УДК 004.056.53

Makovii. A.V.

SECURING SOFTWARE ON LINUX: ESSENTIAL PRACTICES, FEASIBILITY AND STRATEGIES

Vinnytsia National Technical University

Анотація

У цій статті розглядається проблема системи безпеки Linux, розвінчуються хибні уявлення та з'ясовується необхідність додаткових механізмів захисту від нових загроз.

Ключові слова: Linux, відкритий код, безпека, загрози, антивірусне програмне забезпечення, операційна система.

Abstract

This article explores the problem of Linux security, explains why it is important to have additional mechanisms to protect against new threats.

Keywords: Linux, open-source code, security, threads, antivirus software, operation system.

Introduction

Previously, it was widely believed among the IT community that the Linux operating system was threat immune, its architecture was not susceptible to attacks, and its open source code was protected from weaknesses by its very nature. However, in recent years, this perception has changed even among experts [1]. It has become apparent that Linux, like any other system, depends on programs and services that can be exploited by attackers. For example, web servers required to access the Internet can be sensitive to Cross Site Scripting (XSS) attacks. In addition, Linux systems are exposed to malware, such as viruses, trojans, and harmful programs that can cause damage, compromise personal data, or exploit the system for malicious purposes.

Research results

Not long ago, the main target of cybercriminals was only end users, to make money, and therefore Linux servers were relatively safe at the time. Today, attackers are targeting businesses with great potential to make much more money, and you don't have to look far to see it. For example, in 2021, experts discovered a modification of the RansomEXX trojan that could encrypt data on Linux machines. The attack was designed specifically for targeted attacks on specific organizations, with the code and ransomware being customized for each new target [1].

There are certain safety measures that increase security in Linux. First, you should use a VPN, as a VPN allows you to have a secure Internet connection that hides data. Second, avoid booting from external devices. Attackers can use external devices to access sensitive information. Third, avoid unnecessary software. Users may be forced to install new software that adds a large number of programs to the device, making it more susceptible to new potential attacks in the future. It is important to update software regularly, as new releases contain fixes for problems and solutions for new security issues. It is necessary to use strong passwords, because to avoid threats, you need a strong password that will contain at least ten characters: numbers, uppercase and lowercase letters, special characters [6].

But in some cases, low-cost tools that provide basic operating system protection may not be enough. Large businesses and companies need to have a much higher level of protection that will take place in real time. As such, paid programs are offered that provide a wide range of security features. Below are the top 3 most popular software security tools for Linux that include antivirus protection [2]:

GravityZone Endpoint Security Tool for Linux. The producer of this product is the Romanian company Bitdefender. The software offers a wide range of functionality to protect Linux systems. The characteristics and functionality of this program are as follows [3]:

- protection against viruses for file servers;

- the ability to protect (scale) up to 100 computers at one time;
- security threat analysis;
- scanning not only for harmful files, but also for suspicious processes that programs run on the network.

Security for Linux. The manufacturer is the Czech company Avast. It includes the following functionalities [4]:

- scanning and detection of viruses;
- provides a centralized control point for IT administrators;
- automatic sending of regular updates.

VirusScan Enterprise for Linux. The developer is the American company McAfee Antivirus. The software provides the following features [5]:

- real-time protection;
- automatic scanning of the file server in the background;
- blocking new malicious programs;
- firewall protection.

One of the problems of software protection is the problem of protection against unauthorized research and dumping, i.e., the removal of programs from memory. Anti-dumping programs for Linux include the following:

Armadillo. The country of development is Germany. The program has the following features [7]:

- free access and open source, which makes the program a good choice for users looking for low-cost anti-dumping solutions;
- is simple and easy to use;
- effective code protection. The program can effectively protect executable files from reverse engineering and other code changes;
- supports several file formats. The program can protect a wide range of executable files, including ELF, PE32, Mach-O.

MPRESS. The country of development is the United States. The program has the following features and functions [8]:

- free and open source;
- support for many file formats;
- powerful compression capabilities, i.e. reducing the size of executable files;
- security features such as encryption and obfuscation. The program can encrypt executable files to protect them from unauthorized access and obfuscate the code to make it harder for attackers to understand and crack.

ExeGuard. Country: The country of origin is the United States. The program has the following features and functions [9]:

- is designed to protect executable files from reverse engineering, which is what it was developed for;
- prevents attackers from modifying the code of executable files, i.e., implements protection against hacking;
- the program implements code obfuscation, protection against unauthorized debugging, and copy protection;
- supports many different file formats.

Conclusion

Linux is a powerful and flexible operating system that is used in a wide range of applications. However, just like any other operating system, Linux is sensitive to malware and other threats, such as unauthorized copying, exploration, hacking, and dumping. To protect your Linux system from these threats, you need to use security software tools, such as antivirus programs, firewalls, firewalls, and other security features. In some cases, low-cost operating system security tools that provide basic protection are not enough. Therefore, it is necessary to use additional security tools.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Pozhogin A. Does Linux need protecting? [Електронний ресурс]. Режим доступу: URL : https://www.kaspersky.com/blog/linux-security-hybrid-cloud/41259/

2. Vigderman A., Turner G. The Best Antivirus Software for Linux [Електронний ресурс]. Режим доступу: URL : https://www.security.org/antivirus/best/linux/#avast-antivirus

3. Website of Bitdefender [Електронний ресурс]. Режим доступу: URL : https://www.bitdefender.com/media/html/consumer/new/2020/cl-offer-opt/?pid=50offer&cid=aff|c|ir&dclid=CjgKEAiA0syqBhCNhIGNlpb1m1gSJAAuHv5EpNWu7JXxCnVRkGSqotkLmg6i74eVcSMKoLpkl0dx4_D_BwE

4. Website of Avast [Електронний ресурс]. Режим доступу: URL : https://www.avast.com/en-gb/store?c=108922&utm_medium=affiliate&utm_source=commissionjunction&utm_campaign=100003607&utm_content=13156052&couponfield=yes&cjevent=902c4b0ed3485c3df27d63d51903c8d1e7c01874b51c27b9e&trafficSource=affiliate&partnerid=100003607&programtype=CJ&clickID=7714a65b830711ee81c100760a18ba73#all

5. Website of McAfee Antivirus [Електронний ресурс]. Режим доступу: URL : https://www.mcafee.com/consumer/en-us/landing-page/direct/aff/mtp-family/desktop/mcafee-total-protection.html?irclickid=UFJVdb2KjxyPW6vSiK0Vt3rWUkFVvqTucy571w0&clickid=UFJVdb2KjxyPW6vSiK0Vt3rWUkFVvqTucy571w0&csrc=LQ&csrcl2=1377816&sharedid=&adid=74047&ccstype=partnerlinks&ccoe=direct&ccoel2=am&affid=1079&param3=&param2=&param1=&&culture=en-us&prgt=lc

6. Dehtiarova Y. Three problems of security in Linux and hot to solve them. [Електронний ресурс]. Режим доступу: URL : https://blog.iteducenter.ua/articles/linux-security/

7. Website of Armadillo. [Електронний ресурс]. Режим доступу: URL : https://sourceforge.net/projects/arma/

8. Website of MPRESS. [Електронний ресурс]. – Режим доступу: URL : https://www.djmaster.com/freepascal/bindings/mpg123.php

9. Website of ExeGuard. [Електронний ресурс]. Режим доступу: URL : https://softexe.net/

10. Туржанська І. Захист програмного забезпечення в linux: необхідність, доцільність і способи [Електронний ресурс]. Режим доступу: URL : https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2024/paper/view/19801

Маковій Андрій Васильович – студент групи 5ПІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: makoviystud@gmail.com

Науковий керівник - Бойко Юлія Василівна, старший викладач кафедри іноземних мов, ВНТУ , e-mail : boiko@vntu.edu.ua

Makovii Andrii V. – student of the 5PI-22b group, faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia e-mail: makoviystud@gmail.com

Supervisor - Boyko Yuliia, senior teacher of foreign languages department ,VNTU , e-mail : boiko@vntu.edu.ua