ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

Distributed Intrusion Detection System using mobile agent in LAN Environment

Trushna T. Khose Patil[1], C.O.Banchhor[2]

Department Of Information Technology ,SCOE ,Pune,India[1]

Assistant Professor Department Of Information Technology,SCOE,Pune,India[2]

Abstract:- In network intrusions, there may be multiple computing nodes that are attacked by intruders. The evidences of intrusions have to be gathered from all such attacked nodes. An intruder may move between multiple nodes in the network to conceal the origin of attack, or misuse some compromised hosts to launch the attack on other nodes. To detect such intrusion activities spread over the whole network, we present a new intrusion detection system (IDS) called Distributed Intrusion Detection using Mobile Agent In LAN Environment (DIDMALE).

Keywords: IDS,DIDMALE

I. INTRODUCTION

Intruders attack on multiple computing nodes in network. Some of the computer services may be made unavailable to other users. Due to huge and complex infrastructure of computer networks it is very difficult to completely secure such networks. So, an intrusion detection system (IDS) is needed. Whenever the confidentiality, integrity, and availability of computer resources are under attack, it will help to detect and respond effectively. From all such attacked nodes the evidences of intrusions have to be gathered. An intruder may move between multiple nodes in the network. Due to this the origin of attack is concealed. We propose a new intrusion detection system (IDS) called Distributed Intrusion Detection using Mobile Agent in Local Area network Environment DIDMALE.This system is helpful to detect such intrusion activities spread over the whole network.

II. LITERATURE SURVEY

When attacks occur or after the attacks took place Intrusions detection systems (IDSs) try to detect those attacks. IDSs collect traffic information and then use this information to secure the network. In this concept signature-based network intrusion detection techniques are a main technology to protect target systems and networks against such malicious activities. In threat detection technique for (IDSs) Signature-based detection is most extensively used. In signature-based IDSs there is some challenges like to keep up with large volume of incoming traffic when each packet needs to be compared with every signature in the database therefore may .miss potential attacks. So here this paper proposes a new model. Signature-based Multi-Layer IDS which uses mobile agents. They can detect imminent threats with extremely high success rate by dynamically and automatically creating and using small and efficient multiple databases. At the same time at regular intervals using mobile agents they provide mechanism to update these small signature databases.

In anomaly based IDS attempts to analyze abnormal activities and flag those activities as attacks. Anomaly detectors detect behaviors on a computer or computer network that are not normal.

Limitations:

If the normal module is not defined carefully in a normally based intrusion detection system, there will be lots of falls alarms and detection system suffers from degraded performance.

This is layered framework mechanism which is designed to support heterogeneous network environments for identifying intruders at its best. In traditional computer detection system identify known attacks efficiently. But their performance is very poorly in other cases. Anomaly detection system has the potential to detect unknown attacks. Without having prior knowledge about specific intrusions is a very challenging task to detect unknown attacks. The aim of proposed method is that the system can detect anomalous user activity. This method is use to look at both user activity and on program operation concurrently. The proposed method implements a layered framework. It is designed to satisfy the core purpose of IDS and it allows detecting the intrusion as quickly as possible with available data using mobile agents. This framework was mainly proposed for providing security for the network using mobile agent mechanisms to add mobility features for monitoring the user processes from different computational systems.

Limitations:

Agent migration introduces agent mobility and portability issues.

Mobile agents are intelligent agents, they are able to migrate among hosts and can execute tasks autonomously in dynamic environments. This paper includes an overview of several Network and Agent Based Intrusion Detection systems. Shows a superior performance compared to central sniffing IDS techniques and also saves network resources compared to other distributed IDSs. The model shows use of three major components which are Network Intrusion Detection Component, Mobile Agent Platform, and distributed sensors residing on every device in the network segment.

Limitation:

1) Security:

Malicious MA can damage a host. For example virus can be disguised as a MA an distributed in the network causing damage to the host that execute the agent.

On the other hand a malicious host can temper with the functioning of the MA.

2) Code Size:

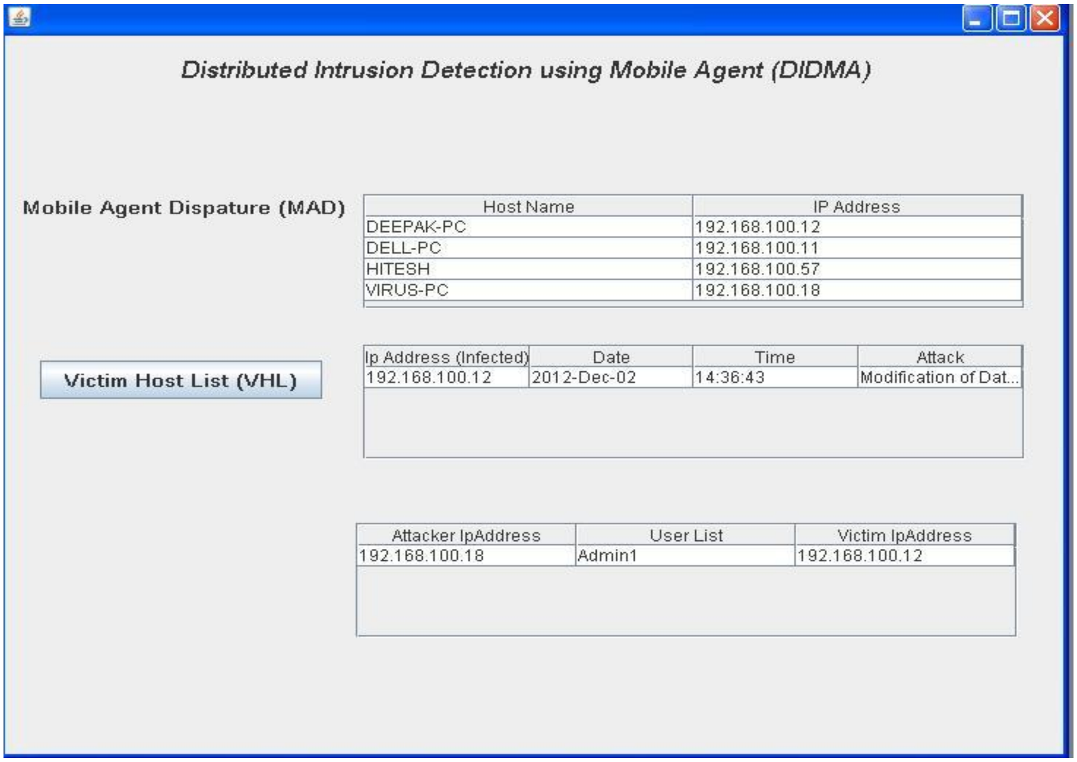
An IDS is a complex piece of software and agents that implement its functionality might get rather large. Transferring the agent code over the network may take some time.

3) Performance:

Agent is often written in scripting or interpreted language to be easily ported between different platforms. This mode of execution is very slow compare to native code as an IDS has to process a large amount of data under very demanding time constraints. The use of MA's could degrade its performance.

III.RESULT

There are several attacks are implemented. Result is showing below.History of all nodes are store into the database.



Distributed Intrusion Detection using Mobile Agent (DIDMA)

Mobile Agent Dispature (MAD)

Host Name	IP Address
DEEPAK-PC	192.168.100.12
DELL-PC	192.168.100.11
HITESH	192.168.100.57
VIRUS-PC	192.168.100.18

Ip Address (Infected)	Date	Time	Attack
192.168.100.12	2012-Dec-02	14:36:43	Modification of Dat...

Attacker IpAddress	User List	Victim IpAddress
192.168.100.18	Admin1	192.168.100.12

IV. CONCLUSION

DIDMALE overcomes some of the disadvantages of the centralized distributed intrusion detection systems. DIDMALE uses Hosts as monitors and mobile agents for collecting data, aggregation and correlation, and to give response to any attack. Use of mobile agents in DIDMALE makes application advantageous such as it reduces network bandwidth usage, it increases scalability and flexibility. It can be able to operate in heterogeneous environments. DIDMALE offers a new and good technique for decentralized data analysis which is carried out by mobile agents at the site of audit data instead of sending the audit data to some central data analysis component.

V.REFERENCES

[1] P. Kannadiga, M. Zulkernine, and S. Ahamed, "Towards an Intrusion Detection System for Pervasive Computing Environments," to appear, Proc. of the International Conference on Information Technology (ITCC), IEEE CS Press, Las Vegas, Nevada, USA, April 2005.

[2] G. Helmer, J. Wong, Y. Wang, V. Honavar, and Les Miller, “Lightweight Agents for Intrusion Detection,” Journal of Systems and Software, Elsevier, vol. 67, pp. 109-122, 2003.

[3] Mueen Uddin, Azizah Abdul Rehman, Naeem Uddin, Jamshed Memon, Raed Alsaqour, and Suhail Kazi, “Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents” University Technology Malaysia, International Journal of Network Secu rity, Vol.15, No.1, PP.79-87, Jan. 2013.

[4] N.Jaisankar and R.Saravanan K. Durai Swamy, “Intelligent Intrusion Detection System Framework Using Mobile Agents”, VIT University, International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009

[5] Dr. Bhushan Trivedi, Jayant Rajput, Chintan Dwivedi and Pinky Jobanputra, “Distributed Intrusion Detection System using Mobile Agents”, MCA Dept.,GLS ICT, Ahmedabad, India, CICA, Education Campus, Changa, India, 2009 International Symposium on Computing, Communication, and Control (ISCCC 2009).

[6] Jianxiao Liu, Lijuan Li, “A Distributed Intrusion Detection System Based on Agents”, epartment of Computer and Communica tion, Hunan University, 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application,2008.