MULTI-AGENT DISTRIBUTED INTRUSION DETECTION SYSTEM USING ONTOLOGY

[1]Devasia Thomas, [2]Krupa Brahmkstri, [3]Avdhoot Jadhav, [4]Suraj Sawant

Student[1,2,3] , Professor[4], Department of Computer Engineering and Information Technology,
College of Engineering Pune
[1]thomasda91@gmail.com, [2]brahmkstrikp09.comp@coep.ac.in, [3]jadhavavdhoot7@gmail.com, [4]sts.comp@coep.ac.in

Abstract- Web Services are being used day by day. But many users are unaware of the vulnerabilities possible due to Semantic Web. Semantic Web is a standard that promotes common data formats on the WWW. The various attacks are single or distributed which are at times not detectable by firewalls. Hence there is need of IDS. But for distributed attacks and that too in a LAN, a single IDS cannot perform to its fullest. So comes the need of a Distributed IDS. To share the data among different IDSs and networks, we need to use ontology. Ontology is defined as a formal, explicit specification of a shared conceptualization. Ontology overcomes the difficulties faced by taxonomies. Previously, a minor change needed the whole system to be updated. There were compatibility issues due to the use of different languages across networks. So, it was very difficult to co-operate. By just adding additional information, a new attack pattern can be generated, thus promoting reusability. This further helps the agents involved in the IDS to take a proper intelligent decision and enhances the communication between them. Some traditional IDSs have a signature based detection system. These have a problem of false positives and fails in detecting new attacks. Hence the need of ontology based approach.

Index Terms— Distributed IDS, Ontology, Artificial Intelligence, Multi Agent

I. INTRODUCTION

With the number of attacks on computer systems through web services and applications increasing day by day, there is a high need to have a check on them and prevent the attacks from taking place. These attacks that occur are basically those that take an advantage of the vulnerabilities and misconfigurations on the independent or a combination of systems. In other words, it is the designs that are inappropriate for the system.

The purpose of the attack may not be known to the defender but it is very clear to the attacker. Even with the presence of firewalls and proxies, the attacker is successful in detecting the vulnerabilities and gaining access into the system.

The web attacks are of various types and are classified into one of the following groups of attacks i.e. Probing Attacks, Denial of Service (DoS) Attacks, Remote to Local (R2L) remote access Attack and U2R i.e User to Root Attacks.

Further, to detect an attack comes the need of an Intrusion Detection System (IDS). An IDS monitors all the network activities and detects suspicious patterns that may be harmful to the system. In the case of distributed attacks on a single LAN, a single IDS is not sufficient. Therefore a Distributed Intrusion Detection System comes into importance.

For the sharing of various packets data especially the attack packets, ontology is needed. Ontology is defined as a formal, explicit specification of a shared conceptualization. Ontology overcomes the difficulties faced by taxonomies. Previously, a minor change needed the whole system to be updated. There were compatibility issues due to the use of different languages across networks. So, it was very difficult to co-operate. By just adding additional information, a new attack pattern can be generated, thus promoting reusability. This further helps the agents involved in the IDS to take a proper intelligent decision and enhances the communication between them. Some traditional IDSs have a signature based detection system. These have a problem of false positives and fails in detecting new attacks.

In order for the attack detection to be much faster and hence make the whole system safe, multi-agents are used. Agents are nothing but programs that are present on each of the individual IDS and help in detecting an attack by passing information from one IDS to other. Thus they help in improving the overall performance of the system including its efficiency, robustness, flexibility and reuse.

In this paper we consider the detection of DoS and U2R attacks from the KDD Cup99 DataSet which is a widely used dataset for the evaluation of the IDSs.

II. LITERATURE SURVEY

With the various kinds of attacks being discovered day by day, there have also been various approaches to have an intrusion detection system in a LAN, some of which are discussed below.

To detect the four kinds of the IDS attacks, the network simulator used in [1], has various scripts that are executed on the terminal to detect the attacks. Here, there are different scripts for different attacks which no doubt detects the attack efficiently but there is no mention of a situation having distributed attacks and its detection. Again, how the attacks on one IDS can be communicated to the other is not described.

In [2], the researcher has described a two agent based intrusion detection system using Ontology namely Master Agent and the IDS Agent. The job of the IDS agent is the same as that of an IDS, only the reporting is done by the Master Agent. The proposed model is stated to detect more than 99.9% of attacks. Here again if the IDS agent was divided into more agents, the work could be parallelized and a better efficiency can be obtained.

In [3], the authors have proposed a really very efficient way of detecting attacks in a multi-agent based DIDS. The agents described are the Monitor Agent, Analysis Agent, Executive Agent, Manager Agent, Retrieval Agent and the Result Agent. As stated in their paper, the first four are static agents and the other two are mobile agents. As this is just a proposed model, no results about its efficiency are mentioned.

The researchers of [4] propose a system consisting of Monitoring Registry Agent (MoRA), Monitor Agent (MoA) and Managing Agent (MA). MoRA initializes and identifies MoAs, MoAs collect data about attacks and transmit to MA to enable them to detect for intrusions. Here, various attributes like source and destination IP addresses, source and destination ports, etc. are selected to monitor and hence check for a malicious packet. The authors just describe their model here without stating its implementation.

III. IMPLEMENTATION

This paper proposes an ontology based model which involves four agents namely Monitor Agent, Analysis Agent, Executive Agent and Manager Agent. A Knowledge Base which stores all the ontologies of various attacks and normal packets is present for each node in the system.

To detect the efficiency of our proposed system, we take into account the KDD Cup99 dataset which consists of various packets that are either malicious or are normal packets.

The malicious packets are one amongst the attacks namely, DoS Attacks, U2R attacks, R2L attacks or probing attacks [5]. This paper describes how well the proposed system detects DoS, U2R and normal attacks.

Firstly, the Monitor Agent receives the various packets from the network. In our case, it is the random packets taken from KDD Cup99 dataset. It monitors each packet and checks for particular attributes and forwards the necessary data to the Analysis Agent for the analysis of the packet data.

The Analysis Agent receives these attributes from the Monitor Agent and checks if the packet is normal or not depending on the information available in the knowledge base. This processing that is done is either in the form of packet sniffing or parsing. The comparison that is done is based on the fact that the knowledge base has a set of ontologies that are both the attack ontologies and the normal pattern ontologies. The Analysis agent after receiving the attributes from Monitor Agent constructs an ontology and compares this ontology with the already existing ontologies in the knowledge base. The ontologies are created with the help of Protégé tool. Protege is a free, open source tool that is used to construct ontologies given the attribute information. The ontologies that are created are stored in the .owl format.

These ontologies are then parsed using the Jena API [6]and Java. After parsing, the instances are queried and the result of the comparison is obtained.

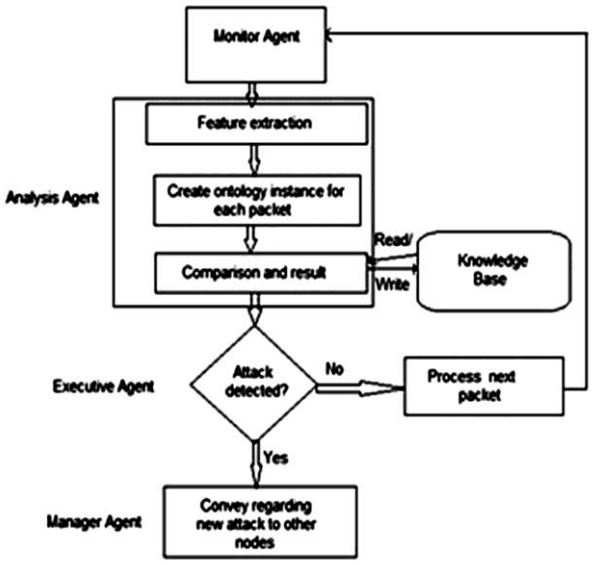

Fig. Proposed Model

If the ontology matches any of the ontologies in the knowledge base, we have a clear result. If there is no result, the packet is treated as a malicious packet and a new ontology of the same is created and stored in the database.

This is self learning, a part of Artificial Intelligence where decisions are taken by the system itself without any human intervention.

The result of the comparison is passed to the Executive Agent which decides what is to be done next. If the result states that the packet is normal, nothing is done. But if an attack is detected, the Executive Agent warns the other nodes about the malicious packet. It sends this information to the Manager Agent of the other nodes.

The Manager Agent receives the information about the attack from the Executive Agent and stores it in the knowledge base of its corresponding node.

IV. RESULTS

By considering various factors including source and destination address, source and destination port, bytes of data transferred, durations, flags, etc. we have the following results:

Total number of packets- 311,027

Total number of DoS packets- 164091

Number of DoS packets correctly detected- 163475

Total number of U2R packets-5000

Number of U2R packets correctly detected-5000

Total number of normal packets-45250

Number of normal packets correctly detected- 44500

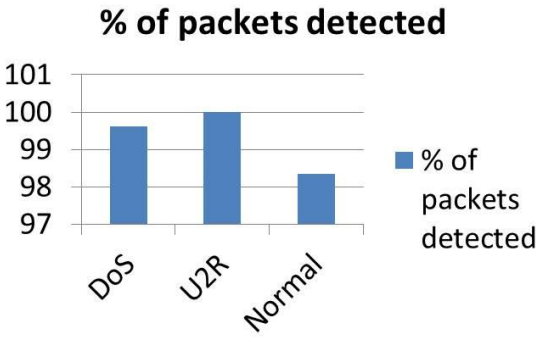

Fig. Efficiency of proposed IDS model

V. CONCLUSION

As from the results, it is evident that the proposed system gives about 98.5% efficiency. The implementation that was performed was based on the static data that is already available in the form of a standard dataset. Our next task would be to monitor the network traffic that is dynamic and thus determine our system's efficiency which would be the future scope of the system.

VI. REFERENCES

[1] Sapna S. Kaushik, Dr. Prof.P.R.Deshmukh, "Detection of Attacks in an Intrusion Detection System", International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011, pp. 982-986

[2] F. Abdoli and M. Kahani, "Ontology-based Distributed Intrusion Detection System", Proceedings of the 14th International CSI Computer Conference (CSICC'09), pp.65-70

[3] Dayong Ye, Quan Bai, Minjie Zhang, "Ontology-Based Knowledge Representation for a P2P Multi-Agent Distributed Intrusion Detection System", IFIP International Conference on Network and Parallel Computing, 2008, pp.111-118

[4] Yu Lasheng , and MUTIMUKWE Chantal, "Agent Based Distributed Intrusion Detection System (ABDIDS)", Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09), pp. 134-138

[5] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009)

[6] "Jena - A Semantic Web Framework for Java". Retrieved January 5, 2012, from http://jena.sourceforge.net/index.html.

◈◈◈