AN INTELLIGENT DISTRIBUTED INTRUSION DETECTION SYSTEM IN GRID ENVIRONMENT USING IDS

Mr.Mahalingam T [1], Ms.Jeevitha.R [2], Dr.Shunmuganathan K.L. [3]

Abstract-Intrusion Detection Systems have been used along with various techniques to detect intrusions in networks, distributed databases and web databases. However, all these systems are able to detect the intruders with high false alarm rate. In this paper when the intruder enters the grid system with the help of brute force attack to the data base stored in the grid environment. When a intruder enters the grid system a R-LOGIN-ID is created, to avoid the such kind of attacks create the DIDS . Distributed Intrusion Detection System for Grid environment which has the ability to detect the intruder in the grid environment, track and monitor his malicious activities until a threshold. Once the intruder reaches the threshold, he is prevented from moving forward in his malicious activities. The grid environment and the identification and prevention of intrusions in the distributed grid environment is to be simulated.with the help of central manager to secure storage, data analysis to detect intrusions, discovery of distributed sensors, and sending of alerts.

Index Terms: Distributed Intrusion Detections (DIDS), Intrusion detection systems (IDS),Local IDS(LIDS),Grid Computing,Grid Section (Grid Sec).

1. INTRODUCTION

Grid is a hardware and software infrastructure or space that provides proactive, autonomic, trustworthy, and inexpensive access to pervasive resource sharing capabilities anytime and anywhere. Grid computing techniques can be used to create very different types of grids, adding flexibility as well as power by using the resources of multiple machines. A diagram to visualize the grid environment is given below.

Figure1.Distibuted Grid Platform

The goal of Grid computing is to create the illusion of a simple yet large and powerful self managing virtual computer out of a large collection of connected heterogeneous systems sharing various combinations of resources. To full fill this goal many distributed systems were created, but not all can be classified as Grid systems. Grid systems are considered to be the network middleware connecting applications and network resources. The intention is to enable Grid computing Internet in general, the possible threats that every system faces include attempted break-in, masquerading or successful break-in, and penetration by legitimate user, and inference by legimate user need.

1.1 DISTRIBUTED INTRUSION DETECTION ALERT CORRELATION

DIDS can be deployed at various grid sites supported by alert correlation sensors. These sensors are scattered around the computing Grid. They generate a large amount of low-level alerts. These alerts are transmitted to the alert correlation modules to generate high- level intrusion reports, which can provide a broader detection coverage and lower false alarm rate than the localized alerts generated by single IDS.A DIDS needs services for the location of and access to distributed data from different IDSs. Auditing and monitoring services take care of the proper needs of the DIDSs such as: secure storage, data analysis to detect intrusions, discovery of distributed sensors, and sending of alerts, receiving the acknowledgment generated by the different IDSs that compose DIDS based on the user request.

2. SYSTEM ARCHITECTURE

The overall architecture of GridSec DIDS consists of Authentication Server, Local IDSs and a Central Manager. The Authentication Server has two functions namely authentication of the grid users and allocation of resources for the requests of the users. The user provides his username and password for authentication. All the grid resources have local IDS. The local IDSs are intended to check for maliciousness in the incoming data in the node where they have been set. The IDSs generate alerts when they encounter suspects or malicious activities in their respective nodes. At the heart of the DIDS architecture is the Central Manager. The Central manager maintains a database where it stores all the incoming alerts from various IDSs. The Alert Clustering and Merging module of the Central Manager merges similar local alerts into global alerts. The Alert Correlation module correlates related alerts based on some correlation rules and generates correlation reports from which the intention of the intruder is recognized and actions are taken to neutralize the intruder's plan. The Sensor is an entity that performs two tasks namely routing data to intended node, and monitoring the activities of a user at a node which has been allocated for him. The design diagram of the GRID SEC-DISTRUBUTED DETECTION SYSTEM is shown in the Fig

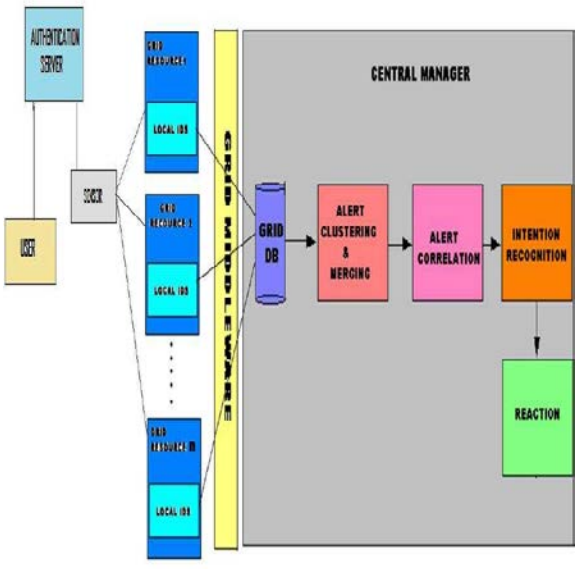


Figure 2.Sytem Architecture Model

2.1SENSOR

In the GridSection , When the user logins the sensor monitors his activity that include the services he has used ,the files he has accessed ,time of login and time of logout .all these in formations are monitored by the sensors and are maintained as log file for future reference.

2.2AUTHENTICATION SERVER

In this paper the welcome screen is shown first. The authentication requires two inputs namely user name and password.If the information provided by the user is correct then it is allowed to access the services. If the information provided is wrong, an alert is generated and then it is asked to provide the proper information again. As soon as the user selects a particular service, the user is allocated a node with a new randomly generated rlogin id.

2.3 LOCAL IDS

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.It generally detects unwanted manipulations of computer systems, mainly through the Internet. The manipulations may take the form of attacks by crackers. An intrusion detection system is used to

2.3.1 Preprocessr: Checks the incoming data packets for potential maliciousness and it checks whether the Data packet is from unknown IP address. The preprocessor looks at every single packet. For example, the preprocessor determines whether or not the packet is part of an established connection and on port 80, otherwise the packet is ignored.

2.3.2 Signature Comparison: Compares the data with the attack signatures in the local attack database. If the data packet is found not malicious in the above two modules, then it is allowed to continue.

2.3.3 Action: If the data matches with any of the attack signatures, then one of the appropriate actions is taken.
DROP:If the action performed is drop then the particular data packet from the particular user is dropped.

2.3.4 CUT CONNECTION: In this part the connection of the user with the particular node is cut. The user cannot proceed to access the resource further.

2.3.5 ALARM: Alerts are generated when the user performs a suspect able task which is under the threshold. The alerts are used to track the intruder's actions.

components can be run at different consoles therefore giving a grid-like simulation.

All the components namely, theAuthentication Server, Sensor, Central Manager, and the seven nodes are made to listen at different port numbers which gives a feeling like they all run at different systems.

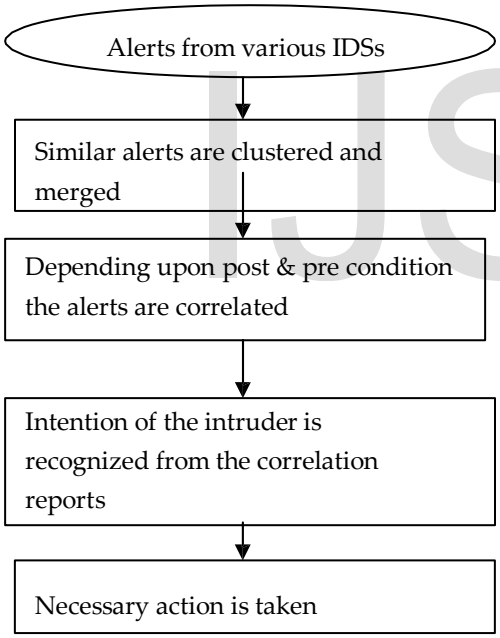
The sensor performs both routing and traffic monitoring to different nodes to look for malicious traffic. The Sensor looks up the port numbers of the entities that is stored in the database, for routing purpose. The IDSs running at all the nodes, the Authentication Server, and the Sensor, all generate alerts when they encounter a suspicious activity, which are directly forwarded to the Central Manager, where they are processed.

2.3.6 CENTRAL MANAGER:

In the grid environment for a intruder to attack a system he takes a number of steps which takes place in different nodes when these activities are suspected alerts are generated from different nodes .these distributed alerts have to be coordinated which is done in the central manager .the central has the following sub module

1.Alert clustering and merging
2.Alert correlation
3.Intention recognition
4.Reaction

FLOW OF EVENTS IN CENTRAL MANAGER



3.EXPERIMENT

3.1SIMULATION OF GRID ENVIRONMENT

The GUI in the simulation is done using Java Swing. In this project, the grid is simulated by 7 nodes, a sensor, an Authentication Server, and a Central Manager that have been simulated using Java Swing. The 6 nodes have 6 different services they can provide to the grid users. All the nodes have a local IDS running at each of them. Three default grid users are set with different usernames and corresponding passwords. All the

3.2 INTRUSION DETECTION METHODOLOGY

An example of grid database storing alerts is shown in Figure. Till now the alerts are called local alerts. Similar local alerts are clustered and merged into global alerts. Then the alerts are correlated based on some correlation rules and related alerts are correlated and correlation reports are generated. In this project, the correlations of alerts are done based on the pre-condition and post-condition of the alerts. Two alerts are said to be correlated if the pre-condition of one alert is the same as the post-condition of the other alert. From the correlation reports, the activities of the intruder till then are tracked and intruder plan and intention are recognized. Based on the intention of the user, the Central Manager takes appropriate action to neutralize the intruder plan. Thus intrusions are detected in the grid environment and neutralized by the GridSec DIDS architecture.

4.RESULT

The functions of central Manager simulation shows below

4.1 ALERTS:

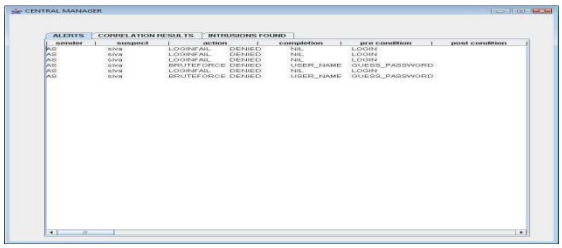


Figure 3.Alert from server to central Manager.

4.2 INTRUSION AND CORRELATION:

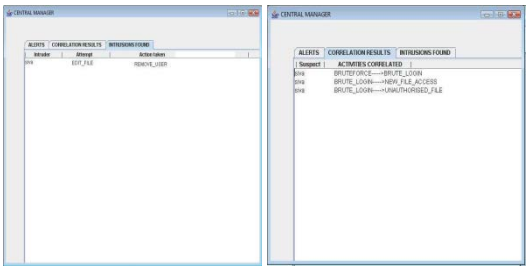


Figure 4.Intrusion and Correlation process.

4.3 DATABASE SCREEN SHOTS:

4.3.1 ALTER TABLE:

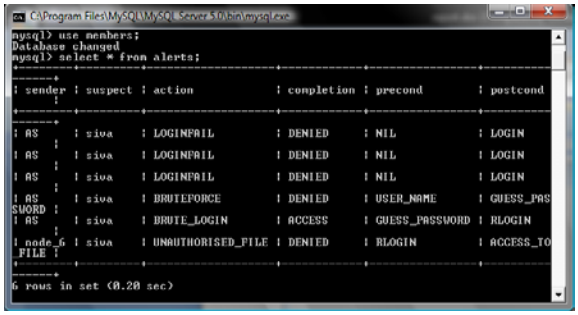


Figure 5.Database alter table process.

4.3.2 NODE TABLE:

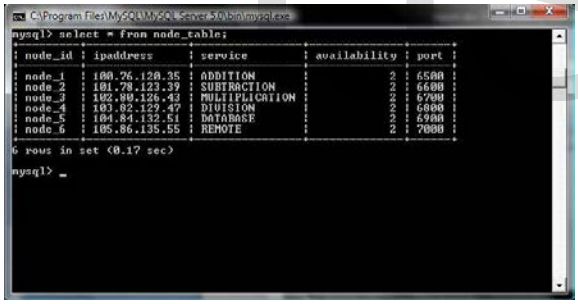


Figure 6.Node Creation for each request.

4.3.3 CURRENT USER TABLE:

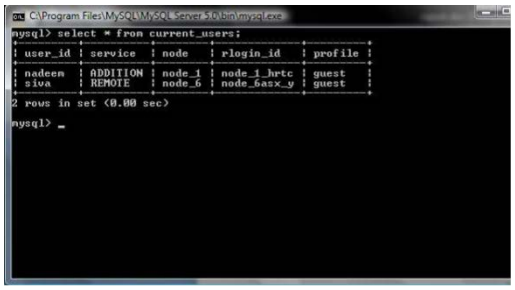


Figure 7.Current user based on our work.

5. CONCLUSION AND FUTURE WORK

In a highly distributed environment like grid, the problem of an intruder posing his attacks from node to node to attack the target has been handled by fixing a Central Manager at the heart of the GridSec DIDS architecture. The local IDSs are unable to identify intrusions since the attacker uses different nodes at different points in the course of his attack. To overcome this, the IDSs respond to a suspect by sending alerts to the Central Manager. The Central Manager stores all the alerts from various local IDSs in an alert database. The Central Manager clusters and merges similar alerts, correlates related alerts, and identifies the intrusions and the intruders from the correlation reports. The intentions of the intruders are recognized from the intrusion reports and their plans are neutralized as a reaction. Thus the GridSec DIDS not only identifies intruders, but also recognizes the intruder's plan and takes necessary reactions .

Further enhancements to the project can be made by adding many vulnerable services and providing many chances of intrusions to occur, and identifying them. Many more correlation rules can be devised concentrating on many more types of intrusions to improve the intrusion detection rate of the GridSec DIDS.Future works in this direction could be use of tuple reduction techniques for reprocessing in the Intrusion Detection Model.

6. REFERENCE

[1]. Farhan Abdel-Fattah, Zulkhairi Md. Dahalin and Shaidah Jusoh,"Dynamic Intrusion Detection Method forMobile AdHoc Networks Using CPDOD Algorithm", *IJCA Special Issues on "Mobile Ad-hoc Networks MANETs*, pp. 22-29, 2010.

[2]. Snehal A.mulay, P.R Devale, G.V.Garje, "Intrusion Detection System using Support Vector Machine and Decision Tree", *International Journal of Computer Applications*, Vol. No.3,pp.0975-8887, June 2010.

6.1 AUTHOR DETAILS:

MahaLingam .T obtained Masters Degree in Bharahadasan Univeristy,pursuing Ph.d in Satyabama University and working as Associate professor in Bhajarang Engineering College.

Jeevitha.R, obtained Masters Degree in Sai Ram Engineeering College,(**Anna University Rank Holder**) and working as Assistant Professor in Bhajarang Engineering College.