ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

SELinux & Linux Repository: Introduction

Anjali Kundu
CSE Dept
P.D.M College of Engg.
Bahadurgarh, India

Parveen Bano
CSE Dept
P.D.M College of Engg.
Bahadurgarh, India

Abstract :- This paper emphasis on the recent developments in Linux. In preliminary study, security concern is studied that means the tools to enhance the Security of Linux, how they are used. The security tools used to SeLinux is TrustedBSD, AppArmor, Linux Intrusion Detection System (LIDS), GRSecurity, and Trusted Solaris. Then, YUM Server is studied which is a vital software utility. It is a Software repository which contains the other entire related Server in it such as FTP Server, SMTP Server etc.

Keywords :- SELinux, YUM, Repository, RPM

I. INTRODUCTION

As we all know, Linux Operating System is commonly used operating system because of its various advantages over Windows Operating System. Linux is a "Unix based" Operating system developed by Linus Torvalds. It is a free and open source Operating system and distribution which means the source code is available which is used, modified and distributed (commercially or non-commercially) by everyone under GNU Licenses. The major components of Linux are kernel, System utilities and system libraries. The KDE open source software desktop is used in Linux and UNIX. The KDE is available online and its source code is freely available on internet.

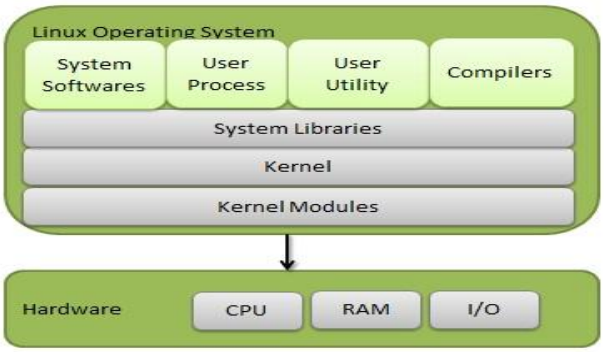

Figure 1. Components of Linux

II. RELATED WORK

Linux today, used in various fields and many new projects and works are done in this. In this, only 2 fields are discussed in detail.

A. SELinux:

The SELinux is a mandatory Access Control (MAC) security mechanism designed especially for kernel. It contains three modes that are Enforcing, Permissive, and Disabled [7]. According to Ranjit Nimbalkar, Paras Patel and Dr. B.B Meshram, some advanced Linux Security is introduced. Following describe some overview on that:-

B. Trusted BSD:

It consists of branches like Access Control Lists (ACLs), Event Auditing and OpenBSM, Mandatory Access Control and many more. It included some features such as file tagging, data transformation between kernel and Input-Output devices, Security Event Auditing etc. [1]

C. App Armor:

It is a part of SUSE distributions but now it is available under GPL. It is a Linux Security Module. It relies upon application profiles for making decision. It allows system administration to bind a security profile with each program so that it restricts the capabilities of program. AppArmor provide a Mandatory Access Control (MAC) for file-paths.[3]

D. Linux Intrusion Detection System(LIDS):

LIDS is a patch designed for Linux Kernel and an administrative tool to enhance the Kernel Security by Mandatory Access Control (MAC). It includes many measures to minimize the damage such as hide sensitive processes, security protection online etc. [3]

E. GR Security:

It is a collection of multiple patches for Linux Kernel which focuses on Security of kernel. Its major components are PaX and Role-based access control. PaX is mainly guard memory from being overwritten. [2] Role-Based Access Control support features like configuring process accounting, human readable configuration, no run-time memory allocation Secure policy enforcement and many more. [3]

F. Trusted Solaris:

Trusted Solaris Extensions, a component of Solaris 10. It includes the facilities like auditing, accounting, Mandatory Access Control labeling and Role-Based Access Control.

G. YUM Server:

YUM is expanded as Yellowdog Updater Modified developed by Seth Vidal written in Python language [4]. YUM is like App Store having software Repositories i.e.

collection of packages which may be accessed locally or in a network connection i.e. a LAN. It contains repository of another servers such as FTP Server, SMTP Server, making Domain Name Server (DNS). It provides information about the packages. This known as metadata. It contains easy and simple commands to install and use YUM. Repository is a storage area where we store all the package information.

It can perform operations as following [5]:-

a. Installing the packages
b. Deleting the packages
c. Update the existing install packages
d. Show list of available packages
e. Show list of install packages

Steps to install Yum Server [6]

a. Mount /dev/cdrom/mnt
b. Cd /mnt
c. Cd packages
d. Ls(REO COLORED Files.rpm)
e. Rpm –ivh vsftpd*//Rpm is redhat package manager. Here, all the needed packages are installed.
f. Rpm –ivh delta*
g. Rpm –ivh python_delta*
h. Rpm –ivh createrepo*
i. Mkdir /var/ftp/pub/Yum
j. Cp *-rv /var/ftp/pub/Yum
k. Cd /var/ftp/pub/Yum
l. Create repo –v current location
m. Cd /etc/yum.repos.d
n. Rm *
o. Vim b.repo

Press i for inset mode

Then type :-

[yum]
Name=yum
Baseurl=FTP://Your IP/pub/yum
Enabled=1
Gpgcheck=0

Then Press “esc” button and Type “:wq”

a. Service vsftpd restart
b. Chkconfig vsftpd On
c. Yum install dialog

By these above steps, Yum is successfully installed.

III. CONCLUSION

Linux is preferred due to its advantages like multitasking, portable, Open Source, Secured and many more. It most widely used in embedded System like tablet phones, television, network routers, video Games and many other. Androids, which are most commonly, used operating system in tablets and smart phones work on Linux Kernel. Linux operating system not only used for technical users but also for technical community, application developers, industry, and end users.

IV. REFERENCES

[1]. 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.(**Article in a journal)**

[2]. C. J. PeBenito, F. Mayer, and K. MacMillan. Reference Policy for Security Enhanced Linux. In SELinux Symposium, 2006.

[3]. http://www.ajer.org/papers/v2%283%29/B0230712.pdf

[4]. Brown, Robert G. "Yum (Yellowdog Updater, Modified) HOWTO - Introduction". Duke Physics. Retrieved 12 July 2013.

[5]. Jang, Michael H. (2006). Linux Patch Management: Keeping Linux Systems Up to Date. Bruce Perens' Open Source series. Prentice Hall Professional. pg. 199 Retrieved 2014-08-26.

[6]. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/ch-yum.html

[7]. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-Enabling_and_Disabling_SELinux.html