Linux Security: A Survey

Conference Paper · May 2019

DOI: 10.1109/EIT.2019.8834112

CITATION
1

READS
363

3 authors, including:

Matthew R. Yaswinski
East Stroudsburg University
1 PUBLICATION **1** CITATION
SEE PROFILE

Md. Minhaz Chowdhury
East Stroudsburg University
23 PUBLICATIONS **60** CITATIONS
SEE PROFILE

Linux Security: A Survey

Matthew R. Yaswinski, Md Minhaz Chowdhury, Mike Jochen
Department of Computer Science
East Stroudsburg University of Pennsylvania
East Stroudsburg, PA, USA
Email: myaswinski@live.esu.edu, mchowdhur1@esu.edu, mjochen@esu.edu

***Abstract*—Linux is used in a large variety of situations, from private homes on personal machines to businesses storing personal data on servers. This operating system is often seen as more secure than Windows or Mac OS X, but this does not mean that there are no security concerns to be had when running it. Attackers can crack simple passwords over a network, vulnerabilities can be exploited if firewalls do not close enough ports, and malware can be downloaded and run on a Linux system. In addition, sensitive information can be accessed through physical or network access if proper permissions are not set on the files or directories containing it. However, most of these attacks can be prevented by keeping a system up to date, maintaining a secure firewall, using an antivirus, making complex passwords, and setting strong file permissions. This paper presents a list of methods for securing a Linux system from both external and internal threats.**

Keywords- File, Firewall, Linux, Malware, Security.

I. INTRODUCTION

The usage of Linux has increased in a variety of places since the Linux kernel's creation. In many cases, Linux has replaced Windows, which costs over hundreds of dollars. This makes free distributions of Linux very attractive. Also, Linux works very well as a server operating system, so many businesses may use it for this purpose. However, out of the box, Linux distributions, like other operating systems, have limited security. In order to prevent malicious hackers from gaining access to another machine, leading to possible theft of confidential information, it is necessary to implement other security features and practices to secure the information on the machine. Security is one of the prime considerations during the use of computer systems. Security breach has many facets e.g. deception [1-4]. As counter measures of security issues, different scientific studies are in use e.g. machine learning, data mining, artificial immune system etc. Machine learning is a branch of artificial intelligence that infers a mathematical model from data e.g. data about a specific task [1, 5]. Similarly, data mining is the process of extracting specific information from a large collection of data [6-8]. Likewise, artificial immune system is a branch of artificial intelligence where the system learns from past experiences following a logical model of mammals' immune system [9].

Linux is being used by many people on their personal computers, both because it offers users easy methods of acquiring software and it is generally more lightweight, so it can be run on older hardware. Since many wireless internet networks often have poor security, if any security at all, it is largely the responsibility of the users to protect the computers they are using. Since this is the case, it is important for these users to learn security practices that can better secure their data on these less-than-ideal networks. Also, if people have more than one user on a certain machine, or there are guest accounts on a computer, security features should be put in place to prevent someone with physical access to the machine from getting access to user files that should be unavailable to them. Preventing hackers from other computers, as well as ones with physical access to a target machine, is discussed in this paper [10]. These topics includes creating firewall rules and viewing and setting file permissions. In addition, it is possible for password crackers to guess either a user password or a root password if the length is not long and the password is not complex [11]. However, they can also be used by a Linux user to test if a password is complex enough before a machine is ever left unattended. Password crackers are also being discussed in this paper.

Like other operating systems, viruses can be downloaded from the internet and cause a machine to be unusable. This includes both software made for Linux systems and software made for Windows that can be run on Linux through Wine, which is a program that creates directories to make the system appear as Windows to a program made for Windows [12]. While this results in the convenience of running some Windows software on Linux, which reduces the need of either having more than one machine with one operating system or dual-booting one system, this can introduce malware to a computer that would otherwise not be running it. Fortunately, there are ways to scan for files that may have viruses in them on Linux before they are even installed. Scanning files with an antivirus is also discussed in this paper [13].

In addition to personal computers, Linux is being used on a large number of servers, which are often rented to other businesses, around the country and the world. The reason for this is that Linux is lightweight, allowing for the companies that purchase the space on the server to access data more quickly. As a result of businesses using these servers, they can either store sensitive business data like financial documents, client data like names or birthdates or social security numbers, or both of these types of data. This means that not only business data, but likely personal client data, is being stored on servers that are running a Linux distribution.

Businesses that use or supply the server space could face legal or financial consequences if there is a breach and sensitive data is lost or stolen. Hence, it is extremely important for the

businesses to use many of the same practices, for personal computers, that are mentioned in this paper.

In this paper overall, various methods of protecting the security of a Linux system is discussed. The topics covered consist of scanning for viruses, using firewalls for preventing unwanted access from a separate machine, as well as security concerns that come with running Windows software through a Linux compatibility layer. All of these practices will result in a safer Linux machine for both servers being used for business operations and for personal computers.

This paper is organized into four sections. Section 2 describes what Linux is and the basic information on how Linux works. In addition, this section discusses a few threats that users could face. This section also describes various Linux distributions. Section 3 discusses the methods of securing a Linux system. This section includes setting passwords for both users and the root account, as well as using password crackers to test the security of the passwords [11]. This section also includes the safe methods of downloading software. Software files are scanned to detect viruses when the software download process can not follow these methods [13]. This section also mentions the security concerns of using Wine, a virtual layer that enables windows operating system to run on Unix based machines. This section covers additional topics, for example, preventing unauthorized access of external computer systems through the firewall. Section 4 presents the conclusion of this presented paper.

Although there are many security concerns that come with running a Linux system, there are many solutions to these problems. In addition, these features and practices are not difficult to implement and can save both time and money in the long run since they could prevent a system from being infected. In addition, money can be saved since private files will not be exposed to people that are not authorized access to specific files or directories. Setting up firewalls, setting file permissions, and scanning for vulnerabilities in software can secure Linux systems facing threats from viruses and malicious attackers, keeping personal and sensitive information safe.

II. Background

Linux is a kernel that a variety of operating systems run on. This kernel is open-source, meaning that anyone can use it and modify it. A large number of operating systems, known as distributions (or distros), run on this kernel. One of the most popular of these is Ubuntu, but there are many others, such as Debian. Many distributions have a focus as well. For example, Debian has access to a large amount of software, which makes it a choice for many programmers. In addition, many are used for penetration testing, such as Kali Linux [14] and Parrot Security OS. There are also distributions that are meant to be friendly for users migrating from Windows or Mac OS, such as Elementary OS and Zorin OS, and many are made to be easy to use and be aesthetically pleasing, such as Ubuntu. Since there is a large amount of uses for Linux, it is used by a very large number of users.

Another operating system based on the Linux kernel is Android. This operating system, now owned and maintained by Google, powers most of the smartphones on the planet. This means that the presence of Linux extends beyond personal computers; it reaches to mobile devices as well. The large amount of people that use a Linux-based operating system every day shows how important it is for people to keep their systems secure.

Many people make a switch to Linux because most distributions are free. This means that, many new users to the operating system may soon realize that they do not have access to all of the same software that they do when running Windows or Mac OS. So, many may turn to either virtual machines running Windows, or run Windows software directly on Linux. This can be done with a program called Wine [12]. Wine works by creating a minimal amount of system files to make it appear to be Windows from the point of view of the Windows software attempting to be run on Linux. This allows many people new to a Linux distribution to leave the Windows operating system while using still having access to some of the software that is only made for Windows, making the transition much easier. However, this opens up a new set of vulnerabilities that could be taken advantage of by people with knowledge of Wine and how it runs Windows software [3]. As a result, Linux computers can be infected by Windows software.

In addition, some Linux software, or files downloaded from the internet, can still infect Linux systems. This software may either mask itself as a real useful program, or it may contain code that can harm the security, and possibly the performance, of the system. Therefore, it is important for people to understand how to use an antivirus on Linux, and how to avoid downloading harmful software on the web [13].

One aspect of Linux that help people choose what distribution is the method that most software is obtained; it is downloaded from repositories in the command-line. Different distributions offer a large variety of software in their repositories. For example, Ubuntu gives access to software that everyday consumers would use, such as a Steam installer for video gaming. (Also, Ubuntu has a separate set of software, called snaps, that gives users even more choices.) However, a different distribution made for penetration testing, such as Kali Linux, has access to a completely different repository, including things like Metasploit to do vulnerability tests and launch exploits on vulnerable computers [14]. Also, some distributions, like Kali Linux, are based on other distributions. Kali Linux is based on Debian, so users have access to both the Debian repositories and the Kali Linux repositories. This is true of many distributions since a large number of them are based on either Debian or Ubuntu. Generally, this is a safer method of downloading software and helps prevent viruses. But some software is not available in any repositories. For example, Google Chrome is not available in repositories, but it is available for download from the internet. This software is safe, but other software may not be, so it is important for users to understand what is safe to download and what is not.

In Linux, local accounts are made on a machine for different users to gain access to the system. This is unlike the current method of using Windows, which by default asks for a Microsoft account when first setting up a machine. If someone signs in with

a guest account, or another account made for them, it is possible for them to gain access to certain files if they know the root password, or if a file has certain permissions that it should not have. This means that people should know how to set permissions to files and directories, and they should know how to set a root password to be different than a user password [10]. In addition, password crackers can be used to test the security of a password and the likelihood of it being hacked [11]. Also, depending on what services are running, another machine could have access to a person's computer if they are on the same network. Attackers may use certain ports to gain access to another user's machine and gain access to the filesystem. However, firewalls, and the iptables package [15], can help users' close certain ports, preventing attackers from exploiting vulnerabilities and putting sensitive information at risk.

Linux distributions offer potential and current users very powerful operating systems, but they can be put at risk. The software people use and download, as well as the permissions and restrictions placed on the files and services on a computer, can leave users vulnerable to attacks. However, practicing good Linux security can prevent these vulnerabilities from being taken advantage of, resulting in a safer computer experience.

III. METHODS OF SECURING A LINUX SYSTEM

There is a large amount of threats for Linux systems that make them vulnerable to hackers, but there are plenty of solutions that help to prevent these people from taking any sensitive information from them. This section describes the methods of securing a Linux system from external as well as internal threats. These methods include: securing the system with the best practice of using repositories, using antivirus to check if a downloaded software is a virus or not, taking precautions when compatibility layer is used to run Windows software on Linux systems, updating software, configuring firewall rules, password management and using different access permissions for different users.

A. Security through Repositories

One of the most important things for users to do is to be careful of what software is being downloaded and installed to the system. In Linux distributions, software is usually downloaded and installed from repositories, which hold a very large number of packages for users to download and use [16]. Some software, like different display managers, are offered for almost all distributions, but some are more specific to certain ones. For example, Kali Linux has software specific for penetration testing [17]. This method of installing software is generally seen as very safe because the creators of these Linux distributions approve of what repositories are allowed with the default shipment of the operating system. However, not everything is offered in repositories, such as Google's browser, Google Chrome. Though Chrome is a safe download, other programs may not be. Overall, users should refrain from installing software from the internet or from other sources as much as possible, and they should mainly install software from the repositories provided by the Linux distribution that they have decided to use.

B. Use of antivirus: ClamAV

If a user has no other choice but to install software from outside of a repository, he or she should know how to check if it has a virus. One of the most common methods of doing this on Windows is through an antivirus program. This has become such a common practice that Microsoft includes their own Windows Defender with every commercial version of Windows 10. To scan a specific folder or file for a virus, right-clicking an item and selecting to scan the item for viruses from the context menu can check for viruses. In addition, going into Windows Defender itself can present the option to scan the entire computer for viruses, or to do a one-time scan during boot. Similar functions can also be done with both free and paid antivirus programs for Windows. Linux however, does not have an antivirus preinstalled, but one is in almost every single Linux distribution: ClamAV, presented in [13].

ClamAV is a package within Linux repositories, or available from the ClamAV website, that scans files and directories for viruses and malware [13]. Once ClamAV is installed, a variety of commands for configuring the antivirus can be accessible by the user. Like Windows Defender, schedules can be set for setting times for the antivirus to run, specific directories can be included or excluded from the scan, and different types of scans can be done on the system. In addition, individual files and directories can be scanned outside of a scheduled scan by specifying the file or directory with the command to run it. In addition, daemons can be installed for both running the system scan and for updating the database of known viruses in the background.

For computer users who do not like to use the terminal or who are new to a Linux distribution, there is a GUI of the program to be used in addition to the main ClamAV package that allows for schedules and settings to be set and changed outside of the terminal. This program also lets the users choosing specific files to scan at any time.

Unlike Windows Defender, though, the context menu in Linux is not changed after installing the antivirus, specific files can only be scanned from executing the scan within the program itself. This program helps preventing people from malware installation onto Linux systems because this program scans the file against a constantly updated database and returns a report at the end of the scan saying if the files scanned have any viruses or malware. If they do, then the user can delete the program, preventing it from having a negative effect on the system. In order to prevent malicious software from being installed on a system, potentially putting sensitive information at risk, files shall be scanned with an antivirus such as ClamAV before they are opened or installed [13].

In summary, antivirus software recommended by recent research works are ideal candidates to be installed protecting a Linux based system from computer viruses.

C. Precautions using Linux compatibility layer: Wine

There are research works describing the potential security problems with running Windows software on Linux [12]. Usually, Windows software cannot be run on a Linux system. Linux usually allows software to be installed using .deb

files, .rpm files, or by using AppImages. Since Windows software is most often a .exe file, it cannot be installed on a Linux machine in the same way. However, it is possible to provide a compatibility layer on Linux to run Windows based software on Linux. Example of such compatibility layer is Wine [12].

The research on determining the security risks associated with Wine is still in progress [12]. Example of such research, presented in [12], is determining which malwares successfully effected the Wine i.e. which Windows malwares were successfully able to run themselves on Linux Operating Systems through the compatibility layer Wine. After testing a variety of malware, [12] found that, about 20% of the malware samples had partial success and 16.7% of the samples had complete success in running themselves in the Linux system through Wine. The experimental results from [3] concluded that the malware samples running in Wine is not likely to successful to achieve their goal of running themselves.

However, the results also confirmed that there are few malwares that can be installed and run on Linux systems through Wine. These malwares could not be presented without the use of this virtualized layer of Wine i.e. the malwares could not be installed and run on Linux without virtualization. This exceptional scenario of Windows based malware run on Linux through Wine proves the security implications that come with running software through Wine.

The reveal of Wine's security flaw does not imply a ban on its use, but implies a precaution instead. The precaution means that users should check if there are any viruses or if there is any malware in the programs they want to run before trying to install it on the Wine system. Such precaution will result in a safer system and will secure the files.

In summary, the possibility of windows based malware running successfully on Linus operating system through Wine is low. Although the possibility is low, precautions need to maintain during the installation and run of a software though any virtualization or compatibility layer on top of Linux systems.

D. Updating Software

In order to keep specific software and packages secure, they should be updated regularly. This can assure that software has the latest security patches so exploits are abused. For example, in 2017, there was a break-in of Equifax that caused Social Security numbers, addresses, and other private information to be exposed and stolen for around 143 million people. Attackers were able to break in through a vulnerability in Apache Struts, which is an open source web development framework [18]. This framework is used by at least half of all Fortune 100 companies according to Ian Folau, who is the CEO of GitLinks, so many companies and customers could have their information exposed through this vulnerability [18].

Originally, this vulnerability was discovered before the attack happened, but the framework was patched after it had occurred [18]. This not only shows how many people do not upgrade or update software as quickly as they should; it also shows the potential consequences of not updating as soon as a patch is released.

In order to keep a Linux system safe, both downloaded programs and system packages should be updated. This can be done by either going to the website where the software was downloaded and installing the updated versions, or using the terminal to run distribution-specific commands to update everything that was downloaded from the repositories, such as an updated browser or an updated kernel.

In summary, by keeping Linux systems up to date, disasters like a loss of data can potentially be avoided.

E. Firewalls

In order to prevent attacks from computers on the same network, firewalls can be set up. A firewall is a set of rules that lists what ports are open to outside machines and what the local machine can send to other machines [19]. For example, SSH is a network protocol that allows for one computer to connect to another securely over a network. However, if the other people on the network are not known or it is a public network that is in a public place, certain connections should not be allowed to be established. In addition, DDoS attacks can be launched on a machine that has too many ports open, leaving the system open to the possibility of becoming unusable until a restart.

Using the iptables package available in most Linux repositories, rules can be set to prevent attacks like these. For example, a firewall specifically for a home network can be less restrictive in order to allow for connections such as SSH. A different set of rules can be made for public networks that just allow for HTTP and HTTPS to be active but prevents ports for SSH and FTP from being used and targeted by other people on the same network. Once both of these sets of rules are made, they can be switched using "iptables-restore < rules" where rules are the file of firewall rules in the current working directory.

In summary, setting firewall rules and knowing how to set them can prevent attackers from gaining access to the Linux machine on the same network.

F. Passwords management

When a Linux distribution is installed on a system, users are usually prompted to set up a user account, which creates a directory for all the files for that user within the filesystem. These files shall be kept separate from the root user to prevent either the accidental or intentional deletion of important system files of the user. In addition, if multiple people use the same machine, different accounts shall be made for each person using it. This isolation will allow individual user files separate from each other and will also keep the files inaccessible to anyone that does not know the account password. Again, the root password and the user password shall be different from each other. This can prevent anyone from either gaining access to a user to gaining access to the root account by only knowing one password.

Password crackers can be used to guess a password that is for someone else's account, but they can also be used to test the security of a new password. For example, a program called Crack can be installed on a machine, and it can be fed an input file of a password, and the included Reporter program will display what passwords were guessed. However, depending on how good passwords are, Crack could use over 95% of the CPU

[2]. However, it is very valuable to know if a user or root password could be guessed, signaling that it could be guessed by a hacker and it should be changed.

G. File access Permissions

In order to prevent other users on a machine from gaining access to files that they should not have access to, different permissions must be set on a machine. These can be done with commands like chmod. In addition, groups of users can be made so permissions can be set for multiple users at once using the chgrp command [10]. Setting permissions for who can read, write, or execute files will prevent users from manipulating or executing files, and possibly changing the system in ways that they should not.

IV. Conclusion

Deceptions This paper presents the different ways of securing Linux based systems from different attacks. Most of the attacks on Linux systems can be prevented by keeping a system up to date, maintaining a secure firewall, using an antivirus, making complex passwords, and setting strong file permissions. Setting up firewalls, setting file permissions, and scanning for vulnerabilities in certain packages and files can keep Linux systems safe from malware and hackers. Since Linux has a variety of uses, ranging from business computers and servers to private use in homes, it is important to practice good security techniques to prevent information from being stolen or lost. For example, setting up firewalls can prevent people on the same network from gaining access to a Linux machine, and setting appropriate permissions and good passwords for other users on one Linux machine from gaining access to files that they should not have access to. Also, getting software from trusted sources, such as a distribution's repository, and checking downloaded software from the internet with an antivirus can prevent malware from being installed on the system, especially since Windows malware can be run on a Linux system using Wine. As a result, the Linux machine that these practices are done on will be safer against malware or other threats.

Knowing the different ways of securing Linux can lead to users have a safer experience on their Linux computers. It can also help businesses that use these distributions in the workplace in some way since a large amount of consumer data can be held by these systems. Overall, a variety of distributions are used for different reasons, and knowing how to secure them can save home users and corporations alike from losing important information and possibly save them money.

In conclusion, maintaining the security of a Linux system is easy to implement and it protects the integrity of sensitive information within the system.

Future research may include a more in-depth analysis of specific malware and how to prevent it from affecting a Linux machine. This could include the malware's origin and what programs or software it is often found in. The research could also include how people exploit the vulnerability and how to prevent them from doing so. Another area of research can be security of other operating systems. Specific vulnerabilities could be researched, or the differences between malware on a Linux system and a system running a different operating system. Comparisons could be made between the different malware and different fixes for vulnerabilities.

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/. [Accessed 12 November 2018].
[Accessed 12 November 2018].

[15] R. Russel, M. Boucher, J. Morris, J. Kadlecsik, H. Welte and H. Eychenne, "Man page of IPTABLES," 25 June 2015. [Online]. 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. [Online].

Available: http://techgenix.com/linux-security-concerns/. [Accessed 27 November 2018].

[19] D. Barrera, I. Molloy and H. Huang, IDIoT: Securing the Internet of Things like it's 1994, arXiv preprint arXiv:1712.03623 (2017).