Enhancing Security in Linux OS

Ashvini T. Deshmukh
Department of Computer Engg,
Smt. Kashibai Navale college of Engineering,
University of Pune, MH, India.

Parikshit N. Mahalle
Department of Computer Engg,
Smt. Kashibai Navale college of Engineering,
University of Pune, MH, India.

ABSTRACT

The security of Linux depends on many configuration file both at system level and application level. Most important is security of the Linux system is never static. Once you secure your Linux system it does not perpetually stay secure because operational and functional changes had done through threats or new exploits are available for packages or applications hence need of secure system .The primary focus of this paper is securing Linux production system. There are many Linux Security requirements that need to pass various audits in an enterprise. Linux has many configuration files and many configuration files consist of security attributes which are the focus of this paper. This paper consists some standard security practices which are basic for Linux security.

.

General Terms

Linux , Security, Attacks,Risk,Algorithms.

Keywords

Computer Security, Security Parameter, Threats, Script, Vulnerability.

1. INTRODUCTION

Linux is open source operating system. It is free to modify. Computer security is a general term that covers a wide area of computing and information processing. The biggest problem people is securing anything is the very narrow scope. They are not sure about what to secure and how to secure it. This is because people don’t fully understand what security is. But most likely it’s because security is such a loaded word that it can mean too many things [1] . Security is “separation of an asset from a threat.” So to separate the threat from the asset, you have three options: Physically remove or separate the asset from the threat, Destroy the threat, Move or destroy the asset. In practical terms, destroying the asset is undesirable and destroying the threat is often too complicated or illegal. However, separating the two is normally achievable. Computer security is often divided into three distinct master categories, commonly referred to as controls[2] : Physical, Technical and Administrative control. Administrative security is our main objective. Providing administrative security is nothing but define the human factors of security. It defines which user have to what type of access . e.g. Personal registration and account checking. We need security for Confidentiality, Integrity, Availability of data. Nowadays vulnerabilities are addressed in different areas such as OS vulnerabilities, server application vulnerabilities and non-server application vulnerabilities. Because of popularity of the Internet and it was one of the most important developments that prompted an intensified effort in data security. This paper offers a good baseline for Linux system compliant with various audit requirements. Linux security requirements including account policies for Linux systems that are being audited is main objective of Linux security discussion. Linux is secure but it’s security comes in picture when it’s security parameter are set to good practices i.e standard values of security parameter then only linux become more secured.

1.1 Areas Where We Can Enhancing Linux Security Are

Workstation Security , Network Security and Server Security. Vulnerabilities which we addressed regarding this three areas was mentioned in [3]. How security is enhanced in above three security areas are explained in literature survey.

1.2 Verifying Security Action Items and Proposed Idea

There is number of vulnerabilities in Linux, so need of checking these vulnerabilities and try to overcome these vulnerabilities by setting vulnerable security parameter to its good security practices. Hence checking these security parameter using command prompt is very critical and time consuming task.so we planned develop a script which is strongly recommended which verify that all security action items have been executed. Even the best system admins can make mistakes and miss steps. There should be scripts for checking security action items to manage lager Linux Environment and these scripts should be run periodically manually or as Cron job.

2. MOTIVATION

Linux system never stay secured as time goes it become less secured because operational and functional changes had done through threats or new exploits being available for packages or applications. Setting security parameter to incorrect values increases the risk to following [4] .

2.1 Workstation Security

Workstation or home PC as target for attacker is probably less happens than network and server security. Still it contains sensitive data so providing security to this also important.

2.1.1 Bad password

Providing bad password is vulnerability in workstation security. If root password is hacked then attacker will become owner of system and hence there will be data loss or data may be stolen.

2.1.2 Vulnerable client application

Telnet or FTP services over public network are also big vulnerability because password and username information can be stolen when it passes over network.

2.2 Network Security

2.2.1 Insecure Architecture

A misconfigured network setting means open way to enter into network and get unauthorized access i.e. giving chance to attacker enter into network so without any hard work attacker can gain whole access over network ,render into network and do his bad intentional work.

2.2.1 Broadcasting

Hubs and routers are used for broadcasting when packet transmit across network, packet will broadcasted in network until it receives by receiver node due to this Denial of service attack may occurs.In recent years we have experienced a wave of DDoS attacks threatening the welfare of the internet [5] .

2.2.2 Centralized Server

Use of centralized server is major threat to network security .We uses centralized server because it is easier to manage more than one system and another thing is that cost considerably less. But it is single point of failure once attacker gain access at this point then he will easily manage that network according him.

To be able to address these issues, you need to have a solid understanding of the underlying basic security requirements of your system [6] .

3. LITERATURE SURVEY

In[7] author addresses the different aspect of security problems in network operating system. Most important are weak authentication and improper configuration identified.

In [8] author addresses the network vulnerabilities. This paper focuses on log monitoring in linux. Log includes network traffic log,attackers log, and observer log. **O**ne of the key facets of maintaining a secure and hardened environment is knowing what is going on in that environment.You can achieve this through your careful and systematic use of logs. This is usually enough for you to diagnose problems or determine the ongoing operational status of your system and applications. When it comes to security,you need to go a bit deeper into the logging world to gain a fuller and clearer understanding of what is going on with your systems and applications and thus identify potential threats , attacks [9] .

In [10] main objective of Linux security discussion is Linux security requirements including account policies for Linux systems that are being audited.

In [11] this book author given deployment guide about package management and user management. A very important step in securing a Linux system is to determine the primary function or role of the Linux server. You must aware about what is on your system and what not. Remove the unnecessary things i.e. packages from your system so that you can easily update required packages and kernel patches hence your system stay updated. For maintenance and troubleshooting purposes there should be minimum packages on system. A good approach is to start with a minimum list of packages and then add packages as needed. It may be time-consuming but worth the efforts. author given idea of Enforcing Stronger Passwords

Simple password hacked easily so restrict people to use strong password. Undoubtedly, it is important to practice safe password management. In my opinion, a password should have at least one digit number, one other character, and one upper case letter. But keep in mind not to make it overly complicated.

3.1 How To Enforce Stronger Passwords

For enforcing strong password edit following: */etc/pam.d/system-auth* file.

3.2 Restricting Use Of Previous Passwords

Password cannot be reused for at least 6 months and that at least 3 characters must be different between the old and new password. Enabling Password Aging we set PASS_MIN_DAYS to 7, which specify the minimum number of days allowed between password changes.

3.3 Displaying Login Banners

It is prudent to place a legal banner on login screens on all servers for legal reasons and to potentially deter intruders among other things. Consult legal counsel for the content of the banner. If you want to print a legal banner after a user logs in using ssh, local console etc., you can use the /etc/motd file. Create the file if it doesn't exist and type in the banner that applies to your organization .For SSH you can edit the Banner parameter in the */etc/ssh/sshd* config file which will display the banner before the login prompt. For local console logins you can edit the */etc/issue* which will display the banner before the login prompt. On an audited production system it is very important to know who switched to which system or shared account. Therefore it is prudent to restrict direct account logins for all system and shared account where more than one individual knows the password All users should do a direct login using their own account and then switch to the system or shared account.

4. PROPOSED SYSTEM

The Linux security is centered on how the configuration is made. Configuration files for various system processes, application and servers play the vital role in hardening the Linux. Configuration file contains various security related attributes that need to be considered while at the time of configuration of particular application, process and server.So we focused on various configuration files that are critical from security perspective and security attributes present in such configuration files. The following Fig. 4.1 shows the detail description about how to make Linux more secure so that impact of security breach can be minimum.

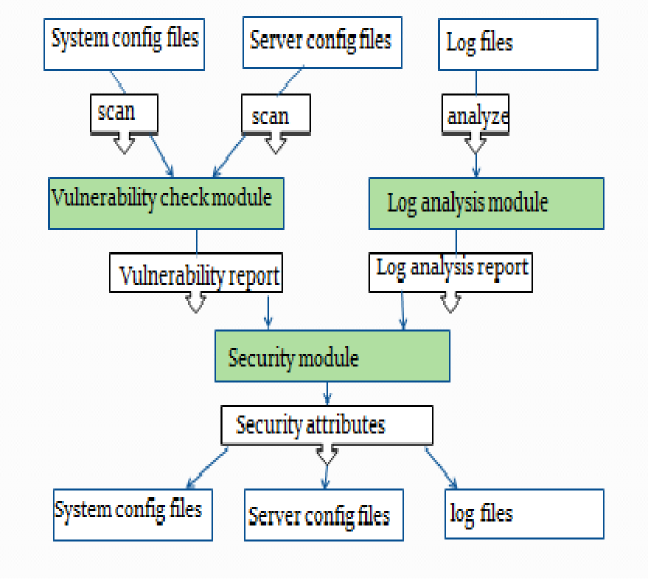

Fig 4.1: System Implementation

The Linux Hardening model consists of three modules which makes the Linux more secure from the attackers which are:

1. Vulnerability check module
2. Log Analysis Module
3. Security Module

4.1 Vulnerability Check Module

As Mentioned in the literature survey there are various configuration files such as system configuration file and server configuration files which contains attributes that are critical. This module will check such configuration files and scan for attribute which are important from security perspective. This module check current attribute value with best security value required for that attribute. If current configured value is not a best security value then it will consider it as vulnerability and generates the vulnerability report. Generated report is given to the security module.

4.2 Log Analysis Module

Linux system consists of very strong logging mechanism maintains the log for kernel, servers, users, system processes etc. These entire logs by default placed at different location. This module collects the log from these various places and generates report. This generated report is useful for finding the vulnerability. Generated report is given to the security module.

4.3 Security Module

This module collects the vulnerability report and log analysis report and applies security. By looking vulnerability report this module get the vulnerable configuration files and modify them with best security practice. Similarly by looking log analysis report this module apply the security attributes accordingly. This model is actually responsible for modifying the configuration files and making the Linux more secure.

5. MATHEMATICAL MODEL

Input

F1 → Sys Conf Files
F2 → Server Conf Files

Intermediate Results

A={a1,a2,a3}
a1: Vul Module
a2: LogA Module
a3: Sec Module

OutPut:

-Generate Vulnerability report
-Generate Log analysis report
-Generate Alert messages

6. PROPOSED ALGORITHM

6.1 Vulnerability Check Module

This Module scans the various configuration files and generates the vulnerability report.

```
Input : any configuration file
Vcheck(configuration file)
do
    file ← configuration file
    fopen (file)        #open configuration file
    do
        attr ← security attribute;
        val ← security value
    while(end of configuration file)
    If val!=security requirement    #check the attribute value
    then Vulnerability ← attr    #Mark the attribute as vulnerable attribute
    Generate and store the vulnerability report
    Generate and store the vulnerability report
while end of the file
Output : vulnerability report
```

Fig : 4.2 Vulnerability Check Module

6.2 Log Analysis Module

This module reads the various log files and generates the log analysis report.

```
Input : Log file
LogAnalysis(log file)
do
    file ← log file
    fopen (file)        #open log file
    do
        val ← malicious activity;
    while(end of log file)
    If val
    then        line ←    read the log line
    Generate and store the log report
while end of the file
Output : Log analysis Report
```

Fig: 4.3 Log Analysis Module

6.3 Security Module

A security module read the vulnerability and log analysis report and modifies or adds the security parameters in appropriate configuration file.

```
Input : Vulnerabilty report
Security (vulnerability report)
do
    file ← vulnerability report
    fopen (file)        #open vulnerability file
    do
        attr ←     vulnerability attribute #read the vulnerable attribute
        fopen(configuration file)
        if attr            #if attr in configuration file
        then            #if attr not in the configuration file
            attr = new value
        else
            attr=value
        save the configuration file
while end of vulnerability report
Output : modification of configuration file
```

Fig: 4.4 Security Module

7. DATA STRUCTURE DESIGN

7.1 Data structure For Configuration Files

Attribute Name	Value

Where

Attribute Name is name of the configuration attribute in the configuration file.

7.2 Data Structure for the Vulnerability Report

Vulnerability	Description

7.3 Data structure For Log Analysis Report(Authentication Report)

#	D	T	A	H	T	E	S	e

Where:-

#- serial no, D-date of authentication, T-time of authentication, A-name of the account, H- host name, T-terminal name, E-exe file name, S-authentication success or not, e-event no of log.

8. PERFORMANCE ANALYSIS

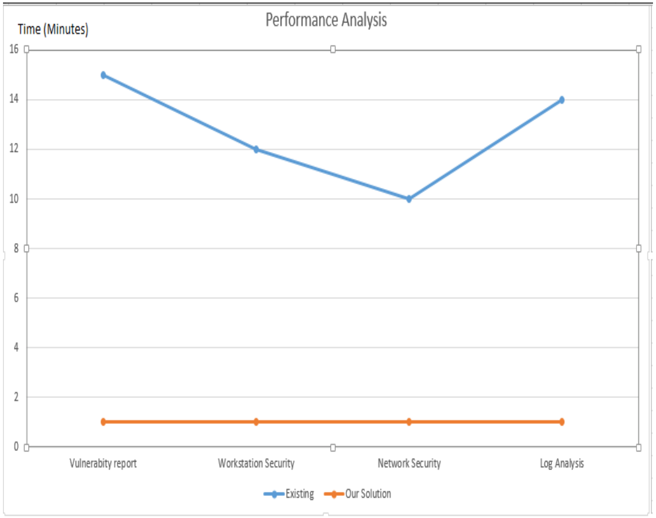

Fig8.1: Performance of existing system Vs proposed system

In above graph it shows time required for generating vulnerability report , workstation Security , network security, Log analysis report in minute. Existing system takes more time than the current solution ,in proposed solution it gives within 1 to 2 minute.

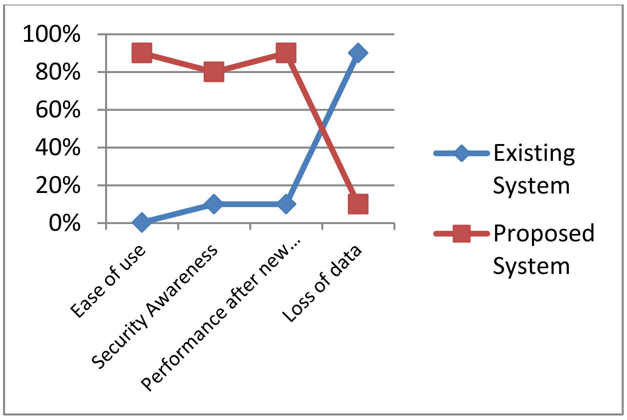

Fig8.2: Evaluation parameter comparison for existing Vs. proposed System

In above graph shows parameter considered for evaluation such as ease of use , security awareness , performance after new patch added , loss of data in percent. In proposed system loss of data is low and another parameter value are high but in existing system vice warsa.

9. CONCLUSIONS AND FUTURE SCOPE

Linux system never stay secured as time goes it become less secured because operational and functional changes had done through threats or new exploit being available for packages or applications. Setting security parameter to incorrect values increases the risk and Because of most organizations are increasingly dynamic in nature, their workers are accessing critical company IT resources locally and remotely, hence the need for secure computing environments has become more pronounced. thus This paper describes how simply, consistently, and practically secure your Linux environment. In future scope we can extend it for commands which are not covered can be harnessed and automated into a generic reusable tool that will provide the desired results.

10. REFERENCES

[1] Andrea Barisani , Thomas Bader, Hacking Linux Exposed Linux security and secerets, Edition 3,2008.

[2] Manuel Cheminod,Luca Durante,Adriano Valenzano, “Review of security issues in industrial networks”,IEEE transaction onindustrialinformatics,Vol.9,No.1,FEB2013.

[3] Ashvini T. Dheshmukh, Parikshit. N . Mahalle.Survey on linux security and vulnerabilities IJECS Publisher,v-3 issue 9 sept-2014,page no 8265-8269.

[4] Red Hat Engineering Content Services, Red Hat Enterprise Linux 6 Security Guide A Guide to Securing Red Hat Enterprise Linux, Edition 3, 2011.

[5] Udi Ben-Porat,Anat Bremler-Barr,”Vulnerability of network mechanisms to sophisticated DDoS attacks”,IEEE transaction on computers Vol.62,No.5,May 2013.

[6] Nigel Edwards, Joubert Berger, and Tse Houng Choo. A Secure Linux Platform. In Proceedings of the 5th Annual Linux Showcase and Conference, November 2001

[7] Stefan Lindskog and Erland Jonsson,”Different Aspects of Security Problems in Network Operating System”,

[8] Hannes Holm,Mathias Eksted,”Empirical Analysis Of System-Level Vulnerabilities Metrices through Actual Attacks” , IEEE transaction on dependable and secure computing,vol 9,no 6,Nov/Dec 2012.

[9] James Turnbull, “hardening Linux”, 2005.

[10] P. A. Loscocco, S. D. Smalley, P. A. Muckelbauer, R. C. Taylor, S. J. Turner, and J. F. Farrell,” The Inevitabil-ity of Failure:The Flawed Assumption of Security in Modern Computing Environments”, In 21st National Information Systems Security Conference, pages 303–314. NSA, 1998.

[11] Jaromír Hradílek Red Hat, Inc. Engineering Content Services,”Red Hat Enterprise Linux 6 Deployment Guide Deployment, Configuration and Administration of Red Hat Enterprise Linux” , Edition 3,2012.