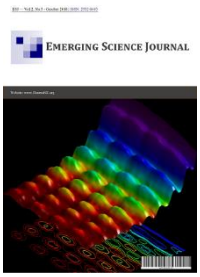
Available online at www.IJournalSE.org

Emerging Science Journal

Vol. 2, No. 5, October, 2018



Provides a New Way to Enhance Security in the Linux Operating System

Hamid Reza Ganji [a], Kiarash Aghakhani [b*]

[a] *Department of Computer Engineering, Arak Branch, Technical and Vocational University of Amirkabir, Arak, Iran*

[b] *Young Researchers and Elite Club, Arak Branch, Islamic Azad University, Arak, Iran*

Abstract

The security of the configuration of files in the Linux operating system depends on many factors that can be referenced to the system level and the applicable level. The most important thing about the security of Linux operating systems is its dynamism, for example, when you secure your Linux system, it will not stay safe forever, because applications and cyber criminals through new threats and/or new exploits that are packaged Systems or applications that cause the operating system to become unsafe, for this reason, we need a secure operating system. The main purpose of this article is to provide a new way to enhance the security of the Linux operating system. For this purpose, how can simple, continuous, and practical Linux environment be secured, solutions are presented, also based on performance analysis of the proposed method and evaluation parameters for existing systems against the proposed system, the superiority of this method is introduced.

Keywords:

Linux Operating System;
Security in the Operating System;
Attacks on the Operating System;
Computer Security;
Security Parameters.

Article History:

Received:	30	March	2018
Accepted:	01	October	2018

1- Introduction

Linux is an open source OS that makes changes free. The term "computer security" covers a very large and wide range, including computing and processing information. One of the biggest problems for people seeking security in every field is their limited range of information about security in that area. They are not sure what security should be provided and how this security should be provided. Because of this, people cannot fully understand what security is. One of the main reasons is the word security that has many meanings. [1] Security means separating assets from threats. There are three choices to separate the threat from assets. 1-Physical removal or separation of assets from threats 2-Destruction of threats 3-Moving or removing assets. In actual circumstances, the destruction of assets is not desirable, and the destruction of the threat is usually very complex or illegal. Although the separation of these two is usually possible. Computer security is usually divided into three main distinct categories, which are usually referred to controls: [2] physical, technical, and administrative controls. Administrative security is the main objective of this article. Providing administrative security is nothing but defining the human factors of security. This definition is how the user has access. For example, register a person or check an account. We need security because of the confidentiality, integrity, and availability of data. Today, vulnerabilities occur in a variety of areas, such as operating system vulnerabilities, server vulnerabilities, and non-server program vulnerabilities. Because of the Internet's reputation and the fact that it's one of the major factors behind development, many efforts have been made to increase data security. In this paper, a suitable infrastructure for the Linux system is being examined in accordance with different needs. The Linux operating system security requirement includes user account policies for the Linux operating system, which is considered as the main issue of Linux operating system security. The Linux operating system is secure, but the correct security image comes when the security parameters are correctly set to the values i.e. So that only then will the Linux operating system be safer.

* **CONTACT**: Aghakhani_k@yahoo.com

DOI: http://dx.doi.org/10.28991/esj-2018-01153

1-1- The Areas where Security of the Linux Operating System can be enhanced

Recent vulnerabilities are addressed in three areas: 1- security stations; 2- security networks; 3. security servers; [3] which will further highlight security enhancements in these three areas.

1-2- Confirmation of Practical Security Issues and Ideas

There are a number of vulnerabilities in the Linux operating system, which requires looking at and finding a way to overcome these vulnerabilities. One of the ways to overcome the vulnerability is by setting security vulnerabilities in security settings. Therefore, checking these security parameters using the command line environment is a very important and time-consuming task. We are considering expanding on a series of recommended guidelines for all security measures. Even the best system administrators can make mistakes by forgetting one step. Therefore, the guidelines for security measures in large environments for managing Linux operating systems.

2- Motivation

The Linux operating system will never be completely secure and will slow down its security over time. Because of the existence of applications and systems that make changes through threats, or exploit new packets that are available, or adjust security parameters for incorrect amounts of risk, it increases risk [4].

2-1- Work Station Security

The probability of attacking workstations or home computers is less than security networks and servers. Of course, workstations and home computers also contain sensitive information that is important for their security.

2-1-1- Inappropriate Password

The inappropriate wording of the passwords causes security vulnerabilities in the workstations. If the root password is hacked, the attackers become the owners of the system and hence the possibility of losing or stolen data.

2-1-2- User-Side Vulnerabilities Programs

Telnet or FTP service on public networks is still a major vulnerability, as password and username information can be stolen over time.

2-2- Network Security

Network security includes regulations and policies adopted by network management that are designed and implemented to prevent and monitor unauthorized access, abuse, modification, or constraint on computer networks and resources available on the network.

2-2-1- Insecure architectures

False network configuration settings mean an open way to access the network and unauthorized access, for example, by giving the attacker the chance to enter the network without any hassle, the attacker can easily access the entire network and enter the network and the cases Do your intentions deliberately.

2-2-2- Broad Playback

Hubs and routers are used for broad playback. When a packet is transmitted over a network, that is, the packet is broadly broadcast and continues until it is received by the receiver system, and this broad broadcast creates signs of the service, and these indications the possibility of an attack occurring. For example, in recent years, we have experienced a wave of DDoS attacks that eliminates peace and security on the Internet [5].

2-2-3- Centralized Servers

Using centralized servers is a big threat to network security. But we use centralized servers because it is easier to manage than one system, and the other reason is that costs are significantly reduced. But one of the biggest weaknesses in centralized servers is when the attacker finds a way to access the server, which can easily control the server and set up the network as desired [6].

3- Background Research

Lindskog and Jonsson (2002) pointed to various aspects of security issues in the network operating system, the most important of which are weak authentication and poor configuration [7].

Holm et al. (2012) examined the various network vulnerabilities and the main focus of the article is on monitoring and logging into the Linux operating system. Logging can include several things, such as logging into network traffic, entering attackers, or logging in [8]. One of the key ways to maintain the safety and security of the environment is to be aware of the surrounding streams. Which can be achieved through the precision of the use of reports. Using these methods, you can diagnose problems or become aware of ongoing system operations on the operating system [9].

The main purpose of Linux security and its security needs. These policies include the user accounts for Linux systems under review [10].

According to the Deployment Guide for package management and user management, is a very important step in securing Linux operating systems, recognizing the basic functions and role of the Linux server, which should include all files that Whether or not they are on the system are aware. Removing unnecessary files such as packages from the system that can be easily updated in the future. Also, keep the system up to date. In order to repair, maintain, and troubleshoot, there must be at least the number of packages required on the system. One of the most useful and safe ways is to start the update with a minimum number of packages, and then the required packages can be added in the future. This may be time-consuming but worth the effort [11].

The author has given an idea of how to pass strong words because simple word passwords easily hack, so they should encourage users to use strong words. Undoubtedly, the practice of managing secure passwords is important. For example, a pass phrase must have at least one number, a character, and a large letter, but keep in mind that the password is not too complicated [11].

3-1- How to Strengthen the Password

Edit the file below to force the password

/etc/pam.d/system-auth (1)

3-2- Restrict the use of Previous Passwords

The password cannot be reused for at least six months, and at least three characters must be different between the passage of the previous word and the passage of the new word. So we set up at least 7 days to enable our old password.

3-3- View Banner Entry

To be careful, placing a valid banner on the login page on the account on all servers for legal reasons and potentially preventing intruders from entering. Legal counselors have recommendations on the content of banners. If you want to print a banner after the user is logged in, use SSH, on the local console, etc., you can use the (/ etc / motd) file. Create a file and type the text that your organization accepts for the banner. For SSH, you can edit the banner parameters in (/ etc / ssh / sshd). The configuration files that display the banner are before the login sign-up. To log in to the local console, the (/ etc / issue) address can be edited by the banner displayed before the login notification. In an audit system, it's very important to know who in the user accounts have touched, which account or which account is used jointly. Therefore, it is wise to limit direct access to the account of all systems and all common user accounts. On common accounts that know more than one person, all users must use their account directly. And then tap into their shared account.

4- Recommended System

The configuration should be made in such a way that the security of the Linux operating system is focused. Configuration files play critical roles in various system processes, applications, and servers in Linux hardware. Configuration files include various properties related to the security of the Linux operating system, which should be addressed. So we focus our attention on configuring files that are very important for security and security features in such configuration files, as shown in Figure 1, with details of how to make Linux safer. So that the impact of security flaws can be minimized.

The proposed Linux operating system hardware model includes three modules that make Linux more secure.

1-Vulnerability Check Module 2-Log Analysis Module 3-Security Module

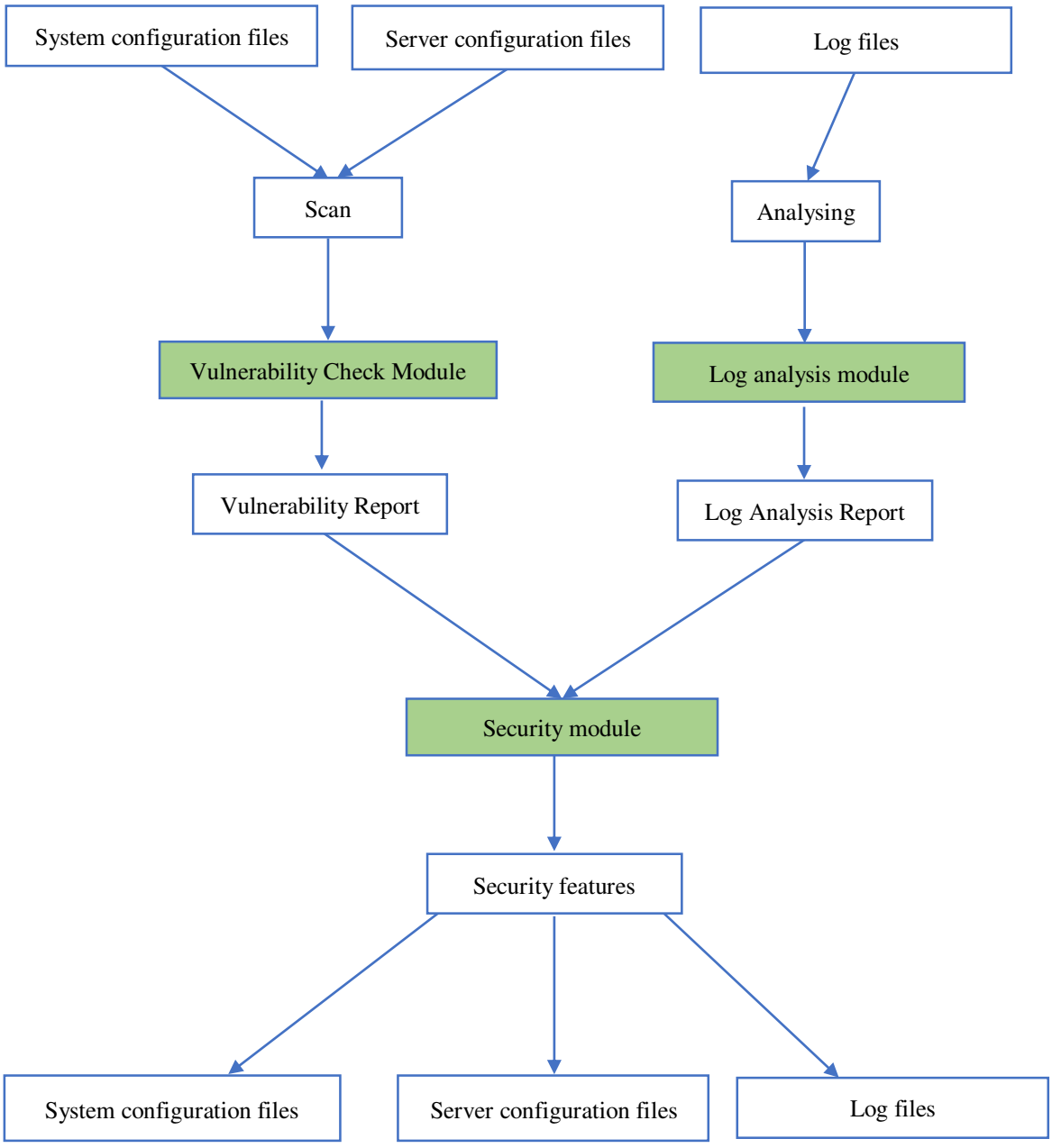


Figure 1. System implementation

4-1- Vulnerability Check Module

As mentioned above, there are several configuration files, such as system configuration files and server configuration files, which include very important features. The vulnerability check module looks at these configuration files and scans their features, which are important from a security perspective. This module examines the current values of the properties with the values of the best security model of that feature. If the current configuration value does not have the best security value, it will be vulnerable and will generate a vulnerability report that will be delivered to the security module.

4-2- Log Analysis Module

The Linux operating system includes a very powerful login mechanism that protects users from entering the kernel, servers, other user accounts, system processes, and so on. All of these entries are located in a different location by default. This module has the task of collecting information from different locations and generating reports from it. This report is very useful for finding vulnerabilities, which ultimately results in a report being delivered to the security module.

4-3- Security Module

This module has the task of collecting vulnerability reports, log analysis and security logs. By looking at the vulnerability report, this module can detect vulnerable configuration files and modify them with the best security methods. This module can apply the best security features based on the information available, so this model is responsible for modifying the configuration files and safer Linux operating system.

5- Mathematical Model

Input:
System configuration files F1
Server Configuration Files F2
Average results:
A= {a1, a2, a3}
a1: Vulnerability module
a2: Log analysis module
a3: Security module
Output:
-Report a vulnerability report
- Generate log analysis report
- Generate alert messages

6- Proposed Algorithm

The next steps in the various phases of the algorithm, which include: Vulnerability Check Module, Log Analysis Module, and Security Module are provided. Finally, the data structure for the configuration file, the vulnerability report, and the report analysis report, are the same as the process report authentication process, and the steps in the proposed method will end.

6-1- Vulnerability Check Module

This module examines various configuration files and generates a vulnerability report that is presented in Table 1 of the steps in this module.

Table 1. Vulnerability Check Module

	Input: any configuration file
	Vcheck (configuration file)
1	do
2	File configuration file
3	fopen (file) #open configuration file
4	do
5	Attr security attribute
6	Val security value
7	while(end of the configuration file)
8	If val!=security requirement #check the attribute value
9	then Vulnerability attr #Mark the attribute as a vulnerable attribute
10	Generate and store the vulnerability report
11	while the end of the file
	Output: vulnerability report

6-2- Log Analysis Module

This module reads various input files and then generates a log analysis report that is presented in Table 2 for the execution of this module.

Table 2. Log Analysis Module

	Input : Log file LogAnalysis (log file)
1	do
2	File log file
3	fopen (file) #open log file
4	do
5	Val malicious activity;
6	while(end of the log file)
7	If val
8	Then line read the log line
9	Generate and store the log report
10	while the end of the file
	Output: Log Analysis Report

6-3- Security Module

It reads and modifies security modules, vulnerability reports, and log analysis, or adds the appropriate security parameters to the configuration files that are presented in Table 3 of this module's implementation.

Table 3. Security module

	Input: Vulnerability report
	Security (vulnerability report)
1	do
2	File vulnerability report
3	fopen (file) #open vulnerability file
4	do
5	Attr vulnerability attribute #read the vulnerable attribute
6	fopen(configuration file)
7	if attr #if attr in the configuration file
8	Then #if attr not in the configuration file
9	attr = new value
10	else
11	attr=value
12	save the configuration file
13	while the end of the vulnerability report
	Output: modification of configuration file

7- Database Design

At this stage of the proposed method, the following three steps are proposed to design the data structure.

7-1- Database for the Configuration File

Feature Name	Value

The place where the Feature name is written will write the name of the configuration Feature that is included in the configuration file.

7-2- Database for Vulnerability Reporting

Vulnerability	Description

7-3- Database for Reporting Log Analysis (Authentication Report)

e	S	E	T	H	A	T	D	#

Where:

#: Serial number
D: Authentication date
T: Authentication time
A: Account name
H: Host name
T: Terminal name
E: executable file name
S: Success or failure in authentication
e: Events not logged in

8- Performance Analysis

Figure 2 shows the time required to generate a vulnerability report, workstation security, network security, log analysis and analysis report in minutes. Existing systems spend more time on the proposed solution, which can be done in one or two minutes in the proposed method.

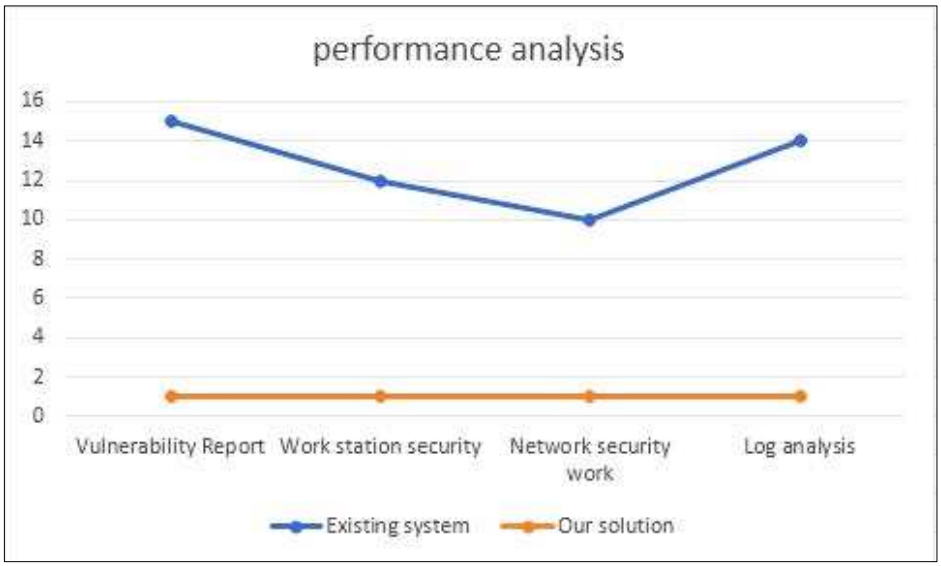


Figure 2. Existing system function against the proposed system

In Figure 3, the parameters for evaluation such as ease of use, security awareness, performance after adding a new patch and loss of information are considered. In the proposed system, the probability of losing lower information and other parameters is high, but in the existing systems vice versa.

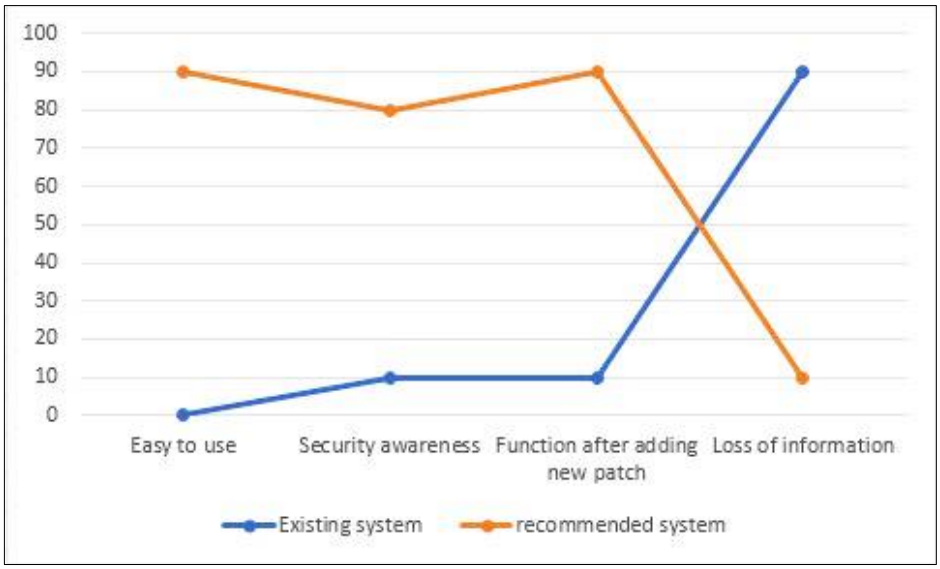


Figure 3. Comparison of evaluation parameters for existing systems versus the proposed system

9- Conclusion

The Linux operating system will never be completely secure and will slow down its security because of applications and systems that make changes through threats or exploit new programs or packages that are available. Configuring security parameters with incorrect values increases the risk, and also because many organizations naturally provide their critical resources, such as IT resources, locally or remotely to their employees, hence, the need for more secure computing environments has become more prominent. Therefore, this article describes how to easily maintain, maintain, and maintain the Linux environment. It can also be controlled and covered by increasing orders that are not covered and automatically converted to a general use tool, with the desired results presented.

10- References

[1] Barisani, Andrea, and Thomas Bader. "Hacking Linux Exposed Linux security and secerets." (2008).

[2] Cheminod, Manuel, Luca Durante, and Adriano Valenzano. "Review of Security Issues in Industrial Networks." IEEE Transactions on Industrial Informatics 9, no. 1 (February 2013): 277–293. doi:10.1109/tii.2012.2198666.

[3] Dheshmukh, Ashvini T., and Parikshit N. Mahalle. "Survey on Linux Security and Vulnerabilities." International Journal of Engineering And Computer Science 3, no. 09 (2014): 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] Ben-Porat, U., A. Bremler-Barr, and H. Levy. "Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks." IEEE Transactions on Computers 62, no. 5 (May 2013): 1031–1043. doi:10.1109/tc.2012.49.

[6] Edwards, Nigel, Joubert Berger, and Tse Huong Choo. "A secure linux platform." In Proceedings of the 5th annual Linux Showcase & Conference-Volume 5, pp. 3-3. USENIX Association, 2001.

[7] Lindskog, Stefan, and Erland Jonsson. "Different Aspects of Security Problems in Network Operating Systems." In Proceedings of the Third Annual International Systems Security Engineering Association Conference (2002 ISSEA Conference). 2002.

[8] Holm, Hannes, Mathias Ekstedt, and Dennis Andersson. "Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks." IEEE Transactions on Dependable and Secure Computing 9, no. 6 (November 2012): 825–837. doi:10.1109/tdsc.2012.66.

[9] James Turnbull, "hardening Linux", 2005.

[10] Loscocco, Peter A., Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, and John F. Farrell. "The inevitability of failure: The flawed assumption of security in modern computing environments." In Proceedings of the 21st National Information Systems Security Conference, vol. 10, pp. 303-314. 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.