Linux server security and hardening

Engineering, Computer Security

The main purpose of the case study is to illustrate an understanding about the topic Server hardening. Server hardening means securing or protecting the server from unauthorized access of users, protection from virus and malware. Once we done with the case study we will be able to provide a basic idea about what is hardening, how to secure the server, and mainly why is it required? Here we are going to discuss about how harden the base operating system, firewalling and securing the host connections.

Securing the server will reduce the increase in risk. Servers are used mainly in corporate world, and their date is very much confidential. So all these data need to be secured and also many applications too. Here we will concentrate more about Linux Server Hardening. In order to protect the Linux server we need to look into many areas like Linux host, main applications like e-mail, FTP, DNS and base operating system. There are many ways to harden the Linux server. Going forward we will discuss more on how to harden the server, what are the ways to secure the server and benefits and drawbacks of these methods?

Many ways can be used to secure a system. The ultimate of goal of this is to secure the system. This could be by the uninstallation/removal of an existing service or a software component. We will start from physical security measures to prevent unwanted access to the server. There is common belief that Linux is a secure OS, it is partially true and partially not. It is derived from UNIX operating system, so the process is different for a user logged into the system has limitations on what he can do in that system. After reading this report an administrator should be able to get an idea about making security related choices and decisions.

Linux system is built in such a way that the security policies are imposed. Attacking a system is like to try to overcome privilege restrictions that the system administrator is anticipated scenario. A hardened system increases the bar by dropping the area that the system exposes to the attacker (it is known as attack surface). A hardened system can help in preventing measures to reduce the effect of susceptibilities in the parts of the systems that must be visible to a potential attacker.

Linux Kernel security is considered into different module such as file system security, Access control, and network security. We will discuss about each model briefly.

Why Server Hardening is Necessary?

What will happen if the server is not secured? This is a big question for a layman. Think about a house which is not locked and it contains lot of valuable things inside it. Hackers will come inside and steel all the valuables; this is the same in the case of a Server. If we did not secure it properly, the valuable data may get hacked by others. Now we will discuss more detailed about the different methods on how to secure the Linux server.

Steps to Remember before planning

Before planning to make any implementation need to know more about the security architecture. There should be certain rules and security models already available. It always follows some frame work for easy execution. These common principles are known as “ CIA triad” (confidentiality, Integrity and availability).

Threats:

Anything and everything can make damage or serious problem to the working system/server/computer can be called as threat.

Basics of Server Security

This discussion will give you the capability to apply security enhancement techniques to a wider range of server-based services and programs. We can split the security in different level like Physical security, Security Policies and Procedures, Monitoring the system, Automation, Management, Network security, Remote Access etc. Going forward we will discuss more on these.

1. Physical Security

Physical security should be the highest concerns. Linux production servers should be in kept in a datacenter and should lock in all the time, provide access to the people who passed security checks. Depending on the circumstances, you can think about providing boot loader passwords. The amount of physical security required on a particular system depends on the situation, and can also vary widely by available funds.

2. System lock

Most of the datacenters have their own locking mechanism. Usually this will be a hasp/cylinder lock on the front of the rack that allows you to turn an included key to a locked or unlocked position – granting or denying entry. Some servers also have case locks. These locks can do diverse things according to the design of the system vendor and construction.

3. Locking down the BIOS

The BIOS (Basic Input/output System) is the lowest level of software that decrees system alignment and low-level hardware. BIOS varieties allow setting Boot level password for security.

4. Boot Loader Security

GRUB2 is the Linux default boot loader and can set the boot password. If a password is definite, GRUB 2 will prohibit any interactive control until you press the key C and E and enter a correct password. There is one main thing to keep in mind, whenever you are setting up the password need to remember the same.

5. Firewall

IP tables are used for firewalling, but different companies use different firewalls to protect their production network.

6. SELinux

SELinux (Security enhanced Linux) is an advanced technology used for securing the Linux systems. It is anothet security architecture integrated into the 2. 6. x kernel using the Linux Security Modules (LSM). SELinux provides a flexible Mandatory Access Control (MAC) system erected into the Linux kernel. SELinux defines the access and change rights of every user, application, process, and file on the system.

7. Removing Unwanted Packages (RPMs)

It is very important step in securing a Linux system is to regulate the primary functions of the Linux server. Or else it will be difficult to know what needs to

be secured. Therefore, it is critical to look at the default list of software packages and remove any avoidable packages.

8. Patching the Server

Building an arrangement for patch management is a very important part of a proactive and secure production Linux environment. It is suggested to have a written policy and procedure to handle Linux security updates. Network related security vulnerabilities should be in high priority list and should be addressed instantly. The assessment stage should happen within a testing lab, and initial roll out should happen on development systems.

9. File Systems: Securing NFS

NFS (Network File System) is used to share files over a network. But like all network services using NFS involves risks. There are some basic rules given.

- If not required NFS should not be enabled.
- Use a TCP wrapper to restrict remote access, if NFS is really needed.
- While providing the access ensure to provide for needed one only
- In order to weaken spoofing attempts use fully qualified domain names.
- Try to export read only if possible.
- Use only NFS over TC.

Without any doubt we can say that Linux based operating systems are is king of all operating system. This is why because Linux is an open sourced OS and which makes developers attracted towards it. Being open source means that any of the device engineer, programmer, or amateur hacker can download it, hoax with it and build their own custom version.

If we search for the vulnerability bout Linux kernel 2. 6. 32 currently shows almost 182 known vulnerabilities. Many of them are pretty serious. We need to keep in mind is that which kernel version is patched against the known vulnerability.

Audit Details

An analysis on the system response to various foot printing and brute force attacks was performed. There was an audit done in the server for verifying any alert and monitoring system as well as invasion prevention system. Following are the areas of audit and the associated discovery. Audit is been conducted in the below areas.

- Unwanted programs and applications: rpm –qa | less will give the list of installed applications.
- Unnecessary Services running: All the services running on the server will list by the command: ps aux | less
- Password policy: The system which we checked was not set up any password policy. A user can set any password like 123 or a dictionary word. There is no minimum character length specification policy. So it is easy to hack.
- Secure shell security (SSL): SSH is used access the machine remotely. This is a main tool where in the admin is using. So it is very important to secure the SSH. Upon verification noticed that the default SSH port 22 is set for this which is known for everyone.
- Firewall: While checking the status of the firewall (IP Tables) which is inbuilt in Linux OS found to turned off. If the fore is not in ON state and

not configured properly it is easy for the attackers to hack it from any network.

If the server is properly configured the Linux servers are very reliable and secure. As it is an open source Linux it is free more over with this OS many of the applications are free to use. If we rectify all the above issues the cost is about reduce 80%. If the attack risk is not lowered, the impact to project will be credibly high. The lower in the implementation cost means, there are no chances of cost over run which could result in reduced staffing.

Post Implementation Support Resources and Maintenance Plan

After implementing the solutions, it requires continuous maintenance and support people's attention. Periodic modification, analysis and up gradation is required. For short term maintenance of the Information System, systems administrators need to be trained well to operate the firewall and the intrusion detection system. They should be in a position to perform daily operations on the firewall and the intrusion detection system. Thinking about long term the company should hire a well experienced and skilled administrators server implementation and high availability. Need to set up proper backup and recovery procedure, disaster recovery and business continuity plans.

Conclusion

In conclusion this case study about the server hardening and security of Linux servers we have discussed about the various problems associated with Linux servers if it is not secured or hardened and the prevention mechanisms to overcome from this issue. Many attacks start with the information collecting or the scanning phases, where they usually run a scan

through a range of random IP Addresses. The decision taking factor is the result of the scans malicious attackers on which IP Address to include for next phase or which ones to exclude.

Even though the case study is not complete solution for hardening and security for Linux servers, it gives a basic idea about the security aspects of Linux server. Here I tried to give the basic procedure to securing the server. The major areas of learning during this project were the architecture of the Linux Operating System, working model and the response of the system to various attacks.