Different Aspects of Security: Linux

Himanshi Singh, Binny Arora, Ashish Bishnoi
BSc(HONS)CS, CCSIT, TMU
BSc(HONS)CS, CCSIT, TMU
Assistant Professor,CCSIT,TMU Delhi Road,India
himanshi.singh191295@gmail.com
biny0909@gmail.com
ashishbishnoi04@gmail.com

Abstract— **Securing data and other network resources of a computer network is most challenging task for any system administrator. To handle security issues different features are evolved in operating system to enhance the system security. System administrator constantly faces the challenge of hackers and sabotage by unsatisfied employee of company. "Security through obscurity" is a general feel emerged in decade of 90's which suggests proprietary software are more secure. Emergence of open source softwares in recent times challenges the dominance of proprietary software. Open source softwares with new features and tools are proved to be more secure.**

Linux become the front runner in open source software due to its ability to raise the security at different levels. Linux secures its system by granting different privileges to various users of the system and does not provide full administrative privileges to the user.

In this paper, I try to analyse the different security measures and their implementation in linux operating system.

***Keywords*— Operating system, System Security, "Security through obscurity"**

I. Introduction

Security is always most imperative issue in human life. Human beings always try to secure their belongings or precious things they have. From the beginning of the civilization there are certain elements who always try to harm or steal the precious belongings of other human.

With the invention of the computer almost people store their information or data related to their assets in computer system. Now a days this dependencies increases as we have computers with latest technologies to secure the data and other confidential things and files present in it. This announcement of technology not only use by the genuine users but malicious user can also take advantage of it.

In present scenario most of the data is present in the computer system either belonging to the organization or an individual, it can have an email account , account on social site ,account on shopping sites as well as an access to an internet banking. All these provide the separate functionality to ease and save time in hectic life of an individual. There exists the disadvantage of using all these services as there is always a probability that individual user account or information of the user is misused by another individual with the malicious intentions. This threat not only exists for the single individual but it is also for the Education, Business, Banking organizations.

Organizations have to deal threats to their computer systems at multiple levels. These levels are described in sections given below.
Security includes multiple angels by using which all the gaps are patched. Operating system is core of any computer system and hence it is responsible for implementing different type of securities on different applications. Later on, in this paper we will discuss the different security levels and their implementation reference to linux operating system.
Linux is an open source system released in 1991. Till date we have multiple flavours of linux - Red hat, Fedora, SE linux, Ubuntu etc. All these versions of linux operating system is more secure than that of windows.

II. History and evolution of linux

Linux is an operating system that evolved from a kernel created by Linus Torvalds when he was a student at the university of Helsinki. The evolution of Linux is present below:

1983: Richard Stallman started the GNU project with the goal of creating a free UNIX like operating system.

1986: Maurice J.Bach of AT&T Bell Labs published The design of the Unix operating system.

1987: MINIX –a unix like system intended for academic use was released by Andrew S.Tanenbaum.

1991: The 21 year old Finnish student Linus Benedict Torvalds announced his work on a free operating system. Linus 0.01 was released on the net.

1994: Version 1.0 of Linux kernel was released. Red Hat cofounder Marc Ewing announced the availability of Red Hat software Linux.

1996: Version 2.0 of the kernel was released.

1997: Bliss "First Linux virus" was discovered.

2004: Ubuntu came into life with the unusual version number 4.10.

2011: Linus Torvalds announces the release of Linux 3.0.

2013: Linux based operating system for video games consoles.

III. SECURITY ISSUES

Security deals with protecting system from deliberate attacks either internal or external, from individual attempting to steal information ,damage information in some manner. Some common types of violation include:

Breach of confidentiality: Theft of private or confidential information such as credit card numbers trade secrets etc.

Breach of Integrity: Unauthorized modification of data which may serious indirect consequences.

Breach of availability: Unauthorized destruction of data often just for the fun causing havoc and for bragging rites.

Theft of services: Unauthorized use of CPU resources such as theft of CPU cycles, Installation of daemons running an unauthorized file server.

There are 4 levels at which a system must be protected:

A. Physical

The best way of stealing data is to pocket the back up types.

B. Phishing

It involves sending an innocent looking e-mail or website design to fool people. Ex- e-mail from e-bay, credit card companies.

C. Dumpster Diving

It involves searching the trash or other location for password that are written down.

D. Password Cracking

It involves divining users passwords either by watching them type their passwords knowing something about them like their pets name or simply trying all words in common dictionaries.

IV. LINUX SECURITY MECHANISM

Linux emerged as one of the most secure operating system in last decade .Two basics reasons which make linux operating system differ from any other operating system are-

- Linux Kernel does not contain exe files. There executable ports are present in binary files.
- Linux distributes its security mechanism on multiple levels starting from 0(described as least secure) ending as 7 (described as most secure) level in operating system.

Security Level 0

Default mode, normal operation. Everything is allowed as in the default unsecured Linux system.

Security Level 1

Permits almost all normal operations which may lead to dangerous actions. This means direct write access to raw block devices of mounted filesystems and access to devices representing raw memory (/dev/*mem, /proc/kcore) . Security level cannot be lowered. This is intended as the normal mode of operation for the usual desktop linux systems.

Security Level 2

It completely locks user-space into itself, preventing any modification ir sidestepping into kernel. Direct access to hardware is prohibited even for applications with CAP_SYS_RAWIO (usually all tasks running as root) and no modules can be inserted/removed from the kernel. Writing permission to any raw block devices is denied. This is required for normal functioning of linux servers.

Security Level 3

This level ensures that the configuration cannot be altered unauthorizedly. Makes it impossible to change immutable and append file attributes. Devices cannot be (un)mounted, swap devices cannot be reconfigured and mknod() call is disallowed. You are banned to set the time backwards or close to overflow. Hostname and domain name cannot be changed, nor can be the printk logging level.

Security Level 4

This employs even stricter anti-reconfiguration policy, mainly network-wise --- by now it should be already impossible to break the configuration in any way. System prevents you to touch the network interfaces configuration and routing table and iptables rules.

Security Level 5

Attempt to protect running processes from any possible unauthorized distractions. Prohibits even tasks with CAP_KILL (root tasks) to kill processes of other users .

Security Level 6

By now all the special privileges of the root account are disabled. No resource exceptions are applied to root, it is treated as normal user and cannot override the limits. And it cannot adjust time in any way, it cannot reconfigure terminals, chown() is disallowed. We cannot even reboot the machine now.

Security Level 7

This is left for other special security modules as the placeholder for any further possible restrictions, the stock kernel doesn't implement any of the limitations recommended for this level: non-root users can't see other processes and can't even list the system configuration (almost anything in /proc and /sys is non-accessible, sysctl() is unusable), only .text segment should be executable. Some possible special accounting could be employed here. Daemons should ignore any signals or administrative commands and only respond to ordinal user requests.

Besides these levels, different security mechanism are implemented in linux using following points-

1. Authorization and Authentication: In it the user name and password will be checked .Only the authorized user can access to the account, unauthorized user will not be allowed to use the account.
   Linux enforces its user to create the strong password using the command pam_cracklib. The minimum length of the password must be 10. It should contain a letter/digit/special character. User password is stored by linux operating system in file /etc/shadow. The password of all the users present in the encrypted form which ensures that no linux user including root user can able to view the password of the specific user.
2. File access permission: Linux operating system allows its user to assign file permission on the files owned by them. In linux system we can assign the permission in two modes text

modes and numerical mode using command chmod.
Ex- $ chmod 700

3. File Mask: It implies that which permissions we have to hide or mask.It simply improving the security for the newly created file. The command use to mask the file permission is: umask
Ex- $ umask

4. Using Sticky bits on files and directories: Sticky bitb attach to the file ensures that whenever it is called it is loaded fastly into the memory laocation in comparison to other files. Sticky bit when used with directories controls the detection of shared files or directories.

5. Using sudo for privileged access: Sudo prevents users from accidentally running commands as *root* that do not need root access, because a full root terminal is not created. The root user password need not be given out to each user who requires root access . It keeps a log of which normal privilege user has run each privileged command.

6. Network and Firewall
Firewall:It is highly recommended to set up some form of firewall to protect the services running on the system.Many resources do not state explicitly which services are worth protecting, so enabling a firewall is a good precaution.
SSh: Secure Socket shell is a network protocol which provides administrator with a secure way to access to remote computers.
Proxies: Proxies are commonly used as an extra layer between applications and the network, sanitizing data from untrusted sources. The attack surface of a small proxy running with lower privileges is significantly smaller than a complex application running with the end user privileges.

7. Locking down BIOS: Adding a password to the BIOS prevents someone from booting into removable media, which is basically the same as having root access to your computer.

Bootloaders

It is highly important to protect your bootloader. There is a magic kernel parameter called init=/bin/sh. This makes any user/login restrictions totally useless.

GRUB

It supports bootloader passwords as well.It also has support for encrypt boot partitions,which leaves some part of the bootloader code unencrypted.

V. Conclusions

In this paper I concluded that the security features of linux is more powerful than the others. Linux become the front runner in open source software due to its ability to raise the security at different levels. Linux secure its system by providing different privileges to various users of the system. It does not provide the full administrative privileges to its user.

References

[1] The Linux KernelArchivessite ,”The primary site for the Linux Kernel source”http://kernel.org
[2] The Linux Distribution information site,http://distrowatch.com