The theory that convinced most of us to join the Linux OS universe is its impenetrable nature. We were excited that using a Linux Operating system did not require us to have an anti-virus installed on our systems. As the latter statements might be true, we should be careful of using too many sweeteners to build up assumptions about the Linux operating system security metrics. We would not want to deal with any diabetic outcomes in the practical world.

The Linux operating system is risk-free on paper but characterized by vulnerabilities in a production environment. These vulnerabilities entail risk-centered and harmful programs incubating viruses, rootkits, and ransomware.

If you invest your skills to be a Linux OS administrator, you need to sharpen your security measures skills, especially when dealing with production servers. Big brands continue to invest in coping with evolving new security threats targeting the Linux OS. The evolution of these measures propels the development of adaptive security tools. They detect the malware and other flaws in a Linux system and initiate useful, corrective, and preventive mechanisms to counter the viable system threats.

Source URL: http://www.tuxmachines.org/node/144877

Links: