took place. This paper presents a novel anomaly detection technique that can be used to detect previously unknown attacks on a network by identifying attack features. In this paper we discussed about various network intrusion detection techniques like K-means clustering, feature selection and decision tree. This paper also includes various examples from the past and current projects. We hope that this survey will provide a better understanding of the different directions in which research has been done on this topic.

I. INTRODUCTION

The increased dependence of government, military and commercial organizations on Internet technologies to conduct their everyday business creates new challenges for cyber defense. The advancing complexity and variety of cyber attacks have almost rendered traditional IT defences, such as anti-virus software or intrusion prevention systems. A deliberate action against data, software or hardware that can destroy, degrade, disrupt or deny access to a networked computer system is called a cyber attack. Now a day, in the area of intrusion detection, data mining techniques have been employed with success. In particular, the data pre-processing stage, which includes feature selection, has attracted much attention. Feature selection selects relevant subsets from the original dataset in order to minimize the effect of irrelevant and redundant features without greatly decreasing the accuracy of the classifier. In protecting files and other information computer use implies a need for automated tools. In cryptography basically we have to know about some terminology like plain text, cipher text, encryption, decryption and keys. Plain text: The data which is having valid meaning is called plain text. Cipher text: The data which does not having valid meaning is called cipher text. Encryption: Converting plain text into cipher text is known as encryption. Decryption: Decryption is the reverse process of encryption. This means converting cipher text into plain text.

Keys: keys are two types

1. Public key
2. Private Key

Public key is known to every node in the network. And private key is known to only the generated node.

II. LITERATURE SURVEY

Intrusion: A deliberate action against data, software or hardware that can destroy, degrade, disrupt or deny access to a networked computer system is cyber attack. Intrusions are nothing but attacks. Attacks are 2 types 1) Passive attack: where the attacker can read the data.2) Active attack: where the attacker can read, write and modify the data. Intrusion Detection: An intrusion detection system (IDS), therefore, dynamically monitors logs and network traffic, applying detection algorithm s to identify these potential intrusions with in a network.

2.1 Intrusion detection functions include:

1. Monitoring both user and system activities,2. Analyzing system configurations and vulnerabilities,3. Assessing system and file integrity,4. IDS has the ability to recognize patterns typical of attacks,5. Analysis of non-uniform activity patterns,6. Tracing user policy violations Intrusion detection systems are being developed in response to the increasing number of attacks on major sites and networks. Typically, Intrusion detection systems are two types. The

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

first one is host-based and is considered the passive component. The second one is network-based and is considered the active component.

2.2 Network Intrusion Detection:

In computer security, a Network Intrusion Detection System is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. To understand what is a network intrusion detection system one should first know what intrusion is. A deliberate action against data, software or hardware that can destroy, degrade, disrupt or deny access to a networked computer system is cyber attack, and a network intrusion detection system is a system, which detects such intrusions or attacks. NIDS main objective is to find out whether a hacker is hacks your system. It analyzes the traffic on your network to monitor signs of different malicious activity.

2.3 Main objectives and functions of network intrusion detection

Detecting intrusions:

Network intrusion detection system detects security threats and attacks. Offer information: If network intrusion detection system finds any attack then I will provide information about the attack and what kind of attack has occurred. Take corrective steps: After finding the attacks by the system, it provides necessary steps to face the attack.

Storage: Network intrusion detection system stores the information about the intrusion.

Less cost: It takes less amount to deploy the network intrusion detection systems.

Detecting attacks: Network intrusion detection systems can easily detect any type of attacks by scanning all the content.

2.4 Problem Statement

Network security measures to protect data against during their transmission. But, there are different kinds of attacks are possible in network. The attacks are classified into two types. They are known attacks and unknown attacks. In this paper we are going to give clear explanation about to find the unknown attacks by using anomaly based technique.

III. SECURITY ATTACKS

Basic component of every network design is security. As we know that a deliberate action against data, software or hardware that can destroy, degrade, disrupt or deny access to a networked computer system is a cyber attack.

3.1 Active attack :

In this attack Intruder can only read the data in this attack

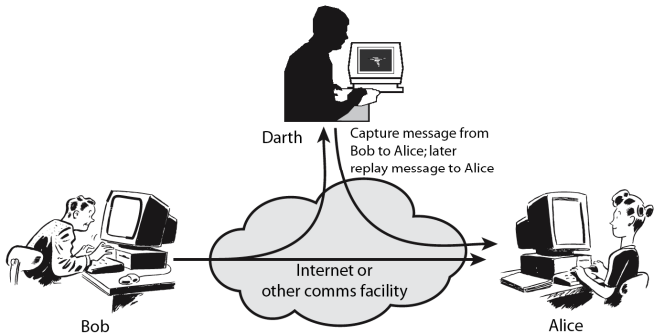

Fig : 2.1 Active attack

Intruder can only read the data of the sender. But he can't write and modify the contents of the data.

3.2 Passive attack:

In this attack, the Intruder can read, write and modify the contents of the data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

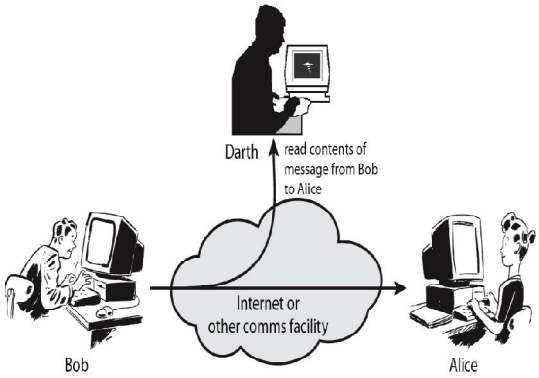

Fig : 2.2 Passive attack

The Intruder can read, write and modify the contents of the data which were send by one person to the other. So these type of attacks are considered to be Passive attacks.

IV. SECURITY POLICIES

Being secure for a system, organization or other entity is known as security policy.
Security policies are :
1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Access control

The three main principles of data security are confidentiality, integrity and availability.

4.1 Confidentiality: Confidentiality means maintaining secrecy while sending the information.

4.2 Integrity: Allowing only authorized persons to modify information. We have to send the data to the destination without any modification.

4.3 Availability: Availability ensures that the data should be available to the users when needed.

V. EXISTING SYSTEM

The three main principles of information security are confidentiality, integrity and availability(CIA), which help to ensure authorized access to information within a system. In an effort to help protect systems, technologies such as firewalls and antivirus software are employed in defensive layers to help detect intrusions, which are violations of the CIA information security policy with in a network or system.IDSs can be split into two categories according to the detection .methods they employ, including (i) misuse detection and (ii) anomaly detection. Misuse detection is perhaps the oldest, most common approach and uses established knowledge of known attack patterns to scan for signatures, monitor state transitions or employ data mining techniques to identify potential attacks. Although misuse detection systems are extremely efficient at detecting a limited set of known cyber attacks with low false alarm rates, their capabilities are limited to the information stored within the database and are thus unable to perform accurately when faced with the challenge of detecting new classifications. However, it is becoming increasingly apparent that enemy cyber attacks with high target specificity can penetrate cyber defenses and avoid detection from application such as Snort. Thus, anomaly detection methods seek to overcome this problem by assuming that cyber attacks are ‘abnormal’ and identifiable by noting their statistical deviation from ‘normal’ behavior model or profile.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

VI. ADVANTAGES

The advantage of this service is the "round-the-clock" aspect, in that the system is protected even while the user is asleep or otherwise away from any computer hooked network. Network based IDS can be deployed for each network segment. An IDS monitors network traffic destined for all the systems in a network segment. Network based IDS are easier to deploy as it does not affect existing systems or infrastructure. The system independent. A network based IDS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running system independent. A network based IDS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running. Host based systems can detect attacks that network based IDS sensors fail to detect. Host based sensors can be very useful in protecting hosts from malicious internal users in addition to protecting systems from external users. If an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the network sensors.

VII. DISADVANTAGES

Based on audit data collected over a period of normal operation. When a noise(intrusion) data in the training data, it will make a mis-classification. How to decide the features to be used. The features are usually decided by domain experts. It may be not completely. Prone to false positives. Potentially to detect previously unknown types of attacks. Heavy processing overhead. Vulnerable to attack while creating time consuming statistically significant baselines.

VIII. PROPOSED SYSTEM

An intrusion detection system (IDS), therefore, dynamically monitors logs and network access, applying detection algorithms to identify these potential intrusions within a network. Many anomaly detection IDS's employ data mining techniques to aid in the processing of large volumes of audit data and the increasing complexity of intrusion behaviors.

8.1 Data mining for intrusion detection:

In recent years, there have been many successful applications of data mining techniques employed in intrusion detection. Data mining is the search for valuable information within large volumes. Clustering is commonly used in anomaly detection to discover groupings and populations where little is known about the spread or relationships within the data. Clustering analysis techniques group objects in to natural groupings based upon the characteristics they possess. The cluster contains same kind of items. But is dissimilar to those in other clusters.

Its advantages in anomaly detection include the ability to detect previously unseen attacks, either by grouping similar attack instances together. There are many different clustering methods, although partition-based clustering is often applied. Partition based clustering methods partition the data points into a number of clusters by iteratively rearranging data points in an initial grouping of a predefined number of clusters.

8.2 Data generation and collection:

Acquiring data that is suitable for experimentation is a challenge within the area of intrusion detection. There are very few datasets available online. DARPA is the evaluation dataset which is used mostly for the research. In consideration of the high resolution approach this piece of research takes, a denial of service (DOS) attack was chosen to act as the cyber attack that the effects based feature identification would identify. A DOS attack is a deliberate intent to prevent a host, router or network from being accessible or receiving normal services from the Internet. Although there are many different descriptive features of a packet, the 10 features used in the following analysis were chosen because they make up the main part of the TCP/IP header. The features used include: protocol, packet length, sequence number, time, source IP, destination IP, source port, destination port, IP length, checksum.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Data analysis:

The data analysis part consist of three novel based anomaly detection techniques namely unauthorized k-means clustering, feature selection and authorized c4.5 decision tree classification. In the first technique unauthorized k-means clustering identifies the clustered features. The second technique feature selection can rank the relevant features to the particular attack and then it identifies and ranking the significant features. The third technique authorized c4.5 decision tree classification can evaluates the significantly relevant subsets of attack features.

IX. CONCLUSIONS

The contributions of this work are as follows. First, the techniques used in this paper are, namely k-means clustering, Naïve Bayes, Kruskal–Wallis and C4.5, allows intrusions, as anomalies, to be pinpointed with a high degree of accuracy within the cluttered and conflicted cyber network environment. Further, the inclusion of the Naïve Bayes feature selection and the Kruskal–Wallis test in the approach facilitates the classification of both statistically significant and relevant feature sets, including a statistical benchmark for the validity of the approach. Unlike previous research in this area that does not focus on the specific features that character is the cyber attack, this approach shows that a statistically relevant and reduced feature set filters out the noisy data associated with non- relevant features.

REFERENCES

[1].K.Kumar, M.Sachdeva,The use of artificial intelligence based techniques for intrusion detection: a review, Artif.Intell.Rev.34(4)(2010) 369–387.
[2].T.Kellerman,Cyber-threat pro liferation: today's truly pervasive global epidemic, IEEE Secur.Privacy8(3)(2010)70–73.
[3]. H.Kargupta, Approximate distributed k-means clustering over a peer-to-peer network,IEEE Trans.Knowl.Data Eng.21(10) (2009)1372–1388.
[4].P.Laskov, P.Dussel, C.Schafer, K.Rieck, Learning intrusion detection: supervised or unsupervised? Image Anal.Process.-ICIAP20053617 (2005)50–57.
[5]. J.B. Mac Queen, Some methods for classification and analysis of multivariate
observations, in: Proceedings of the Fifth Berkely Symposium on Mathematical Statistics and Probability, vol.1, 1967, pp.281–297.
[6].H.Shah, J.Undercoffer, A.Joshi, Fuzzy clustering for intrusion detection, Fuzzy systems,2003.FUZZ '03, in: The 12th IEEE International Conference on, vol.2, pp. 1274–1278vol.2,25–28 May2003.

BIOGRAPHY

Dr.D.V.S.S.Subrahmanyam, Professor , Dept. of Computer Science & Engg , Sreyas Institute of Engineering & Technology , Csi, Nagole , Bandlaguda , Hyderabad- 500068.