Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Hybrid Intrusion Detection System using Weighted Signature Generation over Anomalous Internet Episodes Rules

Bhakti B. Pawar[1], Kalwadekar P N[2]
[1,2]*ME- Comp, SRES College Of Engineering Kopargaon*

Abstract—To provide security to network we use existing Intrusion Detection System(IDS) for identification of known attack with low false alarm,but it is not working when unknown attacks occurs so to identify unknown attacks we use Anomaly based IDS(ADS) with high false alarm. HIDS is the combination of IDS and ADS with their advantages for identification of known as well as unknown attack.IDS used signature based model to identify known attack and ADS used anomaly based model for identification of unknown attack.HIDS used internet episode rules for identify known as well as unknown attacks.

Keywords-Intrusion Detection System,anomaly detection,signature generation,internet episodes, Traffic data mining,Network security,false alarm

I. INTRODUCTION

As we know that intrusions and anomalies are two different kinds of abnormal traffic events in an open network environment. An intrusion takes place when an unauthorized access of a host computer system is attempted. An anomaly is observed at the network connection level. Both attack types may compromise valuable hosts, disclose sensitive data. The intrusion detection system (IDS) offers intelligent protection of networked computers which is much better than using fixed-rule firewalls. These existing IDSs are built with either signature-based or anomaly-based systems.

Signature based IDS- A signature-based IDS employs a priori knowledge of attack signatures. The signatures are manually constructed by security experts analyzing previous attacks. The collected signatures are used to match with incoming traffic to detect intrusions. These are conventional systems that detect known attacks with low false alarms. However, the signature-based IDS cannot detect Unknown attacks without any precollected signatures or lack of attack classifiers. Signature matching performs well only for single-connection attacks. With the sophistication of attackers, more attacks involve multiple connections. This limits the detection range by signature matching.

Anomaly based IDS- A network anomaly is revealed if the incoming traffic pattern deviates from the normal profiles significantly. Through a data mining approach, anomaly detection discovers temporal characteristics of network traffic. This system can detect unknown attacks and handles multiconnection attacks well. However, anomaly detection may result in higher false alarms. The newly proposed HIDS is designed to solve these problems with much enhanced performance.

Hybrid based IDS- Here a new hybrid intrusion detection system (HIDS). This system combines the positive features of both intrusion detection models to achieve higher detection accuracy, lower false alarms, thus, a raised level of cyber trust. An adaptive base support threshold is applied on selected axis attributes in mining the Internet episode rules. The episode rules are used to build the HIDS, which detects not only known intrusive attacks but also anomalous connection sequences.

II. RELATED WORK

In "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous internet Episodes" ,I am using various intrusion detection technique like signature IDS and anomaly IDS. In

this techniques Three algorithms are used like Brute force algorithm which is used for pattern matching, Based support algorithm which is used for generating frequent episode and Apriori algorithm for generating weighted signature[1].

It is used for reference of research on the Intrusion Detection Technology with Hybrid model. I am using data preprocessing method mentioned in this paper[2].

It is used for reference of a Multiple Classifier System Using an Adaptive Strategy for Intrusion Detection. I am using KDD database mentioned in this paper[3][4].

SNORT and Bro are two widely used IDSs that are based on the misuse model. Other attempts to solve the intrusion detection and response problem can be found in[5][6].

Qin and Hwang refined the rule formulation procedure with an adaptive base-support algorithm to mine normal traffic records[7].

III. PROPOSED WORK

In this paper I am proposing a Hybrid Intrusion Detection System used to identify both known as well as unknown attacks. This method combine IDS used to identify known attacks and ADS used to identify unknown attacks but with high false alarm. So to overcome this disadvantage HIDS used internet episode rules to identify both known and unknown attacks.After that it creates signature based on anomaly detected and stored in signature database.

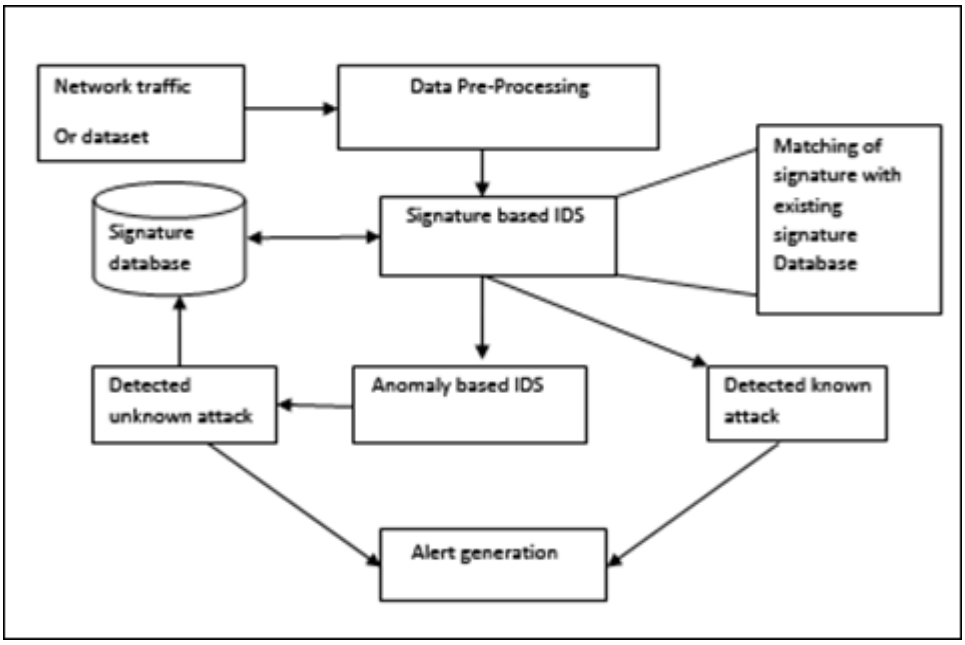

Figure 1. System Overview

It consists of following blocks-

- **Network traffic**- It is input for the HIDS. Network traffic is in the form of packets.
- **Data preprocessing-** The data information coming from multiple sources is usually incomplete, noisy and inconsistent. These raw data must be preprocessed and converted into ASCII network packet information forms or host the event data, and then build the connection records for the network connection or records for the host session data.
- **Signature database creation-** In this module signature database is created by using generating the signatures and store that signatures for detection of known attacks.

The simulated attacks fall in one of the following four categories:

1) Distributed Denial of Service Attack (DDoS): is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users access to a machine.

2) Smurf Attack: The Smurf Attack is a denial-of-service attack in which large amounts of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. This causes all hosts on the network to reply to the ICMP request, causing significant traffic to the victim's computer.

3) Remote to Local Attack (R2L): occurs when an attacker who has the ability to send packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine.

4) Probing Attack: is an attempt to gather information about a network of computers for the apparent purpose of circumventing its security controls.

- **Pattern matching algorithm-** In this module network traffic or packet data matched with existing IDS database by using pattern matching algorithm. Pattern matching algorithm is used to detect known attacks.
- **Behavior database creation-** In this module FER (frequently episode rule) database is created by using generating the rule sets and store that for detection of unknown attacks.
- **Behavior detection algorithm-** In this module normal behavior of packets is detected and matched with FER database by using behavior matching algorithm. It is used to detect unknown attack.
- **Database updating-** In this module unknown attack is detected by behavior detection algorithm then signature database updated i.e. store the signature of this attack in signature database.
- **Alert Generation-** In this module alert generated when signature based IDS found unknown attack or Anomaly based IDS found unknown attack. Alert is in the form of message.

IV CONCLUSION

In this paper I introduces Hybrid Intrusion Dtetection System(HIDS) which is used for identifying known attack as well as unknown attack in network connection. This system provide security to LAN connection. In this paper it gives combination of signature based IDS which is used for identification of known attack and Anomaly based IDS for detection of unknown attack. After identifying any type of attack it generate false alarm. So this HIDS system having advantages over existing IDS and ADS as it used various internet episode rules for identifying both known and unknown attacks.

REFERENCES

[1] Kai Hwang, Min Cai, Ying Chen, and Min Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes”, IEEEtransactions on dependable and secure computing,vol.4,no.1,Jan-Mar 2007.

[2] F. Cuppens and A. Miege, “Alert Correlation in a Cooperative Intrusion Detection framework,” Proc. 2002 IEEE Symp. Security and Privacy, pp. 187-200, 2002.

[3] K.S. Killourhy and R.As. Maxion, “Undermining an Anomaly-Based Intrusion Detection

System Using Common Exploits," Proc.Int'l Symp. Recent Advances in Intrusion Detection (RAID '02),pp. 54-73, Sept. 2002.

[4] W. Lee, S.J. Stolfo, and K. Mok, "Adaptive Intrusion Detection: A Data Mining Approach," Artificial Intelligence Rev., vol. 14, no. 6, pp. 533-567, Dec. 2000.

[5] D.J. Ragsdale, C.A. Carver, J. Humphries, and U. Pooch, "Adaptation Techniques for Intrusion Detection and Response Systems," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 2344-2349, Oct. 2000.

[6] F. Tao, F. Murtagh, and M. Farid, "Weighted Association Rule Mining Using Weighted Support and Significance Framework,"Proc. Ninth ACM Int'l Conf. Knowledge Discovery and Data Mining.(SIGKDD), pp. 661-666, 2003.

[7] M. Qin and K. Hwang, "Frequent Episode Rules for Internet Traffic Analysis and Anomaly Detection", Proc. IEEE Network Computing and Applications (NAC '04), Sept. 2004.

[8] F. Tao, F. Murtagh, and M. Farid, "Weighted Association Rule Mining Using Weighted Support and Significance Framework", Proc. Ninth ACM Int'l Conf. Knowledge Discovery and Data Mining (SIGKDD), pp. 661-666, 2003.

[9] Emna Bahri, Nouria Harbi and Hoa Nguyen Huu, "A Multiple Classifier System Using an Adaptive Strategy for Intrusion Detection", International Conference on Intelligent Computational Systems (ICICS'2012) Jan. 7-8, 2012.

