ISSN:0975-9646

Proposed Multi-Layers Intrusion Detection System (MLIDS) Model

Gargi Agrawal, Megha Kamble
CSE Dept., SIRT, Bhopal

Abstract: In the Digital world security is the primary concerned. Today, most discussions on computer security is centered on the tools or techniques used in protecting and defending networks. In recently every organization or company is using intrusion detection systems (IDSs) for detecting malicious attacks. Generally existing commercial IDSs are based on anomaly detection architecture. In anomaly detection unknown attacks can be detected with known attacks. In this paper, we have proposed multi layer intrusion detection technique (MLIDS) model. Proposed work will use an attacks model to identify various types of attacks and also it will show the layers of attack that mean on which layer it has identified. At last the proposed MLIDS can effectively and efficiently detect the attacks that are similar to DOS, R2L, U2R, and many more.

Keywords: IDS, Protocols, Network, Security, TCP

INTRODUCTION

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat [1]. We’ll cover each of these briefly.

- **NIDS**: Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic; however doing so might create a bottleneck that would impair the overall speed of the network [1, 2].
- **HIDS:** Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected [2].
- **Signature Based:** A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat [2].
- **Anomaly Based:** IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline [2].

Rest of the paper is organized are as follow: Section II presents literature survey where we have study of the related work. Section III presents proposed work where we have discussed proposed work in the field of IDS. And finally section IV present results and conclusion.

LITERATURE SURVEY

In [3] presented about the uses of intrusion detection systems (IDSs) in enterprise networks for detecting network attacks. In this paper authors have discussed on some problem which are coming in misuse detection system. Generally most existing commercial IDSs are based on misuse detection model. In misuse detection, although known attacks can be detected, unknown ones cannot be detected because attack signatures for unknown attacks cannot be generated. In this paper, they have proposed a method for detecting network attacks including unknown ones against servers such as web servers, mail servers, FTP servers, and DNS servers, using protocol specifications and site access policy. Furthermore, they have proposed a method to predict damage from detected attacks using neural networks. In [4] presents a common way to elude the signature-based Network Intrusion Detection System which is based upon changing a recognizable attack to an unrecognizable one via the IDS. For example, in order to evade sign accommodation with intrusion detection system markers, a hacker spilt the payload packet into many small pieces or hides them within messages. In this paper they have try to model the main fragmentation attack and created a new module in the intrusion detection architecture system which has recognized the main fragmentation attacks through verification of integrity checking of TCP packet in order to prevent elusion of the system and also to announce the necessary alert to the system administrator. In [6] the protocol acknowledgement module includes packet filtering and state protocol analysis techniques. Packet filtering technology can filter out the packet that the system does not care about to improve the efficiency of intrusion detection and security of the system itself; state protocol analysis technology that captures the data and maps for the state sequence accurately characterizes the process and attack steps of the protocol, which can effectively detect the invasion of multiple data packets collaboration. DDoS attack device is used to simulate the attack in the experiment. In [8] with the advent of anomaly-based intrusion detection systems, many approaches and techniques have been developed to track novel attacks on the systems. High detection rate of 98% at a low alarm rate of 1% can be achieved by using these techniques. Though anomaly-based approaches are efficient, signature-based detection is preferred for mainstream implementation of intrusion detection systems. As a variety of anomaly detection techniques were suggested, it is difficult to compare the strengths, weaknesses of these methods. The reason why industries don't favor the anomaly-based intrusion detection methods can be well understood by validating the efficiencies of the all the methods. To investigate this issue, the current state of the experiment practice in the field of anomaly based intrusion detection is reviewed and survey recent studies in this.

Issues in Existing System: An anomaly is observed at the network connection level. Both attack types may compromise valuable hosts, disclose sensitive data, deny services to legitimate users, and pull down network based computing resources. The intrusion detection system (IDS) offers intelligent protection of networked computers or distributed resources much better than using fixed-rule firewalls. Existing IDSs are built with either signature-based or anomaly-based systems. Signature matching is based on a misuse model, whereas anomaly detection is based on a normal use model. The design philosophies of these MLIDS are quite different, and they were rarely mixed up in existing IDS products from the security industry. 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. we have analyzed that the signature-based IDS cannot detect unknown attacks without any pre-collected signatures or lack of attack classifiers. Furthermore, 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. On the other hand, an anomaly-based system uses a different philosophy. It treats any network connection violating the normal profile as an anomaly. A network anomaly is revealed if the incoming traffic pattern deviates from the normal profiles significantly. Through a data extraction approach, anomaly detection discovers temporal characteristics of network traffic. This system can detect unknown attacks and handles multi-connection attacks well. Another thing is that anomaly detection may result in higher false alarms. Finally existing system has concentrated on a special type of attack which is the cause of poor security.

I. Proposed Work

The proposed Multi-Layers Intrusion Detection System MLIDS model includes packet monitoring, packet capturing, and packet analyzing with protocol analysis techniques. Packet monitoring technique will monitor packets over public network, packet capturing technique will capture packet which is travelling in public network and packets analyzing technique will analyze the packet and distingue those packet which can be harmful to the efficiency and security of the system. Protocol analysis technology will play an important role with packet capturing technique in the proposed model. This technique will capture the data and maps for accurately attribute of the layers and attack steps of the protocol. In this paper only architecture of the proposed MLIDS has been introduced and its implemented version will come in the future work. The proposed MLIDS model combines the positive features of different layer like application and transport, intrusion detection models to achieve higher detection accuracy, lower false alarms, and, thus, a raised level of cyber trust. Proposed MLIDS is network-based, which should not be confused with the host-based IDS with the same abbreviation by other. 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 MLIDS, which detects not only known intrusive attacks but also anomalous connection sequences. Figure-1 is showing architecture of the proposed MLIDS model. Initially training data set has creating by the proposed model. After preparing training data set, proposed model capturing packets and matching attributes to identify behavior of the packets if its normal then packets will go in the normal behavior data set and if it's abnormal behavior then it will go in the abnormal behavior data set. After completing this, proposed model will analysis which type of attack have captured in the data set and it will show type of attack and layer where its detect.

ARCHITECTURE OF IDS:

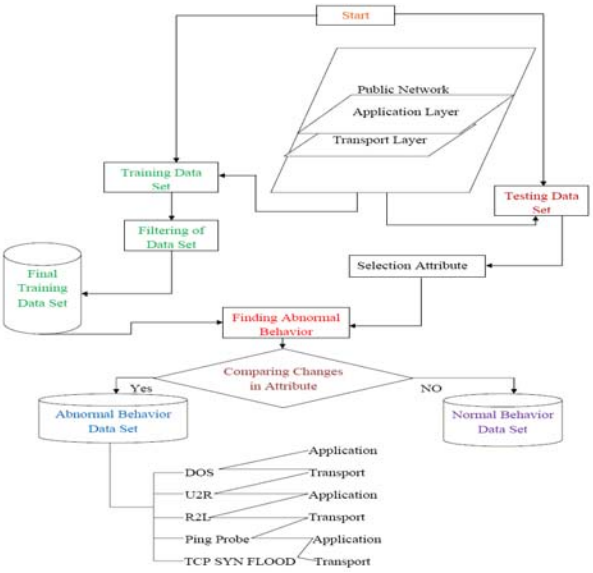

Figure 1:- Architecture of Proposed MLIDS

- **Proposed Model:** The proposed IDS model uses a different philosophy to detect normality and abnormality if the incoming traffic pattern deviates from the normal profiles significantly. This system combines the positive features of both intrusion detection models to achieve higher detection accuracy, lower false alarms, and, thus, a raised level of cyber trust**.**
- **Process Involved:** The proposed work will introduce the Multilayer's concept for intrusion detection. Proposed MLIDS model is a new weighted multilayer's protocol analysis. The new concept is generated from anomalies detected by this model.
- **Terminology used:** The Proposed MLIDS, (Profile based) is a model for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The signatures are manually constructed by security experts analyzing previous attacks. The collected signatures are used to match with incoming traffic to detect intrusions.
- **Anomaly detection:** Here proposed model will compare with database and if it is deviate from knowledge base or exceeding the threshold value or if events exceed the threshold value of already fixed
- **Multilayer's generation:** These are the events which represent no intruder. If there is any anomaly detected it will generate the alarm.

Proposed MLIDS can effectively detect the attack that is similar to DOS, U2R, R2L and "Ping probe" attacks. Table1 is showing different type of attacks.

Table 1: Type of Attack

Type of Attacks	Attacks Category	Description	TCP/IP Layer Category
back	DoS	denial-of-service (fack Address generate)	Application Layer
land	DoS	denial-of-service (fack Address generate)	Transport Layer
buffer_overflow	U2R	unauthorized access to local superuser (root) privileges	Application Layer
ftp_write	R2L	unauthorized access from a remote machine	Application Layer
multihop	R2L	unauthorized access from a remote machine	Transport Layer
nmap	Probe	surveillance and other probing	Application Layer
portsweep	Probe	surveillance and other probing	Transport Layer
TCP SYN FLOOD	DoS	denial-of-service (fack Address generate)	Transport Layer

CONCLUSION

It is possible, using the most up to date tools that are available, to protect against virtually every type of threat that is currently known about. Unfortunately, new threats and security holes in some software package or another are being discovered on a daily basis. It is important in any environment to know what types of threats we might be facing. Be aware of any potential security holes in system, and take care to prevent attacks against these. A new categorization for IDS based on Proposed MLIDS Model which focus on layer is designed that accommodates the three main form of security measure. This categorization improves the performance and scalability of the protocol over different layer. In the Proposed model each IDS type can be specialized to detect a specific category of attacks depending on the layer. Moreover, categorizing IDS will be supported by firewall since IDS is second level of defense after firewall. Proposed model by selecting the appropriate features set the application layers, transport layers and validates their performance. Advantages of proposed IDS are as follow

- First, proposed model can detect various types of attacks or account theft very easily. If a real user or someone using a stolen account starts performing actions that are outside the normal user-profile, it generates an alarm.
- Second, because the system is based on customized profiles, it is very difficult for an attacker to know with certainty what activity he can do without setting off an alarm.
- The proposed model can potentially detect an attack the first time it is used. The intrusive activity generates an alarm because it deviates from normal activity, not because someone configured the system to look for a specific stream of traffic.

Future work wills implementation of the proposed model so this can detect attacks in real time intrusion detection environments.

REFERENCES:

[1]Douglas J. Brown, Bill Suckow, and Tianqiu Wang "A Survey of Intrusion Detection Systems" 2004

[2] Vera Marinova-Boncheva "A Short Survey of Intrusion Detection Systems" 2007

[3] Tatsuya Baba and Shigeyuki Matsuda "A Proposal of Protocol and Policy-Based Intrusion Detection System" published in SYSTEMICS, CYBERNETICS AND INFORMATICS VOLUME 2 - NUMBER 3 2004

[4] Moad Alhamaty , Ali Yazdian and Fathi Al-qadasi "Intrusion Detection System Based On The Integrity of TCP Packet" published in World Academy of Science, Engineering and Technology 11 2005.

[5] Jin-Tae Oh , Sang-Kil Park, Jong-Soo Jang and Yong-Hee Jeon "Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment" published in IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.6, June 2007

[6] Chundong Wang, Quancai Deng, Qing Chang,Hua Zhang and Huaibin Wang " A New Intrusion Detection System Based on Protocol Acknowledgement" IEEE 2010

[7] Asmaa Shaker Ashoor and Prof. Sharad Gore "Importance of Intrusion Detection System (IDS)" International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518

[8] V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad "A Review of Anomaly based Intrusion Detection Systems" International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011