JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Linux Security

Akshata Chenkote, Riddhi Patil, Siddhi Patil, Prof. Mayuri Bapat

"Department of Science & Computer Science"

MIT Arts Commerce & Science College of Savitribai Phule University

Abstract—As cornerstone of many computing infrastructures, Linux operating system play a pivotal role in the digital Landscape. However, their widespread adoption also makes them prime target for malicious actors seeking to exploit vulnerabilities. This paper are provides methods of securing Linux security. Through an analysis of common threats and mitigation strategies, including the implementation of mandatory access controls, privilege separation, and cryptographic techniques, this research elucidates the multifaceted approach required to fortify Linux system against contemporary cyber threats. Linux, as a widely adopted operating system, plays a crucial role in powering numerous devices and infrastructures, from personal computers to enterprise servers and embedded system. Overall, this paper serves as a comprehensive guide for understanding and enhancing Linux security, providing insights and recommendations to bolster the resilience of Linux system in the face of Morden cybersecurity challenges. This paper provides a detailed examination of the Linux Security. Keywords - File, Firewall, Linux, Malware, Security.

Introduction:

The usage of Linux has increased in a variety of places since the Linux kernel's creation. Linux are following a multi-layered architecture designed to provide a secure and stable computing environment. 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. Linux's distribution, 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. Linux incorporates a wide range of security features to safeguard against unauthorized access, data breaches, and malicious activities. Security breach has many facets e.g. deception[1-4]. As countermeasure 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]. Linux employs a Robot permission system, allowing administrators to control access to file directories, and system resource based on user and group privileges.

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 businesses to use many of the same practices, for personal computers, that are mentioned in this paper. Secure boot ensures the integrity of the boot process by verifying the digital signatures of bootloaders and kernel modules, thereby preventing the execution of unauthorized or malicious code during system startup. 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. Implementing security hardening measures such as disabling unnecessary services, enforcing strong password policies, and enabling firewalls can enhance the resilience of Linux systems against attacks. This section also describes various Linux distributions. Section 3 discusses the methods of securing a Linux system. Leveraging security frameworks like SELinux and app armor can provide additional layers of protection by enforcing mandatory access controls and sandboxing applications. Software files are scanned to detect viruses when the software download process can not follow these methods. Monitoring system logs and analyzing security events can help administrators detect and respond to suspicious activities in a timely manner, thereby mitigating potential security breaches. 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. Linux distribution come with built-in firewall solutions such as iptables and notables, allowing administrators to filter network traffic and define rules for packet forwarded, NAT, and port forwarding. 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.

Background:

Linux is a kernel that a variety of operating systems run on. Linux's security refers to the measures taken to protect a Linux -based computer system from unauthorized access, data breaches, and other threats. It would discuss things like vulnerabilities, threat actors, security features built into the Linux kernel, and best practices for securing Linux-based system. Many distributions have a focus as well. The background section would provide context for why Linux security is important, perhaps discussing the growing use of Linux in various industries and the increasing frequency of cyberattacks targeting Linux system. In addition, many are used for penetration testing, such as Kali Linux and Parrot Security OS. It would also touch on the history of Linux security, highlighting key developments and challenges over time.

This operating system, now owned and maintained by 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. It would discuss things like vulnerabilities, threat actors, security features built into the Linux kernel, and best practices for securing Linux-based systems. In addition, password crackers can be used to test the security of a password and the likelihood of it being hacked. 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 file system. However, firewalls, and the iptables package, can help users' close certain ports, preventing attackers from exploiting vulnerabilities and putting sensitive information at risk.

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 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 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.

1) 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 files, rpm files, or by using App Images. 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].

2) Use of antivirus: Clam AV

If a user has no other choice but to install software from outside 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: Clam AV, presented in[13]. Clam AV is a package within Linux repositories, or available from the Clam AV website, that scans files and directories for viruses and malware[13]. Once Clam AV 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 Clam AV 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.

3) Precautions using Linux compatibility layer: Wine

There are research works describing the potential security problems with running Windows software on Linux[12]. Usually, keep your wine installation

up to date with latest patches and security fixes to minimize vulnerabilities. Linux usually allows software to be installed using. deb .

In order to keep 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 updated browser or as updated kernel. In summary, stay informed about security advisories related to wine and promptly apply any recommended updates or patches to protect your system .

4) 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 an 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, who is an open source web development framework. Updating software is crucial to ensure compatibility, security, and access to the latest features. Additionally, backing up data before updating is always wise to prevent data loos.

5) 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.

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.

6) 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 file system. 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 Comparisons could be made between the different malware and different fixes for vulnerabilities.

7) 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 ch mod. In addition, file access permission to refer to rule that determine who can view, modify, or execute a file computer system. 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.

Conclusion:

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.

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 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.

3) 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.

4) 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.

5) A. S. Tanenbaum and H. Bos, Modern Operating Systems, Boston: Pearson, 2015.

6) B. Hatch, J. Lee and G. Kurtz, Hacking Linux Exposed: Linux Security Secrets & Solutions, New York, The McGraw-Hill Companies, 2001, pp. 284-314.

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)] 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.

15)] Allen, Lee, Tedi Heriyanto, and Shakeel Ali. Kali Linux–Assuring security by penetration testing. Packt Publishing Ltd, 2014.