IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Linux Security – Review

Siddhesh Mote, Abu Amir Choudhary, Mayuri Bapat

MIT ARTS, COMMERCE & SCIENECE COLLEGE

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

1. INTRODUCTION:

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.

Security of Linux is a massive subject and there are many complete books on the subject. I couldn't put everything in this one tutorial, but this does give a basic introduction to security and how the techniques, and tools additional security on a Linux computer. Hopefully this will provide sufficient information to be able to investigate other sources of information.

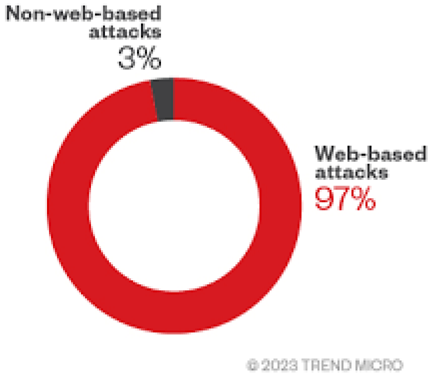
Although Linux users are must less prone to viruses than some other major operating systems, there are still many security issues facing Linux users and administrators.

One of the most important steps in any task is to identify why you are doing it. Rather than just saying we need to make a system secure you need to consider what is meant by secure, what risks there are associated with any data that's available, what impact your security measures will have on your users. Without first considering any of these factors how else will you know if you've met your goal of making a system secure.

2. Linux security module:

As Mentioned in the literature survey there are various configuration files such as system configuration file and server configuration files which contains attributes that are critical. This module will check such configuration files and scan for attribute which are important from security perspective. This module check current attribute value with best security value required for that attribute. If current configured value is not a best security value then it will consider it as vulnerability and generates the vulnerability report. Generated report is given to the security module. Linux system consists of very strong logging mechanism maintains the log for kernel, servers, users, system processes etc. These entire logs by default placed at different location. This module collects the log fromthese various places and generates report. This generated report is useful for finding the vulnerability. Generated report is given to the security modl

This module collects the vulnerability report and log analysis report and applies security. By looking vulnerability report this module get the vulnerable configuration files and modify them with best security practice. Similarly by looking log analysis report this module apply the security attributes accordingly. This model is actually responsible for modifying the configuration files and making the Linux more secure.



These numbers not only solidify the dependability and continued expansion of the operating system's use.

3.Top Vulnerabilities:

Analyzing our telemetry for the most abused vulnerabilities in the wild, the most prominent Common Vulnerabilities and Exposures (CVEs) that we observed listed the following security gaps exploited for threats and attacks:

CVE-2021-44228, also known as the Apache Log4j vulnerability, has a severity score of 10 in the Common Vulnerability Scoring System (CVSS) CVE-2017-12611 and CVE-2018-11776, both Apache Struts vulnerabilities CVE-2022-26134, a zero-day vulnerability in Atlassian Confluence server and data center with a critical rating of 9.8

CVE-2018-15473, an OpenSSH vulnerability that affects all Linux and Unix platforms

Specific applications on Linux platforms have become prime targets for malicious actors as these applications have vulnerabilities that make them susceptible to various types of attacks. Based on our collected data, WordPress emerged as the most frequently targeted application. Additionally, a significant rise in the exploitation of zero-day vulnerabilities, specifically CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105 in Apache Log4j, have captured the attention of attackers. We also saw a rise in the exploitation of Zoho Manage Engine and Magento.

We also noted some old security gaps (CVE-2013-4671, CVE-2013-4670, and CVE-2013-1617) making it to the top 10 of most exploited vulnerabilities in the last year. Aside from the possibility of computers and/or legacy systems still being in use and remaining unpatched, the inclusion of these old vulnerabilities

4.Linux threat landscape:

With its widespread adoption across personal computing, enterprise servers, and cloud infrastructures, Linux is an increasingly attractive target for malware, exploits, and social engineering, among others. To help organizations and guide their respective security teams, we analysed the trends, techniques, patterns, and data relevant to the abuse of the operating system last year. We dissect the different sections and vectors of Linux that were commonly abused by cybercriminals and attackers. Contrary to the belief that Linux is immune to malware, several types, such as ransomware, cryptocurrency miners, web shells, and rootkits have been used to target Linux systems. We break down the malware types and their commonly exploited vulnerabilities While less common than its Windows counterparts, Linux ransomware is not unheard of. From the first quarter of 2022 to 2023, our Midyear Security Report cited that our sensors detected a 62% increase in Linux ransomware attack attempts. One such example is the KillDisk ransomware that targeted financial institutions. Ransomware often exploits vulnerabilities related to outdated software, poor system configurations, or phishing attacks. Regular software updates, careful email handling, and robust backup strategies are critical defences again .

5.LINUX KERNEL FEATURE

Control Groups (Cgroups) are a kernel mechanism for specifying and enforcing hardware resource limits and access controls to a process or a group of processes. Their goal is to prevent a process from hogging all available resources and starving other processes and containers on the host. Thus, croup's isolate and limit a given resource over a group of processes to control performance or security. Controlled resources include Central Processing Unit (CPU) shares, Random Access Memory (RAM), network bandwidth, and disk I/O [5]. It can also be used for task control. The security protection provided by Croup's are:

• Conclusion

This has explained the different factors that need to be considered when working on a security solution for a Linux system. Although the names of some tools have been included it has not gone into the details of how to configure the tools or what changes should be made to

the system to lock out potential attackers. Having worked through this information it should be possible to work out a plan on which areas to focus resources and provide enough background knowledge as a platform for further research.

• 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.

[3]R. Spencer, S. Smalley, P. Loscocco, M. Hibler, D. Andersen, and J. Lepreau. The Flask Securit y Architecture:System Support for Diverse Security Policies. In The Eighth USENIX Security Symposium, pages 123– 139, August 199 9.

://efaidnbmnnnibpcajpcglclefindmkaj/http://troindia.in/journal/ijacet/vol2iss1/12-16.pdf

[4] By Pawan Kinger, Sunil Bharti and Magno Oliveria https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-linux-threat-landscape-report#section

[5] W. Felter, A. Ferreira, R. Raja Mony, and J. Rubio, An Updated Performance Comparison of Virtual Machines and Linux Containers, IBM Research Report, July 21, 2014 https://domino.research.ibm.com/library/cyberdig.nsf/papers/0929052195DD819C85257D2300681E7B/$File/rc25482.pdf