ISSN 2250-3153

Intrusion Detection System

Kashish Kukreja, Yugal Karamchandani, Niraj Khandelwal, Kajal Jewani

Department of Computer Science, Vivekanand Education Society's Institute of Technology, Mumbai, INDIA

Abstract- In our project we have implemented an intrusion detection mechanism in NFS (Network File System). As NFS is a distributed file system and there is no pre-defined authentication mechanism in NFS, it inspired us to go ahead with this project. Intrusion detection can act as a layer of security as it distinguishes legitimate clients and intruders. In this project we have decided on certain parameters related to the client (for example -used id, password, number of mount requests etc.). These parameters are stored in a log file. Then these parameters are compared to parameter thresholds from the access control list file in order to detect anomalous behavior of the client. The basis for intrusion detection is a parameter named sum. Sum is the combination of all parameters. These parameters are scaled by a particular factor depending on their importance in determining the client's behavior. If the value of sum for a particular client is greater than threshold then it is identified as a normal client and it is granted access but if the value of sum is less than zero then the client is identified as an intruder and it is sent to decoy.

Index Terms- Client, Server, NFS

I. INTRODUCTION

As computer networking grows more important in daily usage, Its security is also paramount. Intrusion Detection System (IDS) is an important and integrated component of computer network infrastructure. As a network security watchdog, IDS is often Deployed at the border of enterprise network. Because of ever-increasing volume of clients and network complexity, there is a Need of better IDS that can deliver result in real-time. As we are working with NFS (Network File System) and there is no provision for authentication in NFS, it motivated us to design a mechanism similar to intrusion detection system in order to provide a layer of security to NFS.There is an NFS server that has data files and it allows client to mount and get access to the Data. There are multiple clients that can request mount to the Server. In order to get a mount response the client must Authenticate itself with a valid user id and password pair. The Details regarding the clients' activities are stored in a log file. Different thresholds are defined for different client parameters and these thresholds are compared to the actual values of the client parameters in order to distinguish between normal clients And intruders.

II. LITERATURE SURVEY

Intrusion detection systems (IDS) monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service Attack). A typical example is a system that watches for large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is Attempting a TCP port scan. An IDS may run either on the target machine who watches its own traffic (usually integrated with the stack and services themselves), or on an independent machine Promiscuously watching all network traffic (hub, router, probe). Note that a "network" IDS monitors many machines, whereas the others monitor only a single machine (the one they are installed on). Intrusion Detection systems can be classified into three Categories based on the types of data they examine. These are:
Host Based IDS
Network Based IDS
Application Based IDS

In the host based approach every host has its own IDS and it collects data in the low level operations like network system calls (Monitoring connection attempts to a port, etc.). A network based IDS collects data in the network level, transparently to the Other hosts. Their sensors are located somewhere in the network And monitor network traffic. And the third type of IDS, the application based approach uses data sources from running Applications as its input.

Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much Like local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system. The Network File System is an open defined in RFCs, allowing anyone to implement the protocol. NFS is often used with UNIX operating systems (such as Solaris, AIX and HP-UX) and Unix-like operating systems (Such as Linux and FreeBSD). It is also available to operating such as the classic Mac OS, OpenVMS, Microsoft Windows, Novell NetWare, and IBM AS/400.

III. ALGORITHM

1. Server and Clients Starts
2. The client who wants to access data on the server will send a mount request to the server
3. For sending the mount request the client has to authenticate itself to the server.
4. If the user id and password are correct then the mount request is made.
5. When the mount request is made the client's attributes are stored in a log file.

6. These attributes are then compared with the thresholds specified in the ACL file.
7. The SUM attribute is calculated depending on the parameters like no. of dos attempts, no. of wrong passwords etc.
8. If the value of SUM is greater than a particular threshold then the client is identified as a normal client and mount request is served. The client can then access the shared data.
9. If the value of SUM is less than the threshold then the client is identified as a potential intruder and sent to decoy.
10. If a mounted client sends an unmount request then it is unmounted and it can no longer access the data.

IV. SYSTEM BLOCK DIAGRAM

Systems are created to solve problems. One can think of the systems approach as an organized way of dealing with a problem. In this dynamic world, the subject System Analysis and Design, mainly deals with the software development activities

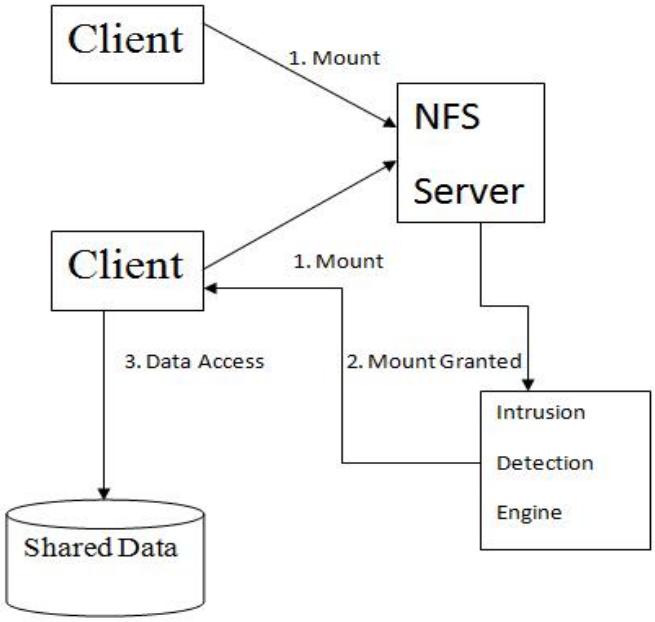

Fig 3.5 System block diagram

V. RESULT ANALYSIS

The Crucial parameter for intrusion detection is the sum parameter which is a combination of various other parameters. Sum is calculated as follows

Sum=5*(No. of Dos attempts) + 4*(Current time-1st start time/no. of mount) + 3*(No. of times wrong password entered) +2*(No. of accesses in unallowed time period) +1*(Total elapsed time/No. of times successfully mounted.)

The scaling factors 5, 4,3,2,1 are demo values and these values can change at run time. These values are priorities of particular and they are different for different clients.

The other parameters are the fields of the 3 log files and some of them are as follows:

- IP address
- User id
- Password
- No. of DOS attempts
- No. of times wrong password entered
- Start time
- End time
- Total Elapsed time etc.

VI. CONCLUSION

Thus we have designed an authentication and intrusion detection mechanism for network file system. As NFS works in a distributed environment, this mechanism can prove useful as it will protect crucial data from illegitimate users. As there is no predefined security mechanism in NFS, this mechanism can be employed as a first level of security.

ACKNOWLEDGMENT

We are thankful to our college Vivekanand Education Society's Institute of Technology for considering our project and extending help at all stages needed during our work of collecting information regarding the project.

It gives us immense pleasure to express our deep and sincere gratitude to Assistant Professor **Prof. Kajal Jewani (**Project Guide) for her kind help and valuable advice during the development of project synopsis and for her guidance and suggestions. We are deeply indebted to Head of the Computer Department **Dr.(Mrs.)Nupur Giri Ma'am** and our Principal **Dr. (Mrs.) J.M. Nair Ma'am**, for giving us this valuable opportunity to do this project.

We express our hearty thanks to them for their assistance without which it would have been difficult in finishing this project synopsis and project review successfully.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support and selfless help throughout the project work. It is great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Engineering. We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement at several times.

REFERENCES

[1] Marks, Crosby, former Haystack Project team member and Haystack Labs employee, telephone interview, September 3, 2001.

[2] McHugh, J. et al. "Intrusion Detection: Implementation and Operational Issues," Software Engineering Institute Computer Emergency Response Team White Paper, January 2001.

[3] Power, Richard, "1999 CSI/FBI Computer Crime and Security Survey," Computer Security Journal, Volume XV, Number 2, 1999, pp. 32.

[4] Proctor, Paul, the Practical Intrusion Detection Handbook, Prentice Hall, 2001.

[5] Sans Institute, "Intrusion Detection and Vulnerability Testing Tools: What Works" Feb 2001.

[6] http://en.wikipedia.org/wiki/Network_intrusion_detection_sys tem

[7] http://www.linuxsecurity.com/resource_files/intrusion_detecti on/network-intrusiondetection.html
[8] http://www.windowsecurity.com/articles/IDS-Part2- Classification-methods-techniques.html#
[9] http://www.securityfocus.com/infocus/1203
[10] http://www.bruggerink.com/~zow/papers/brugger_dmnid.pdf

AUTHORS

First Author – Kashish Kukreja, pursuing B.E, Vivekanand Education Society's Institute of Technology, kashish.kukreja696@gmail.com.
Second Author – Yugal Karamchandani, pursuing B.E, Vivekanand Education Society's Institute of Technology, yugalkaramchandani@gmail.com.
Third Author – Niraj Khandelwal, pursuing B.E, Vivekanand Education Society's Institute of Technology, nirajkhandelwal.nk@gmail.com.
Fourth Author – Kajal Jewani, M.E, Vidyalankar Institute of Technology, kajal.jewani@ves.ac.in