Common Linux Security Issues You Should Monitor

Linux is one of the best operating systems and has provided its services to its users for 30 years now. It is currently rated as the most powerful operating system. This is because it has more users than Windows and the cloud platform for Microsoft. Many users have left windows and are now using Linux because of security threats and vulnerabilities. For a long time, Linux has been more secure than other operating systems, but do you think there are no threats?

Even though Linux is considered one of the most secure OS, it still has drawbacks. In the recent past, Windows experienced serious security threats, and Linux operating systems can also be affected. As users are increasing in the Linux-based cloud, it is becoming a potential target for cybercriminals, which brings more security concerns. These include malware, security gaps, and misconfigurations. For this reason, users are now using VPNs to make their online activities safe. Therefore, we have listed some of the Linux security threats you should consider.

What are 3 examples of Linux security issues?

1. Linux Trojans and backdoors
2. Dual booting with other devices.
3. Ransomware.

Linux Trojans and Backdoors

A Trojan package is a program that gives backdoor access to your data. Most Linux users believe this is not possible while running the program. However, in august 2016, the discovery of Linux security bug changed this. It had self- distribution capabilities; it could perform tasks such as targeting specific content management systems, sending spam e-mails and even carrying out DDoS attacks. It can also infect other machines connected via peer-to-peer. The Trojan is designed for existing autonomously.

Dual Booting With Windows

Even though you won't risk getting viruses with dual booting, the data stored in your Linux PC could be affected if you do it with windows. Doing this will essentially give intruders better chances of accessing your PC.

With your user name and a password to one of the accounts, they can access and interfere with your data. With the tailored software made specifically to read Linux partitions, your Linux data could be at risk of intruders illegally accessing your Windows partition. For example, a dual booter can use Diskinternals Linux Reader at any time to access the files stored in your Linux partition.

If your computer is not well secured, anyone can access it, and if they don't make it to sign into Linux, they may try their Luck using windows. If they manage with either your local windows account or Microsoft online account, your data will no longer be secured. It doesn't matter if they are stored in an Ext4 or NTFS partition.

In other words, you should never assume you are safe if you run on a Linux program. Cyber security criminals will always come up with new ways of infecting or stealing data, no matter which operating system you are on.

Ransomware

It requires the person attacking your system to encrypt and install your data. The thoughts going through your mind must be how this is possible if you are using Linux OS. However, the possibility of this happening is very likely. In 2015 we saw this happen through the Linux encoder ransomware. The use of this program is increasing each day; this is because it is based on web servers. It would be great if you took extra caution when installing any software from unsafe websites or sites. Before you install any software, you should ensure you do the necessary checks online to ascertain if other users have reported any suspicious activities or issues.

Backdoors

It is an unauthorized undocumented method of gaining access to a computer device. Software and device manufacturers often include backdoors for completely legitimate and explainable reasons, such as enabling support teams to administrate and access a server in case of a malfunction. However, these backdoors can also be used by criminals to act against the device's owner's preferences.

Ways To Enhance Linux Security:

1. Use a VPN

VPN enables you to have a secured internet connection which keeps your data hidden. A VPN like VeePN is also responsible for maintaining top servers globally to provide a fast and stable internet connection to its users. Get the best VPN provider to enhance your security.

2. Disable Booting from External Devices

Individuals with bad intentions can use external devices like USBs to access confidential information. It would help if you disabled booting for external devices. This is similar to hacking.

3. Avoid Unnecessary Software

You can be tempted to install new software, but you may find out that not all web services are necessary. Adding more programs to your device makes you more susceptible to more potential attacks in the future.

4. Update Your Software Regularly

Good management of your Linux server security includes addressing and implementing solutions to emerging vulnerabilities.

5. Use Strong and Unique Passwords

A strong password is a feature that every server should have to avoid any possible threats. To avoid any intruders, a good password should have at least ten characters and other features like upper and lowercase letters or special characters.

What is a security vulnerability in Linux?

Linux vulnerability is an accidental flaw in a system that makes it prone to exploitation in terms of access by intruders.

What are some Linux vulnerabilities?

1. CVE-2022-0492
2. CVE-2022-0998
3. CVE-2022-0435
4. CVE-2022-28893
5. CVE-2022-0995