International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Workstation and Network Security in Linux OS

Pramod Nimbalkar[1], Sagar kawade[2], Krishi Sharma[3] , Neeraj Khairwal[4]

[1]*Pramod Nimbalkar: Dept. of Information Technology, VIT Mumbai, Maharashtra, India*

[2]*Sagar Kawade: Dept. of Information Technology, VIT Mumbai, Maharashtra, India*

[3]*Krishi Sharma: Dept. of Information Technology, VIT Mumbai, Maharashtra, India*

[4]*Neeraj Khairwal: Professor, Dept. of Information Technology, VIT Mumbai, Maharashtra, India*

Abstract - *To keep track of personal information and run businesses, system needs powerful, networked computers. In industries network and computer security is important. Now a day's because of the popularity of internet, there is need of data security. Also most organizations are dynamic in nature hence the need for secure computing environments.*

Although not the dominant operating system on the Internet, Linux is quite prevalent, considering that the very strong for servers running web services, email services, and name services because all depend on open-source code that works with Linux. And this is where the trouble begins. So there is need to secure Linux operating system. The security of Linux depends on many configuration files both at system level and application level. Once you secure your Linux system it does not perpetually stay secure because operational and functional changes will be done through threats or new exploits are available for packages or applications. Hence Workstation and network security for the Linux os will be implemented through scripting.

Key Words: vulnerability, workstation, scripting, network, log analysis.

1.INTRODUCTION

Computer security is a general term that covers a wide area of computing and information processing. The biggest problem of people is securing anything in 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 is because security is such a loaded word that it can mean too many things. Computer security is often divided into three distinct master categories, commonly referred to as controls. Objectives of these controls are proper security implementation:

1) **Physical**

2) **Technical**

3) **Administrative**

Physical Controls:

Physical control is the implementation of security measures to prevent unauthorized access to sensitive material .Examples of physical controls are : Closed-circuit surveillance cameras, Motion or thermal alarm systems, Security guards, Picture IDs, Locked and dead-bolted steel doors.

Technical Controls:

Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Examples of technical controls are: Encryption, Smart cards, Network authentication, Access control lists (ACLs), File integrity auditing software.

Administrative Controls:

Administrative controls define the human factors of security. It determines which users have access to what resources and information by such means as: Training and awareness, Personnel registration and accounting. It is nothing but keep on watching what is going in your system that means keep updated status of your system.

General perspective about Linux is that it is quite a secure operating system. But in technical perspective, the security of Linux depends on many

configuration files both at system level and application level. System needs to be focused more on administrative controls in Linux operating system because Linux is open source operating system. Users can easily access and modify it. Linux system secure at a particular instance of time may not be secure at the very next instance because operational and functional changes might have been done through threats or installation of new packages or applications. Hence, there is a need of secure system. Since most of the network application such as DHCP, Telnet and Web servers are running on Linux it is necessary to secure these applications. All the threat, attacks are mostly are network based so the Linux network service must be so powerful to prevent these kind of attacks.

2.LITERATURE REVIEW

The main purpose of this literature survey to take review of the existing work in this area to understand the depth of security of Linux OS. To understand the history and working background of the Linux system. As per studied the existing work which makes understand the Linux system, applications and services run on Linux, architecture, features and awes of each architecture.

[1-3] mainly focuses on security vulnerabilities in general purpose Linux operating system. It is based on primarily collected data from different systems. [3-7] focuses on learning the processes and practices of securing workstations and servers against local and remote intrusion, exploitation and malicious activity.

Empirical Analysis Of System-Level Vulnerabilities Metrics through Actual Attacks

Author: Hannes Holm, Mathias Eksted

In which different levels of system vulnerabilities from modification of system configuration files, packeges are stated.

Mining Security Vulnerabilities from Linux Distribution Metadata

Author: Jeffrey Stuckman, James Purtilo

In which mined vulnerabilities from historical change log data from Linux distribution packages, tapping a yet-unexplored source of security data. Change logs provide a unified view of a application's evolution, and vulnerability patching history.

Linux security and vulnerabilities

Author: A. Deshmukh, P Mahalle.

In which it is stated that security implemented in terms of finding vulnerabilities and analysis of those results are quit secured. Analysis of log and server related threats carried out and security is applied.

3.PROPOSED SYSTEM

There are various configuration files such as system configuration file and server configuration files which contain attributes that are critical. Vulnerability check module will check such configuration files and scan for attribute which are important from security perspective. Vulnerability check 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

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. Log analysis 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

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

Consider the script called network status report. This script will execute the three ping commands for when the command name of the script is typed at the Linux prompt. It will shows following report. So script will perform ping command, test the results and gives conclusion in simplified form also generate the alert message so that administrator understand net-work status . The command do not have executed separately.

Consider ping command as an example for result interpretation. In this project, many more scripts for different security aspects will be developed. Following are the details of the scripts:

1) **Vulnerability report**: In this script four types of reports will be generated. These are work-station vulnerability report, Disk utilization report, FTP server vulnerability report, Network vulnerability report.

2) **Script for user security**, in that script we provide different options for user management such as manage users without password. We can delete user or add password to user who doesn't have password. Functionality is apply age policy and single user mode password.

3) **Script for package management**, in these script three options are there. We can list out installed packages, verify installed package, and install packages.

4) **Script for network security**, this script is very worth because it checks network related security aspects. Following are the options over there -close open ports, remote live monitoring, remote port scan, remote live monitoring, login banner, block pack-et forwarding, block reply to ICMP broadcast, enable protection against bad ICMP messages, enable SYN food protection, block source routed.

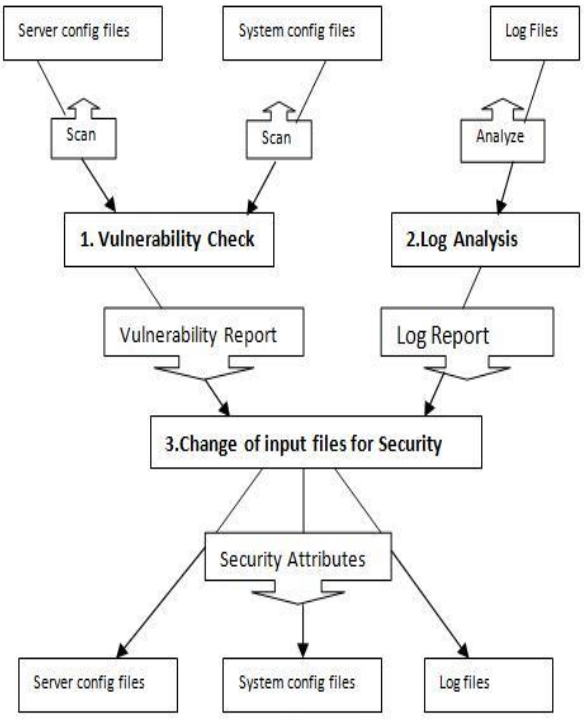

Fig. System Implementation

4.METHODOLOGY

The Linux should be secured from three perspectives:

1) **Vulnerability check module**
2) **Log Analysis Module**
3) **Security Module**

1) Vulnerability check module

There are various configuration files such as system configuration file and server configuration files which contain 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.

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 de-fault 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.

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.CONCLUSION

This research paper purposed a unique security mechanism which is very helpful for the system administrator to develop a good security strategy for securing Linux Operating System.

In limited situations, it is unacceptable to try to implement security without proper tools. There should be each security requirement must be addressed in some way even where extensive commercial tools are not available. Where extensive tools are not available simpler tools of some sort must be implemented to enable basic security.

ACKNOWLEDGMENT

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.

We are highly indebted to Prof. Neeraj Khairwal for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project. We also express our gratitude to Prof. Deepali Nayak and Prof. Kanchan Dhuri for organizing the project reviews timely and giving us proper instructions regarding timeline and submission of the project.

REFERENCES

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

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

[3] Red Hat Enterprise Linux 6 Security Enhanced Linux-en-US (Red Hat Engineering Content Services).

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

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

[6] Red Hat Enterprise Linux 6 Deployment Guide-en-US (Red Hat Engineering Content Services).

[7] 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.

[8] Hardening Linux Copyright 2005 by James Turnbull

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

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