A Study on Security Evaluation in Linux

Annmary Shaji[1], Elizabath Jaison[2], Gibin George[3]

[1]Students Corner
Santhigiri College of Computer Science,
Vazhitala, Thodupuzha, Idukki
annmaryshaji03@gmail.com

[2]Students Corner
Santhigiri College of Computer Science,
Vazhitala, Thodupuzha, Idukki
elizabathjaisonmec@gmail.com

[3]Department of Computer Science
Santhigiri College of Computer Science,
Vazhithala, Thodupuzha, Idukki
george.gibin@santhigiricollege.com

Abstract: ***Linux is an open source operating system that has gained much popularity. More and more people are using it for a variety of tasks. In order to evaluate the security of Linux we need to look at the attacks that are being used against it. Attackers have several ways to attack a server. It can come from an outside source like a hacker on the Internet, or an inside source like an employee at a workstation. Some of the different types of attacks that an attacker can use are listed in it. Security should be one of the foremost thoughts at all stages of setting up your Linux computer. 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. The main security requirements are: Authorisation, Authenticity, Privacy / Confidentiality, Integrity, Non-repudiation and Availability. Linux has in-built security model in place by default. Need to tune it up and customize as per your need which may help to make more secure system. Linux is harder to manage but offers more flexibility and configuration options. Methods that can be used to protect or secure Linux system are: Update your server, Create a new privileged user account, Upload your SSH key, Secure SSH, Enable a firewall, Install Fail2ban and Remove unused network-facing services. It also examines the overall security of Linux as a server as well as provides some possible solutions for increasing security.***

Keywords: Linux; Security; Attacks; User account; SSH key; Firewall; Fail2ban.

1. Introduction

In 1991, Linus Torvalds developed a kernel and called it Linux. Linux has grown to become one of the world's most popular operating systems. It is a free and open-source operating system and the source code can be modified and distributed to anyone commercially or noncommercially under the GNU General Public License. Students like it for the price and the open source flexibility. Network administrators like it because it can communicate with many other operating systems and run on virtually any processor. Internet Service Providers (ISPs) like it because of the native Internet support that it provides [2]. Even with all the strengths of Linux, many claim that Linux isn't secure because of its open source nature. Some feel that the open source code makes it easier for attackers to find and exploit flaws in the operating system. This paper will look at Linux as an open source operating system. We will look at the types of attacks that are used to gain access to a Linux network. We will also see how secure Linux is, compared to other commercial operating systems. We will conclude this paper with some recommendations on what can be done to make Linux more secure.

2. Linux an Open Source Operating System

In 1969, Ken Thompson and Dennis Ritchie developed a small, general-purpose operating system written in Assembly Language called UNIX. In 1973, Ken Thompson and Dennis Ritchie rewrote the UNIX operating system in C. Many vendors, such as Sun, IBM, and Hewlett-Packard, purchased the source code of UNIX and developed their own version of UNIX. The source code of these versions was not freely available, so the developers had to wait for a long time for the release of bug fixes.

In 1984, Richard Stallman, a researcher at MIT's Artificial Intelligence labs, create a free version of the UNIX operating system by the beginning of the GNU (gnu's Not UNIX) in his Free Software Foundation (FSF). In reaction to the new practice of keeping source code secret and enforcing software licensing, Stallman saw the withdrawal of source code as a curtailment of a programmer's freedom to modify and improve software. He also saw the license restriction on copying as being at odds with his philosophy of being a good neighbor and sharing ideas. Stallman's goal was to recreate a complete operating environment that was free of such restrictions, with all the tools and utilities that a computer user would ever need. He chose to model this new operating environment after the Unix operating system (OS).

Stallman realized that if he just made his code available to

everyone, that it could easily be copied by someone else, who could modify it, copyright it, and not make the new code available to everyone. For this reason Stallman chose to copyright his material with the constraint that if any code was copied that the new modified code had to be made available to everyone. The conditions are that anyone modifying the code for later redistribution has to make their source code public on the same terms. This copyright became known as the GNU General Public License [1].

Stallman wasn't successful in creating a completely new operating environment, but had created many peripheral utilities. In 1991, a Finnish Computer Science student named Linus Torvalds wrote the first version of a Unix-like kernel for his own use, and posted the code on the Internet with a request to other programmers to help him build it up into a working system. In 1992, the Linux kernel was combined with the incomplete GNU system to form a completely free operating system. This operating system is called GNU/Linux because it is a combination of GNU and Linux. The GNU/Linux operating system is commonly referred to as the Linux operating system.

Linux follows the open development model. The source code of the Linux kernel is available for study and modifications on the Internet. The current development version of Linux is always open to users. Users can also suggest modifications to the kernel code. When a new version of Linux is released, users can work on the new version to fix bugs, if any. To maintain stability, Linus Torvalds ensures strict quality control and then merges all the new code into the kernel. This is a major reason for the success of Linux.

3. Popularity of Linux

Several things have made Linux a popular operating system. Some of the strengths of Linux are:

3.1 Zero Price Tag

Due to the GNU General Public License, Linux does not need new license. This can reduce the cost to a company with several computers by a significant amount. We also need to remember even though Linux is free, there wouldn't be any benefit if it didn't do the job.

3.2 Flexibility

If you used a non-open source OS and needed something special for your company, you would have to ask the manufacturer to make this change for you. Most manufactures of a commercial OS are not interested in customizing the OS for each company. Even if they were, this would cost a lot of money. With Linux you have the source code that you can freely customize to your needs.

3.3 Stability

Unix is known for its stability. This is one of the reasons that Linux was modeled after it. Linux has the advantage of a quarter century of Unix experience to draw on. Most significantly, the open-source code model of Linux seems to ensure that bugs are detected and fixed early.

3.4 Compliance

Due to the GNU General Public License, Linux cannot have proprietary features. The license therefore ensures that the only changes to the system that will last are those that are accepted by the "community". The community has no vested interest in creating proprietary standards and protocols, and so the OS naturally coalesces around industry standards. Linux is a POSIX-compliant (Standards Defining Unix) OS and it supports ANSI, ISO, IETF and W3C standards [1].

3.5 Hardware Support

Linux will run on virtually every known processor, whether RISC or CISC. Intel has recognized the popularity of Linux and has made an objective to make Linux run fastest on its chips. Intel is pushing its Uniform Driver Interface (UDI) as a common Unix approach to device drivers, and is trying to get the Linux community to help write the drivers [1]. Another Linux strength is that Linux has the ability to run on older computers with less memory and disk capacity than other operating systems. The one drawback is that not all peripherals and cards are supported by Linux, but as the popularity for Linux grows this will change.

3.6 Native Internet Support

Open Source Apache, the world’s most popular webserver, runs naturally on Linux. Addon modules like mod_perl allows Perl CGI scripts to be interpreted and run within Apache’s memory space. The mod_jserv module allows Apache to use Java servlets. The mod_php module allows Apache to run HTML-embedded scripts in a Perl-like Hypertext Pre-Processor language called PHP, a program that works exactly analogously to Microsoft’s Active Server Pages. Linux also supports firewalls like ipchains [1]. These things and others have made Linux a very popular server OS among Internet Service Providers (ISPs). Linux is an excellent, standard platform for web applications. You can use it to build a complete, secure Internet site, including router, firewall, proxy, webserver, mailserver, database server and directory server.

3.7 Interoperability with Existing System

As a server Linux needs to be able to coexist with other operating systems. Linux can talk SPX/IPX in a Netware environment, Appletalk in a Mac crowd, and even SNA to IBM mainframes. Linux can even coexist with Windows systems because it is able to speak TCP/IP [1]. One of the newest languages that Linux can speak is Session Message Block (SMB) protocol. SMB is the protocol that Windows9x/2000 operating systems use for sharing files and printers.

4. Attacks

An attack can be perpetrated by an insider or from outside the organization. An inside attack is an attack initiated by an entity inside the security perimeter (an insider), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

An outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an outsider). On the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments. And their attacks can be either active or passive. An active attack attempts to alter system resources or affect their operation, so it compromises the Integrity or Availability. A passive attack attempts to learn or make use of information from the system, but does not affect system resources, so it compromises Confidentiality.

5. Security requirements

Linux is not a secure OS. To make Linux a secure OS, or at least as secure as it can be we need some security requirements [3]:

- **Authorisation** - Only allow those that need access to the data.
- **Authenticity** - Verifying they are who they say they are.
- **Privacy / Confidentiality** - Ensure personal information is not being compromised.
- **Integrity** - Ensuring that the data has not been tampered with.
- **Non-repudiation** - Confirmation that data is received. The ability to prove it in court.
- **Availability** - Ensure that the system can perform it's required function

6. Security measures

6.1 Update your server

The first thing you should do to secure your server is to update the local repositories and upgrade the operating system and installed applications by applying the latest patches.

6.2 Create a new privileged user account

Next, create a new user account. You should never log into your server as **root**. Instead, create your own account ("**<user>**"), give it **sudo** rights, and use it to log into your server [4].

6.3 Upload your SSH key

You'll want to use an SSH key to log into your new server. You can upload your pre-generated SSH key to your new server using the **ssh-copy-id** command [4]. Now you can log into your new server without having to type in a password.

6.4 Secure SSH

Open /etc/ssh/sshd_config using your text editor of choice, then disable SSH password authentication and restrict root from logging in remotely. Next, restrict the SSH service to either IPv4 or IPv6 by modifying the AddressFamily option [4]. Restart the SSH service to enable your changes. Note that it's a good idea to have two active connections to your server before restarting the SSH server. Having that extra connection allows you to fix anything should the restart go wrong.

6.5 Enable a firewall

Now you need to install a firewall, enable it, and configure it only to allow network traffic that you designate. Uncomplicated Firewall (UFW) is an easy-to-use interface to iptables that greatly simplifies the process of configuring a firewall. UFW denies all incoming connections and allows all outgoing connections [4]. This means any application on your server can reach the internet, but anything trying to reach your server cannot connect.

6.6 Install Fail2ban

Fail2ban is an application that examines server logs looking for repeated or automated attacks. If any are found, it will alter the firewall to block the attacker's IP address either permanently or for a specified amount of time. The software will continuously examine the log files looking for attacks. After a while, the app will build up quite a list of banned IP addresses.

6.7 Remove unused network-facing services

Almost all Linux server operating systems come with a few network-facing services enabled. You'll want to keep most of them. However, there are a few that you might want to remove. You can see all running network services by using the ss command.

7. Linux is More Secure than Windows

When we hear the word "Linux", we automatically think about the heavy-duty computer users who embraced the technology a couple of decades ago. And that's reasonable, but as CBT Nuggets Linux trainer Shawn Powers says in a recent Trainer Talk, "Linux is just not as scary and mysterious as everybody seems to think" [5]. In recent years, the open source operating system has become so user-friendly, anyone can install and work with it. But that isn't the only reason Linux is the right choice for your business. Tech professionals have long chosen Linux for their servers and computers due to its security. Security often comes down to end-user training regardless of OS, there are some things that make Linux systems more secure than other environments. This is especially true when it comes to malicious software.
Here are a few reasons your devices will be more secure with a Linux operating system in place:

7.1 Hackers don't typically target Linux

The most cited reason for Linux's safety relates to its low usage numbers. Linux has less than three percent of the market, compared to Windows, which operates on more than 80 percent of all devices [5]. Microsoft and Linux are practically friends now, so that might change a little.
For those creating malicious software, it makes more sense to target Windows, because one piece of code will reach the largest segment of the population. This keeps Linux users

safer, as even Mac has a larger segment of the market.

7.2 It's more difficult to execute a dangerous attachment in the Linux OS

Linux is easy to learn with the right resources, but there are extra steps to take before executing a malicious software. On Linux, users need to save the attachment before executing it, and if set up correctly, they would need permissions granted before they could open it. These extra steps can help safeguard a business from the internal user Kill that is so often the cause of security breaches.

7.3 Linux does not give users admin access by default

In a Windows environment, users are often given a high level of access automatically. This lets them click on links and download files indiscriminately, easily leading to the issues mentioned above. Many users don't have access to the root directories on their computers, which means that even if they do manage to infect their systems, they'll be limited in the damage they can do.
Of course, good security practices mean that users shouldn't be clicking those links in the first place. Regardless of what device you use, it ultimately comes down to whether your users employ good security awareness practices — and it's up to you to train them.

7.4 Linux has more people looking out for security issues

Although Microsoft has an army of developers working on their OS, the number of developers working on Linux is bigger. And that's one of the biggest reasons to go Linux [5]. With so many people monitoring for issues, it's likely someone will catch a vulnerability long before hackers can target it. Once spotted, Linux users don't have to wait months for Microsoft to finally investigate the issue and fix it. They can repair it themselves, from wherever they are. This not only improves security for the platform, but it also keeps things stable to prevent downtime.
Linux computers tend to be more secure than their Windows counterparts, with less susceptibility to viruses and malware. There's debate as to whether this is because Linux is inherently more secure, or because Linux's low percentage of computer users doesn't entice hackers and malware creators. However, due to the fluid and frequent updates to Linux distributions, security concerns are quickly addressed. By number of viruses, we can see a trend in that Windows has FAR more viruses for it than Linux does and that's purely because it's more lucrative to hack for Windows since you have a greater chance of getting the thing you want. By design, Linux is more secure than Windows because of the way it handles user permissions. The main protection on Linux is that running an ".exe" is much harder [5]. Linux does not process executables without explicit permission as this is not a separate and independent process

Although Linux may be safer, there are things administrators can do to keep systems safe. If a hacker does target your network, these small measures will either prevent it or minimize any damage it might do. This includes encrypting the hard drive of each device, which can be done at the time of installation. A firewall can also help keep your systems safe, and best of all, you have plenty of options available for free. Lastly, make sure you keep all your software up-to-date, just as you would do with any operating system.
If you have been thinking about making the switch to Linux, there has never been a better time. With so much training available to help you learn the basics, you'll be able to deploy Linux within your network infrastructure with minimal effort. Once you have Linux in place, you can build from there, boosting the security across your entire network.

8. Conclusion

Throughout this paper we have evaluated the Linux operating system. Attacks that can be used to gain access to a Linux network have been discussed. We know that with all the strengths of Linux, many claim that Linux isn't secure because of its open source nature. And we discuss some things that can be done to make Linux more secure. And we make a comparison between Linux and window and conclude that Linux is more secure than other OS.

References

[1] http://www.security-science.com/pdf/security-evaluation-of-the-linux-operating-system.pdf
[2] https://www.researchgate.net/publication/335795125_Linux_Security_A_Survey
[3] http://www.penguintutor.com/linux/introduction-linux-security
[4] https://opensource.com/article/19/10/linux-server-security
[5] https://www.cbtnuggets.com/blog/certifications/microsoft/why-linux-is-more-secure-than-windows

Author Profile


Annmary Shaji UG Scholar in BCA in Santhigiri College of Computer Science, Vazhithala


Elizabath Jaison UG Scholar in BCA in Santhigiri College of Computer Science, Vazhithala


Mr. Gibin George Asst. Professor in Santhigiri College of Computer Science, Vazhithala