International Journal of Students Research in Technology & Management

Vol 1(3), May 2013, ISBN 978-93-83006-01-4, pg 342-346

A SERVER HARDENING FRAMEWORK

Siddharth Singh, Garima

Department of IT, Army Institute of Technology, Pune, Maharashtra, India

si9224@gmail.com, garimasingh2692@gmail.com

Abstract

There have been several attempts at improving the security of servers in all the fields be it web servers like apache tomcat ,mail servers like wamp etc. Checklists have been made for different servers from time to time which contains a list of steps that have to be followed in order to improve the security of the particular server. So the user has to have all the basic knowledge about the server before he can make use of the checklist and secure the server. This is the first problem that the user has to be well versed in the basic technicalities of the server configuration before he can secure it for use. Secondly ,till now there is no tool or framework that can bring all the different types of servers together under it so that a single framework can be used to harden or secure multiple number of servers and without any knowledge about the basic configuration of the servers .Hence, we propose to automate the server hardening process by creating a Framework which will be open source and hence new servers could be included in it by users by editing the open source code of the framework which would be in python language. A server hardening framework would help even a person with a layman understanding to secure the server which he is using. He would be able to use the framework for hardening a multiple types of servers as per his requirements. The Framework will provide an option of AUDITING as well as HARDENING. If the User chooses the AUDITING option , then the parameters of the server configuration file would be displayed along with the current values as well as it would be mentioned additionally for the parameters if a particular parameter requires hardening and again the user would be asked if he wants to harden it or not. In case of choosing hardening, the server configuration file would be replaced by hardened file and server be restarted.

Keywords - Server hardening, auditing, parameter, Framework

I. INTRODUCTION

Server Hardening: Server hardening is a process of enhancing server security through a variety of means resulting in a much more secure server operating environment which is due to the advanced security measures that are put in place during the server hardening process.

Server Hardening is probably one of the most important tasks to be handled on your servers, becomes more understandable when you realize all the risks involved. To protect your servers you must

establish solid and sophisticated server hardening policies for all servers in your organization. Developing a server hardening checklist would likely be a great first step in increasing your server and network security. Make sure that your checklist includes minimum security practices that you expect of your staff. If you go with a consultant you can provide them with your server hardening checklist to use as a baseline. Servers are relied upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

II. LITERATURE SURVEY

A .Working of Servers

To understand how a server works, it helps to understand what it is, since the name itself can refer to any number of devices and applications. A server can be a computer or a software application, depending on how it'll be used. The difference is that a computer will typically be used to coordinate the activities of a network of computers, whereas a software application manages user access to certain areas of a system's network.

Servers are designed to carry out a number of different tasks, some of which include file management, printer assignments, email storage and delivery and fax assignments. Integral to the server purpose is the client-server relationship between computers within a network. Within this setup, the computer responsible for coordinating network activities is the server, while the client computers would make up its network.

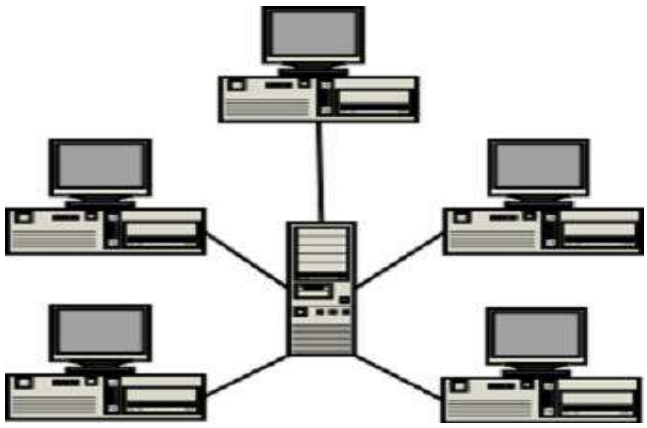

Fig.1 LAN

B. Network Server

Network servers can be set up to handle a number of different processing functions, some of which include FTP requests and web requests, as well as email and proxy requests. Because of the additional work tasks carried out by network servers, these computers have to have more processing, storage and memory capacity than their client counterparts. Networks are usually found within business settings where file, print and email sharing are central to workplace flow.

A network server coordinates processing tasks by sharing its own resources or running applications for its client users. The convenience in using a network means one computer can arrange to have 20 other computers share one printer, as opposed to all 20 computers having a printer each. The type of operating system needed to run a network will depend on what function the computer will serve.

C .Web Server

Being able to pull up a website is made possible by software applications known as web servers. These applications convert online data into readable words and viewable images on the screen. Web hosting is another type of online server that works something like a network, except the client users are individual websites rather than computer terminals. Hosting sites typically rent out space to web users and assign specific web addresses for each space.

Yet another type of web server exists as an Internet service provider, such as the service that provides your Internet access. These types send and retrieve web pages on your behalf using Internet protocols and HTML mark-up language. There are a number of web servers online, all of which cooperate with each other in order to get online users from one place to another.

D. Securing Tomcat

Basically, here we have looked into the default configurations of the Apache Tomcat 5.5 and the steps that can be taken to secure the Tomcat further by making changes in the server configuration file server.xml. For example changing the default port from 8080 to 80 and enabling the SSL port, then changing the shutdown string from ‘SHUTDOWN’ to something more complex.

E. Problem Definition

Design and implementation of a Server Hardening Framework to automate the Server Hardening process which also expands according to the users changing requirements from time to time.
This work can be carried out in two parts.
1. By auditing: The procedure is to customise the hardening as per the user wants.
2. By hardening: The procedure is to harden the server as per the template already provided by the admin.

III. HCF

The approach is to create 'Hardened Configuration files' and store it in the application folder for each of the servers. Whenever the user requests for auditing we compare the user's server configuration file parameters values with the already hardened file parameters. If any of the parameter's value differs from the hardened value then the 'Needs hardening tag is put in front of the parameter. Again the user is asked if he wants to harden the file after auditing it. If he says yes, the user's server configuration file would be replaced by respective server's HCF file and the server would be restarted for the changes to come into effect. The user would be asked the path of the selected server configuration file and which would be stored in the database MYSQL for further references. The Framework being open Source the servers can be added by the users as per their requirement by editing the application in python. More number of the HCFs can be added as per the users requirements.

IV. ADVANTAGES

- The Framework provides a common tool for server hardening for different servers under the same framework.
- It is open source and so the new servers can be added as per changing requirements of the users.
- It helps even a layman who doesn't have in depth knowledge of server configurations to secure a server.
- It provides automation of server hardening which till recently was done by downloading the checklists for different servers and manually hardening the servers.

V. APPLICATION

The applications includes

- Each Corporate company contains internal networks between different departments. The main server would be secured by the system administrator.
- The corporate's internal network server would be protected from attacks from outside through the internet by checking the ports which are unnecessary open.
- In defense sector, the database servers can be secured from hacking attempts on the machines by the enemy forces.
- In universities, the confidential data of students can be secured as the server machine would be secured using the framework.

VI. CONCLUSION

The framework developed would thus help the corporate to keep the internal data intact as well secure their database servers. It would help the defense sector to secure their confidential information more secure on their servers and minimize loss in case of breach. It will also be very useful for the universities to protect the particulars of students and confidential information on servers.

VII. REFERENCES

1. http://www.networkworld.com/columnists/2004/0503sleuths.html?page=2
2. https://www.owasp.org/index.php/Securing_tomcat
3. http://www.ehow.com/how-does_4899740_a-server-work.html
4. http://tomcat.apache.org/tomcat-5.5-doc/config/index.html
5. http://www.serverhardening.com/
6. http://en.wikipedia.org/wiki/Open_source