International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June 2018 www.irjet.net p-ISSN: 2395-0072

Managing Security of Systems by Data Collection

Manisha. M. B[1], Dr. D. K. Mallick[2]

[1]*M.Tech Scholar, Dept. of Computer Science & Engineering, Birla Institute of Technology, Mesra, Jharkhand, India*
[2]*Associate Professor, Dept. of Computer Science & Engineering, Birla Institute of Technology, Mesra, Jharkhand, India*

Abstract – *A computer system is as secure as the components maintaining the security of the system. In this paper, we see how to collect and manage data of client systems using database server. In order to detect intrusion in the system, information related to security are defined and stored in the database. Based on the collected and analyzed information from each monitored system, we can know their status and take action according to it. Furthermore, we also discuss other security management techniques in this paper.*

Key Words: **Intranet, Computer Network, Security Management, Security Information Collection, Intrusion Detection**

1. INTRODUCTION

The growth of technology in this modern world is increasing day by day. In each field and organization, the need to protect their information stored digitally in the system has become critical. Thus, managing the security of these information, is the first thing any organization must look into.

Information is an asset to all individuals and businesses. Information security is intended to ensure the confidentiality, integrity and availability (CIA) of computer system data from any malevolent intension. We can manage the security of information by collecting, monitoring and analysing security related data.

An organization in today's generation is generally heavily dependent on its network infrastructure for achieving its desired goals. Computing is only possible with the availability of secure network. However, the realization of security lies in managing the services and integrated approach. Most organizations lack the ability to detect virus infection or vulnerable node.

Every node (PC) needs to be managed through a centralized console to cater to all the requirements of IT compliance, viz. implementation, enforcement, monitoring and reporting. An application with this requirement would ensure that a database connected server gets all the intelligence of the health parameters of the nodes.

Fear of security breaches on Internet is making companies use private networks to protect themselves. Though Intranets are safer than Internet, it is not immune to vulnerability or attacks. Connecting virus infected external hard drive to a single computer in the Intranetwork can cause a widespread infection to connected computers if they are not managed. Our working environment will be Intranetwork with workstations, desktops and servers as our client system.

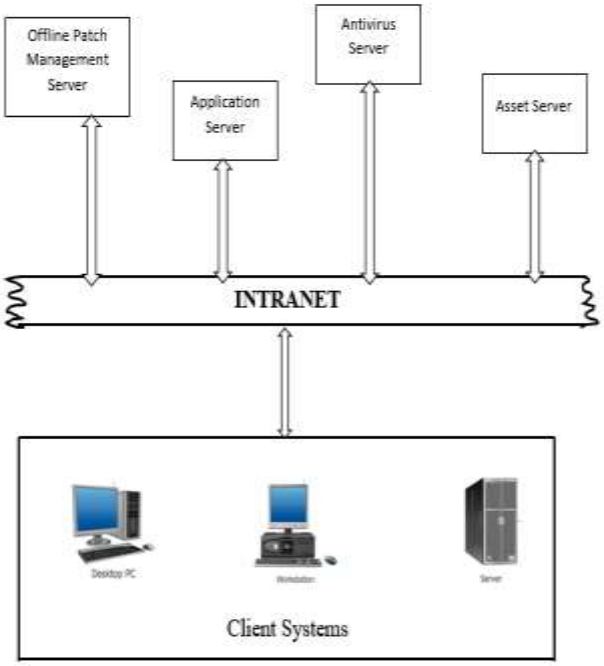

Fig -1: Working Environment

The above Fig 1 shows the block schematic representation of our working environment. Application server, Antivirus Server, Asset Server and Offline Patch Management Server are connected through Intranetwork.

We are creating an application which detects any change in the system as their details are collected regularly from the server. The tasks that the application does is documented and available for retrieving, disseminating, re-arranging and storing the same to database. While the server module will co-ordinate with other servers for data interchange so as to provide integration.

The application reads registry contents, group policy settings, monitor security settings, send status to server on client health, update registry settings, etc. It would have to negotiate the Windows OS security layers to work smoothly. The behaviour of different OS should also be taken care of.

This application also checks if the required patches and service packs are installed, if not it should be able to automatically install it. It is also bi-directional i.e, able to take commands and give the required output back to application server. It collects all security relayed information of clients and store them in database. These records are used to analyse and detect security issues.

2. METHODOLOGY

In this paper, we are using Visual Studio to create an application which will get system information through which we can manage security of the system. We will be collecting data of each system, which will be useful to monitor and detect any unwanted component. These information are sent to SQL Server to store them. Separate servers are maintained to manage separate components as seen in Fig 1, so as to make it easier to manage.

The main feature of our application which differs from other techniques is that, the communication between application and server is bidirectional communication. As we are making the application bi-directional, we are not only able to collect the information of systems but also can send simple commands to it. We can command the application to get only one particular information we want or we can ask it stop collecting any information altogether. We have also added pause and resume features.

Timer is one of the important feature of this application. We are adding interval timer to the application, so that we can collect the information according to the regular interval time it is set. By default the interval time is set to few minutes. As this is bidirectional application, we can change the interval time of a particular system using its IP Address. Some systems need to be monitored more regularly than others. So we can keep very less interval time for systems which we doubt may be vulnerable. We can use SQL Server of the application to change the interval timer. Every few seconds the application will be checking database for any new entry. When we insert only interval time, it will be applied to all the system having the application. If we insert IP Address along with the interval time, then only that system's timer will be changed.

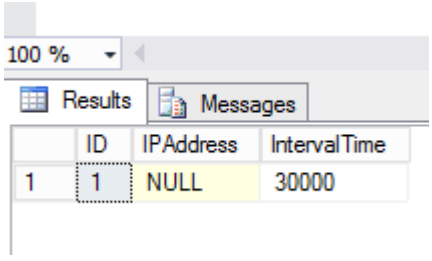

Fig -2: Timer without IP Address

In Fig 2, we see 30 seconds (30000 microseconds) being set as interval time to all the client systems as we are not providing any IP Address along with it.

In the next figure, Fig 3, we are setting 30 seconds as interval time for system having IP Address (ending with) 36 and 50 seconds for system having IP Address 31.

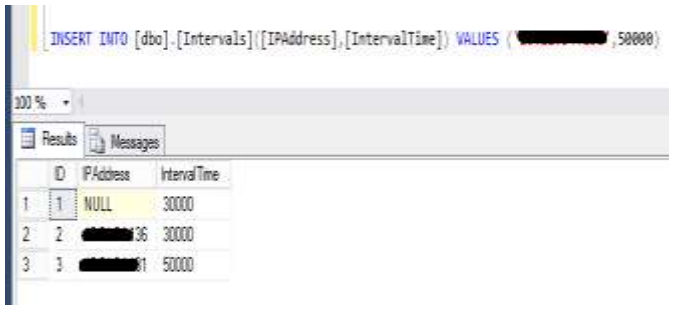

Fig -3: Timer without IP Address

The application or monitoring server is connected and integrated with other servers as shown in Fig 4.

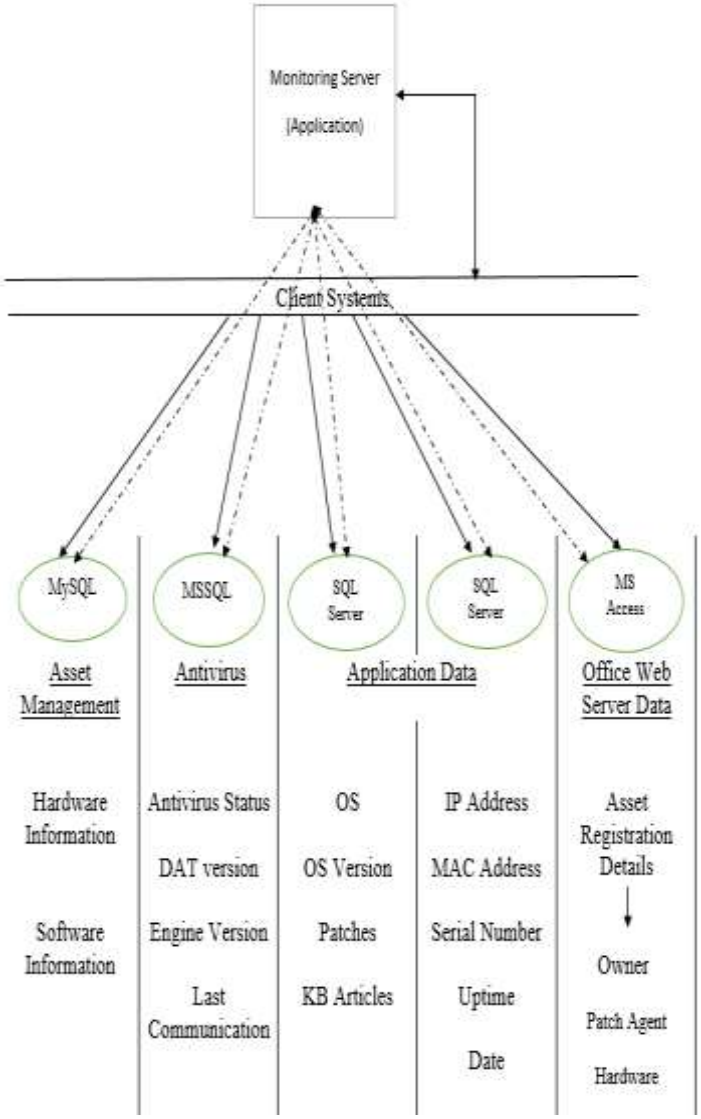

Fig -4: Integrating all servers

Different servers maintaining different components of the system will be using different type of databases according to their prerequisites. Our application collects all the details required to analyze from these servers. It checks if there has been any unusual activity in the system. If any activity has occurred without the knowledge of user, it will either notify the administrator or store them in server. It checks the main three features to manage security: - Confidentiality, Integrity and Availability. If any vulnerable or unlicensed version of softwares are installed without the permission of administrator, it will be considered as intrusion and will be notified.

The application will not be having any GUI. But the application will be running in background and will be shown by an icon in system tray as soon as it is installed. Once the application is installed, that system will be given unique vale in the database. Each system hosting the application will have unique values, through will it will be recognized. Only administrator has the right to uninstall the application. Before uninstalling, the application will send notification to the server and store the time in database.

3. RELATED WORK

There exists many security management tools, each with its own techniques. In this section we are going to see some of these techniques, which helped us in creating our own technique for making an application.

3.1 Intrusion Detection System

Intrusion Detection is the most commonly used technique to alert the vulnerability of the system or to detect when any unwanted component get inside our system. As soon as IDS detects malicious activity or policy violation, it is usually reported to either administrator or collected and stored in the server for analyzing and managing security of information.

Intrusion detection system are classified into:

- Active IDS – is configured to prevent attacks without any external commands, as soon as they are detected.
- Passive IDS – as opposed to active IDS, only monitors and detect attacks or intrusions if any found.
- Host IDS – can monitor only the systems where the software application (agents) are installed and it cannot check entire network for intrusion.
- Network IDS – is kept inside the network segment and monitors all the ingoing & outgoing traffic on network.

In [1], advantages and disadvantages of each type of data collection mechanisms for intrusion detection system are discussed. The authors also mention how data collection is important as they are used to make decision whether system is attacked or not. If the data is incorrect, it may affect IDS and give false sense of security.

Intrusion Detection Systems are also classified based on their component distribution [2]:

- Centralized IDS – is the system where the analysis of information are done in a fixed number of location. Location of data collection does not matter as long as we know the location of analysis.
- Distributed IDS – is the system where the analysis of information are done in more than one location based on number of hosts that are being monitored.

3.2 Security Management using Agent

In [3], authors suggest security manager and agent to monitor and oppose intrusion to the system from outside. Security Agents defines security information and it collects them according to the security policy.

Security Agent executed on local system. It collects information related to security, user information, group information and file information to make sure of the integrity of system files. These information are then sent to Security Manager, which analyses and gives the result.

As the authors of [4] propose, Intelligent Agent are being used in different application areas and functionality. IA technology provides more efficient way in managing security. Their paper show how the multiple autonomous and intelligent agents communicate and use information to perform intrusion detection task efficiently. The agent is made to monitor all incoming and outgoing connections. It can trace intruder by shifting to the working host.

The advantages of using agent for network management is given in [5]. Some of them are:

- The agent handles queries by sending from client to the server. It then carry out task and send the results back to client after completing it. Thus, only agents can be used to exchange information across the network, instead of results and information being sent back and forth.
- Agent architecture gives more flexibility by allowing agent to visit several nodes on the network to carry out required tasks.
- Agent architecture also solves problems created by an unreliable network. For remote monitoring, this would be the best option.

3.3 Protecting Log Files

Log files are one of the important things to consider while managing security of the system. [6] Mentions how to enhance network security by locking down log files. Log files record network traffic, IP Addresses trying to access the system through network, date and time of the attempt. Thus protecting log files to ensure security is important.

Some of the ways to protect log files as mentioned in [6] are:

- Should not allow log files to be edited or delete information. Should be allowed only to append new data.
- Only system administrator must be given permission to configure log files.
- Applying password on log files or directory containing it

3.4 Client/Server Method

Ad-hoc management and Centralized are the 2 approaches which use client/server model to manage network in [7].

- Ad-hoc management approach uses a set of scripts which are written to focus on small tasks like calculating the load or checking configuration parameters. But this approach is very time consuming and expensive.
- Centralized approach uses single application to handle other areas for managing network. It is a very complex approach.

4. CONCLUSIONS

We have reviewed other methods and technology, which helped us in creating our own technique.

We conclude this paper by mentioning that our method gives a bi-directional approach, which is more effective and easier to manage the security. We collect all security related information and store in database, so that the records can be analyzed and compared to form a firm decision. Our application can deal actively when any security issues are detected.

REFERENCES

[1] Eugene Spafford and Diego Zamboni, "Data collection mechanisms for intrusion detection systems," Prude University, CERIAS Tech Report 2000-08, June 2, 2000

[2] Eugene Spafford and Diego Zamboni, "Intrusion detection using autonomous agents," ELSEVIER, Computer Networks 34 (2000) 547-570, 2000.

[3] Soon Choul Kim, Young Su Choi and Jin Wook Chung, "Study of Security Management System based on Client/Server model," ICC 1999 - IEEE International Conference on Communications, no. 1, June 1999 pp. 1403-1408.

[4] K. Boudaoud, N. Agoulmine and J.N De Souza, "Distributed Network Security Management Using Intelligent Agents, "LANOMS, 1999.

[5] W.J. Buchanan, M. Naylor and A.V. Scott, "Enhancing Network Management using Mobile Agents," IEEE International Conference on Engineering of Computer Based Systems, 2000.

[6] B Lantz, R Hall, J Couraud, "Locking Down Log Files: Enhancing Network Security By Protecting Log Files," IACIS, Issues in Information Systems, 2006.

[7] Osman Ertugay, Michael Hicks, Jonathan M. Smith and Jessica Kornblum, "Agents in Network Management," University of Pennsylvania Scholarly Commons, Technical Reports (CIS), Feb 2000.