Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 09, September-2019

A Survey of Security Issues in Linux Open Source Network

Prof. Vinit A. Sinha
(Assistant Professor)
P.G. Department of Computer Applications (MCA)
Prof. Ram Meghe Institute of Technology & Research, Badnera
Amravati. (M.S.) India

Abstract:- Linux is an open source based operating system. Linux Operating system is similar to other operating system such as Windows and OS X. There are number of different issues that need to be considered and potentially dealt with open source environment like Linux. It has different tools and processes available to help eliminate the security exposures they represent.

Security towards networking in general which includes number of different aspects like password protection, data encryption, virus protection, Firewall, VPN's, software bugs, and data backup. The linux operating system has password authentication, file system access control and security logging details. The linux system considered to be free from attack of viruses and malware. Secondly a network topology designed in linux which contains different servers and firewalls. Inference of network configuration of firewalls and applying security measures in server configuration are explained and compared.

Keywords: - Firewall, VPN, Virus, OSS, Linux, netfilter

1. INTRODUCTION:

Security should be one of the foremost thoughts at all stages of setting up Linux system. To implement a good security policy on a machine requires a good knowledge of the fundamentals of Linux as well as some of the applications and protocols that are used. As the network traffic increases and more important transactions are taking place users' risk grows as bad guys try to damage, intercept, steal or alter user data. If there is something worth stealing then someone will try and steal it. Linux-based systems have no special exclusion from this universal rule. A primary reason that Linux systems are so popular is because they are robust and have many sophisticated security measures. It is impractical to discuss security in broad strokes since the idea represents a vast range of concepts, tools, and procedures, none of which apply universally. Choosing among them requires a precise idea of what user's goals are.

2. SECURITY ISSUES ARE MEASURED AS FOLLOWS -

I.Password protection

Linux distribution provides a few standard encryption/decryption tools that can prove to be handy at times. Here in this article we have covered 7 such tools with proper standard examples, which will help user to encrypt, decrypt and password protect user's files

A. GnuPG

GnuPG stands for GNU Privacy Guard and is often called as GPG which is a collection of cryptographic software. Written by GNU Project in C programming Language. Latest stable release is 2.0.27.

```
$ sudo apt-get install gnupg
# yum install gnupg
```

B. bcrypt

bcrypt is a key derivation function which is based upon Blowfish cipher. Blowfish cipher is not recommended since the time it was figured that the cipher algorithm can be attacked.

```
$ sudo apt-get install bcrypt
# yum install bcrypt
```

C. ccrypt

Designed as a replacement of UNIX crypt, ccrypt is an utility for files and streams encryption and decryption. It uses Rijndael cypher.

```
$ sudo apt-get install ccrypt
# yum install ccrypt
```

D. Zip

It is one of the most famous archive format and it is so much famous that we generally call archive files as zip files in day-to-day communication. It uses pkzip stream cipher algorithm.

```
$ sudo apt-get install zip
# yum install zip
```

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 09, September-2019

E. Openssl

Openssl is a command line cryptographic toolkit which can be used to encrypt message as well as files.

```
$ sudo apt-get install openssl
# yum install openssl
```

F. 7-zip

The very famous open source 7-zip archiver written in C++ and able to compress and uncompress most of the known archive file format.

```
$ sudo apt-get install p7zip-full
# yum install p7zip-full
```

G. Nautilus Encryption Utility

It is use for encrypting files in GUI mode

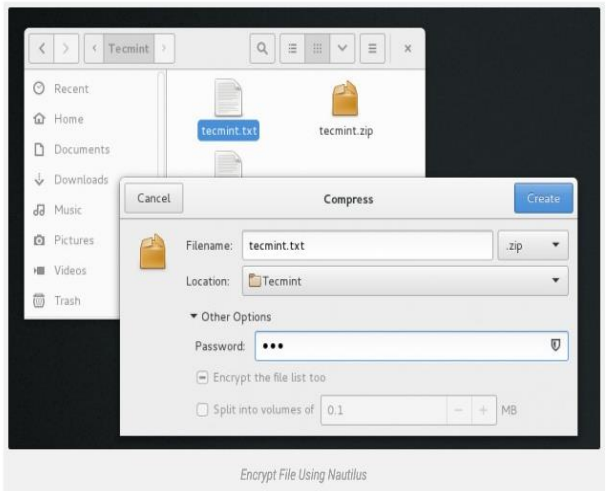

Fig 1. Nautilus Encryption Utility

II.DATA ENCRYPTION

Data encryption is one very solid security measure/precaution that everyone who owns data with significant personal or objective value should perform.

What data encryption does is securing user data when they fall into the wrong hands. While there are decryption methodologies and techniques that can be used to decrypt any encrypted data, some of it may not be retrieved, or the time and effort that it will take may lead the decryptor to the decision that user data isn't worth it.

A. Encrypt with compression

The easiest solution is to compress them using the 7z archive file format, that is open source, cross-platform, and supports 256-bit encryption using the AES algorithm.

B. Encrypt with partitioning

Open the utility called "Disks" or "GNOME Disks" and choose user's pen drive from the list on the left. Then unmount any mounted partitions of the disk by clicking on the "Stop" button located just under the partitions view.

C. Encrypt with Seahorse

GNU PG tool to encrypt anything in system disk. What all need to install first are the following packages: gpg, seahorse, seahorse-nautilus, seahorse-daemon, and seahorse-contracts which is needed if client using ElementaryOS.

III.VIRUS PROTECTION

First and foremost, no operating system is 100 percent immune to attack. Whether a machine is online or offline, it can fall victim to malicious code. Although Linux is less prone to such attacks than, say, Windows, there is no absolute when it comes to security.

Let's take a look at a few tools, offered for the Linux platform, that do a good job of protecting users from viruses, malware, and rootkits.

A. ClamAV

Without a doubt, ClamAV is the most popular option for keeping viruses off of user's Linux machines and out of user shared directories. There are a few reasons why ClamAV is so popular among the Linux crowd. First, it's open source, which in and of itself is a big win. Second, it's very effective in finding trojans, viruses, malware, and other threats.

B. Sophos

Sophos offers a free Linux scanner that does an outstanding job. This particular solution does on-access and on-demand scans for viruses, trojans, and malware. To prevent user's Linux machine from becoming a distribution point for malicious software, Sophos Antivirus for Linux detects, blocks, and removes Windows, Mac, and Android malware.

C. chkrootkit and rkhunter

No tool is more important to the security of your Linux server than either chkrootkit or rkhunter. Once installed, the usage is very simple: Issue either *sudo chkrootkit* or *sudo rkhunter -c*. Both commands will dive into the system and check for any known rootkits. During the *rkhunter* scan, user will have to press Enter on user keyboard (when prompted), as it runs through the different stages of the check. When the scan completes, both tools will report back their findings

IV.FIREWALL & VPN

A *firewall* is a piece of computer equipment with hardware, software, or both that parses the in- coming or outgoing network packets (coming to or leaving from a local network) and only lets through those matching certain predefined conditions. The Linux kernel embeds the *netfilter* firewall. There is no turn-key solution for configuring any firewall since network and user requirements differ.

Netfilter uses four distinct tables, which store rules regulating three kinds of operations on packets:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 09, September-2019

A. filter concerns filtering rules (accepting, refusing, or ignoring a packet);

B. nat (Network Address Translation) concerns translation of source or destination addresses and ports of packets;

C. mangle concerns other changes to the IP packets (including the ToS—*Type of Service*—field and options);

D. raw allows other manual modifications on packets before they reach the connection tracking system.

VPN – Virtual Private Network: -

A Virtual Private Network (sometimes called an extranet) is an encrypted connection from one point to another over any network, acting as if it is a private network. Using the appropriate security measures, user can conduct business (send and receive confidential files, etc.) across the public Internet as securely as if it were user own intranet behind a secure firewall. For best results (both for security reasons and for performance), there should be a dedicated VPN server at each end of the line. The choices are either to install VPN software on a standard Linux system or to buy a customized pre-configured hardware solution. Either method has advantages and disadvantages.

V.SOFTWARE BUGS

A *bug*, also referred to as a *software bug*, is an error or flaw in a computer program that may prevent it from working correctly or produce an incorrect or unintended result. Bugs arise from mistakes made by humans in designing programs and writing their *source code*. Source code, also referred to as *code*, is the version of software (usually an application program or an operating system) as it is originally *written* (i.e., typed into a computer) by programmers using any of numerous programming languages, some of the most popular of which are C, C++, Java, Perl, PHP, Python and Tcl/Tk. The only real way to avert these attacks is simply to stay informed. As soon as these sorts of problems are detected, they are reported in the media or disseminated from user to user via newsgroups and Linux Web sites. Being aware of such problems as soon as they are discovered enables user to minimize the potential for damage. In many cases, there is a temporary workaround that can be used (changing a configuration setting, for example, or disabling a feature) until a software patch is available to permanently correct the problem.

VI.DATA BACKUP

Linux data backup products are adding new capabilities and becoming even more mainstream. Today most major storage management vendors such as Hewlett-Packard (HP) Co. and Symantec Corp. have Linux versions of their storage management tools. In some Linux data backup software, vendors are offering the ability to back up to the cloud, handle virtualized systems and deduplicate data. Clearly there are more choices, and more sophisticated capabilities for users looking to back up their Linux systems. Linux/UNIX provides good set of tools for backup.

- Backing to tape using tar to tape, tar over ssh, cpio, and dump command. tar and friends are good for small backups. For large scale backup or backup that demands large CPU and I/O, use other solution (see below).
- Backing to another server using ftp, ftp to NAS, access NAS server using NFS protocol, access NAS from samba/windows, rsync UNIX/Linux server or windows servers
- Backing to recordable media such as CDR or DVD

3. CONCLUSION: -

In this topic, various security issues of linux open source network are discussed with several security tools. The security is not only restricted to choosing operating system or dedicated server, but it is also related to both physical and application security configured in the network. It is too necessary to mentioned here that right security tool should be configured to get more secured environment and Linux provides us that kind of freedom to build client server platform with help of customizable firewall, VPN, and effective password protection techniques. Network security system is wide area of research in which various tools and techniques for security implementation are updated frequently based on new attacks discovered.

4. FUTURE WORK: -

Extending the work in future by restricting the intruders to gain access to computers by specifying not only technologies to use, but how to design hardware and software product to use them, and which involve the computer hardware and firmware (BIOS) designers, vendors and developers.

5. REFERENCES: -

1) Encrypt/Decrypt and Password Protect Files in Linux https://www.tecmint.com/linux-password-protect-files-with-encryption/
2) Viruses and Malware on Linux https://www.linux.com/tutorials/security-tools-check-viruses-and malware-linux/
3) Data encryption on Linux - https://www.howtoforge.com/tutorial/how-to-easily-encrypt-your-data-on-linux/
4) IBM Corporation 2000 - Addressing Security Issues in Linux – A Linux white paper
5) Linux data backup and recovery- https://searchdatabackup.techtarget.com/tip/Linux-data-backup-and-recovery-strategies
6) Perform backups for the Linux operating system- https://www.cyberciti.biz/tips/perform-backups-for-the-linux-operating-system.html
7) Raphael Hertzog, Jim O'Gorman and Mati Aharonil – Kali Linux Revealed –First edition –page no. 150
8) Mukesh Kumar Mishra, Dinesh Goyal – Security Analysis in Open Source Network – IJCSNS, VOL. 14 No.8, August 2014