



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: IV Month of publication: April 2021

DOI: <https://doi.org/10.22214/ijraset.2021.33618>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Security Measures for Everyday Users in Linux

Shashank Yeri¹, Jashraj Gandhi², Atharva Khadgi³

^{1, 2, 3}MPSTME, Shirpur

Abstract: *Linux is used in a wide range of contexts, from personal computers to entities that store personal data on servers. This operating system is often recognized as more reliable than Windows or Mac OS X, but this does not eliminate the possibility of security risks when using it. Hackers may use a network to breach simple passwords, vulnerabilities can be exploited if firewalls do not close enough ports, and malware can be downloaded and run on a Linux system. If correct permissions are not set on the files or folders containing confidential information, it can be accessed through physical or network access. The majority of these threats can be minimized by keeping a device up to date, implementing a secure firewall, using antivirus software, creating complex passwords, and enforcing strict file permissions*

Keywords: *Cyber security, Kali Linux, Linux, Firewalls, Antivirus, Virus, Malware, Repositories.*

I. INTRODUCTION

Linux usage has expanded in many various places since its release. Likewise, windows have been replaced by Linux due to its cost-effectiveness. Due to this reason Linux usage is very popular. Nowadays many businesses use Linux as their operating system since free distributions of Linux very attractive. But even Linux OS has its limitation like some hardware drivers are not available for **Linux**, limited security, and so on. To stop hackers from gaining access to hardware, protecting against possible theft of well-kept information, it is essential to apply security features and to make sure to secure the information within the machine. Security is one of the major significances in the age of the computer.

The security vulnerability that can be breached and to counter it various studies are in use like data mining, artificial immune system, machine learning, etc. Data mining is the practice of analysing large databases in order to generate new information from big data sources, e.g. Data mining is used to explore increasingly large databases and to improve market segmentation. Machine learning is a method of data analysis that automates analytical model building and it is also a branch of artificial intelligence e.g. predicting data about a stock market. similarly, an artificial immune system is a branch of AI in computer science, it can learn new information, recall previously learned information, and perform pattern recognition in a highly decentralized fashion.

Due to Linux free distribution many people use it on their devices, as it is user friendly and easy to use while acquiring software .it also requires less space so it can be used in primal hardware. Since Linux has major security issues and many wireless internet networks usually have very poor security so its responsibility comes to the user to protect the devices they are using.

Given that security of Linux is poor, so it is a must that users should learn about security patches of Linux and practice it for better security of their respective data. Also, security features should be added to a machine if more than one user is operating the machine to prevent physical entry to the machine from accessing the files that are restricted to respective user-groups. There are several methods to prevent hackers like setting firewall restrictions, rectifying, changing, and updating file permissions and so on. Even though the user has set the password it is quite possible to crack the password or guess it if the user or root password is not strong or complex enough.

There can be many viruses that can affect a machine. Browsing the Internet without safe measures can risk an infection from the viruses or can be transferred from any portable device. Viruses can cause a machine to be unstable since it can be included in programs made for Linux as well as windows. Linux can host Windows OS through a program which supports virtualization which results in the creation of directories to make a system appear as a software developed for Windows. Doing this will reduce inconvenience of executing a few Windows programs on Linux, which also reduces the need of dual booting and hardware requirements. It can also affect a computer or a device by introducing malware. There are many ways to prevent affected files by scanning them with antivirus even before they are installed.

Linux is used by many companies or businesses around the world as Linux is lightweight which allows the companies on private businesses to purchase storage on cloud servers and to get their hands on more data quickly. Several forms of data can be saved or stored like employee data, finance data, client data, and many other types of data. If Linux operating system is used for businesses and there is a breach in the data, there can be legal or financial consequences, so it is exceptionally important to secure their data.

Linux systems and subsystems can be protected by various methods that prevent security breach will be discussed in this paper. The method like consists of scanning for viruses, using the firewall to gain access to restricted files from a certain machine also about security issues which are accompanied with windows programs through the Linux virtualization. Practicing all this method, which will result in proper security for Linux machine that is used for businesses or companies or personal use.

While running a Linux system comes with several security challenges, numerous solutions for these kinds of issues are available. Furthermore, the functions and methods are simple to enforce and can save resources by preventing the infection of a device. Besides that, resources will be saved when confidential files would not be revealed to those who do not have permission to access those data or folders. Installing firewalls, changing file permissions, and checking for program bugs will help protect Linux systems from potential abuses, maintaining confidential data security and personal data.

II. BACKGROUND

The open-source kernel, Linux, runs diverse sets of operating systems that can be modified by any user. The Linux family of operating systems comprises of many distributions called distros which are powered by the Linux kernel. Ubuntu and Debian are the most common distros. Debian is a common go to choose for developers as well as programmers because it has open-source software repositories. A very few of them like, Parrot Security OS and Kali Linux are also used for network security, penetration testing, just to name a few. The distros Zorin OS and Elementary OS, that are designed to be user friendly and visually attractive for users transitioning from Macintosh or Windows ecosystem. Distros like Ubuntu are designed for a commercial take on the open-source market. Linux is used by a vast number of people due to its wide range of applications.

Popular Linux kernel powers the widely used Android Operating System. Most smartphones on the globe run on this OS, which is operated and owned by Google. This means that Linux isn't only used on desktop computers; it's even used on handheld devices. The vast number of users who use GNU/Linux and its distros daily demonstrates the importance of keeping their devices stable.

Since most Linux distributions are free, many people turn to them. As a result, most novice users of the Linux OS could quickly discover that they do not have permissions to any of the same applications and software that users of Windows or Mac OS have. As a result, more people are turning to virtual computers that run Windows OS or operating Windows-based applications directly on host Linux system.

Furthermore, Linux systems can also be infected by any Linux applications. This illegitimate software will masquerade as a legitimate software, it will have some suspicious activity going on in the programming and code which compromises the system's security and potentially its efficiency. As a result, people need to install an antivirus and have knowledge to protect themselves from installing malicious malware.

However, a penetration testing distribution like Kali Linux works with a different archive, which includes tools like Metasploit for performing vulnerability checks and executing exploits on compromised systems. Since Kali is based on Debian, User groups can access both the Debian and Kali Linux repositories. Many distros are based on Debian or Ubuntu, which helps to some extent in cases like these.

In general, this is a better way to update applications and helps to avoid viruses. However, some tech isn't included in all of the libraries. Google Chrome, for example, isn't in the repositories nor can be downloaded through the internet. This program is secure, but other software might not be, so consumers should be aware of what is and is not safe to use.

Users create accounts on a local Linux computer so that they can easily access the system. This contrasts with the approach used by Windows, which calls for an account of Microsoft by default. Configuring computer for the first time, consider this. When anyone logs in using an account for guests or a new user account created for a specific purpose, they will be able to open the files requiring root access, i.e if they are aware of the root password. Linux ensures users can set permissions on any files and folders desired, also root password can be set which is distinct from a password created by a user. Password crackers are used to measure reliability of a password and the possibility of it being cracked. Often, based on what programs are running, another machine on the same network might have access to another computer. Certain ports can be used by attackers to obtain another computer's files. The firewalls and the tables kit will, however, assist users in closing specific ports, stopping attackers from accessing bugs, and placing sensitive data in danger.

Linux distributions have strong operating systems for future and existing users, but they are vulnerable. Users can be vulnerable to threats due to the applications they use, also to the permissions and limitations imposed on the filesystem and resources located in their computers. Strong Linux stability, on the other hand, will avoid these flaws from being exploited, creating a better user experience.

III. METHODS OF SECURING A LINUX SYSTEM

Several threats make Linux systems vulnerable to hackers, but numerous solutions can help deter these individuals from stealing confidential data. These techniques include using libraries to secure the device, use antivirus software to verify whether a downloaded file or a folder is showing any suspicious signs or activity, using compatibility layers to operate Windows programs on Linux with care, creating policies build a firewall, protection for passwords, and various permissions to access the system with multiple users.

A. File access Permissions

A diverse set of permissions should exist on a system to deny access to users for the files that they do not need.

Commands like `chmod` can be used to accomplish this. Additionally, the `chgrp` command can be used to create groups of users with same permissions in a single attempt.

Permissions to be set for users that can execute, write, and read files will prevent users from manipulating or executing files in ways that they should not.

B. Use of antivirus: ClamAV

When someone is forced to update applications from a source other than a repository, he or she should know how to search for viruses. On Windows, one of the most popular ways to do this is to use an antivirus program. This has become so popular that Microsoft now provides Windows Defender in any commercial edition of Windows 10. If you choose to search a file or a folder for a virus, you can do that by right-clicking on it and selecting the check for viruses from the context menu. In addition, entering Windows Defender gives you the option to scan the entire machine against viruses or a single scan at start up. Antivirus programs for Windows, both free and charged, will perform similar functions. Antivirus software is not preinstalled on Linux, but it is used in nearly every Linux distribution

ClamAV is a package that searches filesystem for malicious computer viruses. It can be included in Linux package library or downloaded from the legitimate website. When ClamAV is enabled, the user has access to a range of flexible features setting up the antivirus software. Users can set schedules for when the antivirus runs, individual files can be included or removed from the search, and various kinds of scans can be performed on the device, much like Windows Defender. Specific files and folders may also be checked without a scheduled scan by naming the filesystem or the location. Furthermore, daemons may be built to run the device check as well as update the archive of identified viruses in the background.

There is a graphical version of the software for the users in addition to the command line script, this is for the users who are not used to the terminal or are completely new to the Linux ecosystem. Users will also choose individual files to search at any time using this program. However, unlike the default antivirus in Windows (Defender), the context menu in Linux does not change once the antivirus is installed, and individual files can only be searched by running the search from inside the application. This software aids in the prevention of malware installation on Linux systems by scanning the file against a continuously maintained database and returning a notification after the scan indicating if the scanned files contain any malicious computer viruses. If they do, the user will disable the software, which would prevent it from causing harm to the machine.

In conclusion, antivirus software that has been suggested in recent research works is an excellent candidate for defending a Linux-based device from computer viruses.

C. Updating Software

It is necessary to update software and packages on a regular basis to keep them safe. This ensures most recent security updates, preventing vulnerabilities to be exploited from being used. In 2017, Equifax was hacked, exposing and stealing the public information such as SSN, personal addresses, and other personal details of approximately 143 million people.

A vulnerability in an open-source web development framework called Apache Struts, which allowed attackers to gain access. According to the CEO of GitLinks, this framework is widely used by Fortune 100 companies. Information about businesses and consumers could be leaked in public because of this vulnerability. Initially the exploit was found, and it was patched afterwards.

This not only demonstrates how many people do not, but it also demonstrates how many people do. It is also important to install the update at the earliest. shows the potential effects of failing to update as soon as a new version is available. The patch has been published. The system packages and the installed programmes should be up to date for the safest experience. This can be done by going to the software's official website. Updated versions can be downloaded and installed, or you can use the Terminal to update your distribution. something that was updated in the Linux package library, such as a new browser or a kernel update. In conclusion, incidents such as data loss can be avoided by installing updates regularly.

```
[root@ww1 ~]#
[root@ww1 ~]# yum update
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
AppStream                                0.0 B/s | 0 B   00:10
BaseOS                                   0.0 B/s | 0 B   00:10
Failed to synchronize cache for repo 'AppStream', ignoring this repo.
Failed to synchronize cache for repo 'BaseOS', ignoring this repo.
Dependencies resolved.
Nothing to do.
Complete!
[root@ww1 ~]#
[root@ww1 ~]#
```

As shown in the figure, we have used ‘yum’ repository to update the software and their dependencies. Here the system is up to date.

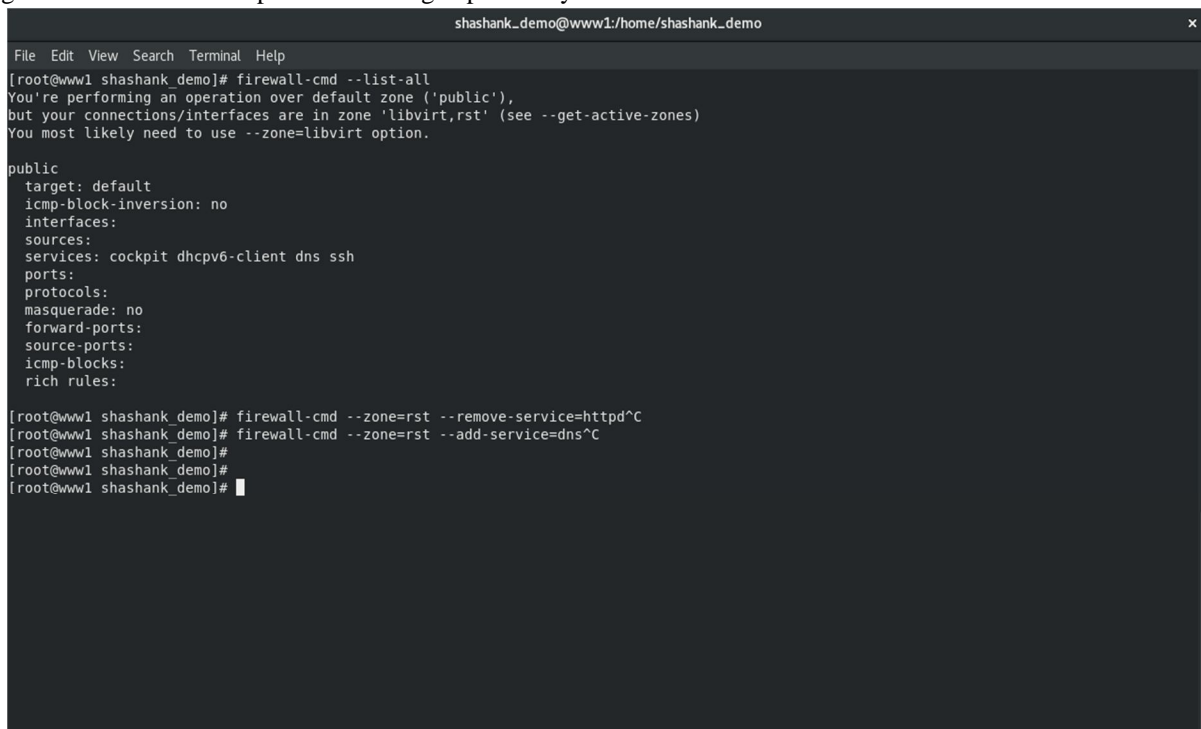
D. Firewalls (E)

Firewalls can be set up to deter attackers on the same network mask. A firewall can introduce a series of rules that protects your computer from outside threats. The firewall lists ports that are open to external access and the ports that are only open to local net mask. The machine can transmit data to other computers. SSH, for example, is a secure network protocol that allows communication between computers on the same network. On the other hand, the same people on the network are unknown, or the network is a public network that is in use, certain connections should not be permitted in a public place.

Furthermore, Distributed Denial of Service (DDoS) attacks can be launched against a system with multiple open ports, rendering the system unusable until it is restarted. Series of rules and restrictions are set to avoid these vulnerabilities, iptables packages can be updated to avoid attacks like these, which is available in most Linux repositories. The design for home network’s firewall is less expensive.

The SSH session restrictions must be strict.

For public networks, restrictions may be implemented that only allow HTTP and HTTPS service to be active and running while preventing SSH and FTP service ports from being exploited by users on the same network mask.



```
shashank_demo@www1:/home/shashank_demo
File Edit View Search Terminal Help
[root@ww1 shashank demo]# firewall-cmd --list-all
You're performing an operation over default zone ('public'),
but your connections/interfaces are in zone 'libvirt,rst' (see --get-active-zones)
You most likely need to use --zone=libvirt option.

public
target: default
icmp-block-inversion: no
interfaces:
sources:
services: cockpit dhcpv6-client dns ssh
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:

[root@ww1 shashank demo]# firewall-cmd --zone=rst --remove-service=httpd^C
[root@ww1 shashank demo]# firewall-cmd --zone=rst --add-service=dns^C
[root@ww1 shashank demo]#
[root@ww1 shashank demo]#
[root@ww1 shashank demo]#
```

Here we use ‘firewall-cmd’ command as shown in the figure to check for the services currently permitted by the firewall. As shown in the figure, DNS, SSH, and cockpit services are active, also no rich rules are applied. To add or remove a service, commands are shown in the figure.

E. Management of Passwords

Users are normally asked to create a user account when a Linux Distro is set up on a system directory containing all of that user's files on the filesystem.

These files must be kept isolated from the root user directory to avoid unexpected or of the user's essential system files.

Furthermore, if multiple users use the same system, separate accounts must be created for each individual who uses the machine.

Individual user files will be kept separate from one another, and the files will not be accessible to anyone who does not know the account password.

The root and the user password must both be unique.

This makes it impossible for someone to gain access to a user or the root account by knowing a single password.

Key Phrase

Password crackers like hashcat can be used to brute-force a password for another person's account, as well as to check the strength and security of a new password.

For example, a programme called Crack can be setup on a machine and input a password input file, and the pre-installed Reporter programme will generate a report.

Show the passwords that were guessed

Crack, on the other hand, will use up to 95% of the CPU determined by the strength of the passwords.

However, knowing if the root or user password can be brute-forced, indicating that it could be cracked by a black-hat hacker and that it must be modified, is extremely valuable

F. Security through Repositories

The most crucial and important instructions people need to follow is to be cautious about the applications they download and run on their computers. Applications are usually downloaded and updated from repositories of Linux distros, there is a wide range of applications for users to download and use. Certain software, such as show managers, is available for most of the Linux distros, but others are unique than others. Kali Linux has applications specifically designed for cybersecurity needs. Since the developers of these Linux distros approve of which repositories are permitted with the default rollout, this method of downloading software is widely regarded as quite secure. However, not everyone is available in libraries, such as Google Chrome, the company's browser. Other applications, Google Chrome is secure when downloaded. Users in general should avoid installing applications, downloading files from suspicious and unknown websites, and use the Linux repositories for installing updates of respective applications.

IV. CONCLUSION

The paper explores different methods of protecting a Linux based system from potential vulnerabilities. Usually, home users or other beginners using Linux are not aware of ports, networks, or firewalls in detail. hence the lack of information among these users lead to attacks of various types and leaves the system vulnerable to viruses and malware from internet sources. To avoid attack from potential threats, we can keep the passwords and other pass-phrases unique and uncrackable. It is a good practice to periodically update the passwords. Suspicious websites should be avoided. Only necessary services should be allowed in the firewall ports else exploits can harm your system. Anti-virus can be installed to keep your system free of malware and other harmful viruses. If a low-level user on Linux system has been compromised, other user groups can still be unaffected, this is a major advantage over other operating systems like windows. Linux offers a range of security options which are completely free, on the contrary other operating systems require you to buy a license for using the operating system as well as for securing it. You can further investigate a few of the vulnerabilities or differences between variety of viruses on one Linux system and other operating systems.

REFERENCES

- [1] M. Chowdhury and K. Nygard, Machine Learning within a Con Resistant Trust Model, The 33rd International Conference on Computers and their Applications (CATA 2018), March 19-21, 2018, Flamingo Hotel, Las Vegas, Nevada, USA.
- [2] M. Chowdhury, K. Nygard, K. Kambhampaty and M.Alruwaythi, Deception in cyberspace: Performance Focused Con Resistant Trust Algorithm, The 4th Annual Conference on Computational Science & Computational Intelligence, December 2017, Las Vegas, NV, USA.
- [3] M. Chowdhury and K. Nygard, An Empirical Study on Con Resistant Trust Algorithm for Cyberspace, the 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing, July 17-20, 2017, Athens, Greece.
- [4] M. Chowdhury and K. Nygard, Deception in Cyberspace: An Empirical Study on a Con Man Attack, The 16th Annual IEEE International Conference on Electro Information Technology, May 14-17, 2017, Lincoln, Nebraska, U.S.A.
- [5] I. Jahan and S. Sajal, Stock Price Prediction using Recurrent Neural Network Algorithm on Time-Series Data, the Midwest Instruction and Computing Symposium 2018, April 6-7, 2018 Duluth MN, USA.



- [6] I. Jahan and S. Sajal, "Prediction on Oscar Winners Based on Twitter Sentiment Analysis Using R, the 2018 SDSU Data Science Symposium, February 11, 2018, Brookings, SD, USA.
- [7] R. Gomes, M. Ahsan and A. Denton, Random Forest Classifier in SDN Framework for User-Based Indoor Localization, the 2018 IEEE International Conference on Electro/Information Technology, Rochester, Michigan, USA.
- [8] M. Ahsan, R. Gomes and A. Denton, SMOTE Implementation on Phishing Data to Enhance Cybersecurity, the 2018 IEEE International Conference on Electro/Information Technology, Rochester, Michigan, USA.
- [9] M. Chowdhury, J. Tang and K. Nygard, An Artificial Immune System Heuristic in a Smart Grid, the 28th International Conference on Computers and Their Applications, 2013, Waikiki, Honolulu, Hawaii, USA.
- [10] A. S. Tanenbaum and H. Bos, Modern Operating Systems, Boston: Pearson, 2015.
- [11] B. Hatch, J. Lee and G. Kurtz, Hacking Linux Exposed: Linux Security Secrets & Solutions, New York, The McGraw-Hill Companies, 2001, pp. 284-314.
- [12] Duncan, Rory and Z. C. Schreuders, Security implications of running windows software on a Linux system using Wine: a malware analysis study, Journal of Computer Virology and Hacking Techniques, 2018, pp. 1-22.
- [13] L. Yang, V. Ganapathy and L. Iftode, Enhancing Mobile Malware Detection with Social Collaboration, 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, New Brunswick, 2011.
- [14] Offensive Security, "Kali Linux - Official Documentation," [Online]. Available: <https://docs.kali.org/>.
- [15] R. Russel, M. Boucher, J. Morris, J. Kadlecik, H. Welte and H. Eychenne, "Man page of IPTABLES," 25 June 2015. Available: <http://ipset.netfilter.org/iptables.man.html>.
- [16] J. A. Galindo, D. Benavides and S. Segura, Debian Packages Repositories as Software Product Line Models. Towards Automated Analysis, the 1st International Workshop on Automated Configuration and Tailoring of Applications, September 20, 2010, Antwerp, Belgium.
- [17] Allen, Lee, Tedi Heriyanto, and Shakeel Ali. Kali Linux—Assuring security by penetration testing. Packt Publishing Ltd, 2014.
- [18] T. Taylor, "Linux security concerns rise as hackers target the OS," TechGenix Ltd., 9 January 2018. Available: <http://techgenix.com/linux-security-concerns/>.
- [19] D. Barrera, I. Molloy and H. Huang, IDIoT: Securing the Internet of Things like it's 1994, arXiv preprint arXiv:1712.03623 (2017).
- [20] Matthew R. Yaswinski, Md Minhaz Chowdhury, Mike Jochen. "Linux Security: A survey", 2019 IEEE International Conference on Electro Information Technology (EIT), 2019



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)