УДК 004.056.53

Туржанська І.Д.

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В LINUX: НЕОБХІДНІСТЬ, ДОЦІЛЬНІСТЬ І СПОСОБИ

Вінницький національний технічний університет

Анотація

У статті розглядається питання захисту програмного забезпечення в операційній системі Linux. Розкривається необхідність і доцільність захисту, а також розглядаються можливі способи його реалізації, а також програмні засоби, які можуть стати у нагоді.

Ключові слова: Linux, програмне забезпечення, безпека, захист, витоки інформації, антивірусне програмне забезпечення, дампінг пам'яті.

Abstract

The article deals with the issue of software protection in the Linux operating system. The need and expediency of protection is revealed, as well as possible methods of its implementation are considered, as well as software tools that can be useful.

Keywords: Linux, software, security, protection, information leaks, antivirus software, memory dumping.

Вступ

До недавнього часу значна частина IT-спільноти була переконана, що операційна система Linux не потребує захисту, що архітектура системи є невразливою і не представляє ніякого інтересу для зловмисників, а сама ідеологія відкритого вихідного коду слугує свого роду гарантією для несподіваних серйозних уразливостей. Однак останніми роками навіть фахівці дійшли висновку, що це не так [1]. Linux використовує програми та служби, які можуть бути вразливим до атак. Наприклад, веб-сервери, які використовуються для доступу до Інтернету, можуть бути вразливими до атак типу "Cross Site Scripting" (XSS). Крім того, Linux-системи можуть бути атаковані за допомогою шкідливого програмного забезпечення, такого як віруси, трояни та шкідливі програми. Шкідливе програмне забезпечення може завдати шкоди системі, скористатись особистою інформацією або використати систему для розсилання спаму.

Результати досліджень

Донедавна головною ціллю кіберзлочинців були тільки кінцеві користувачі, задля заробітку грошей, і тому сервери Linux були відносно безпечні на той час. На сьогодні зловмисники націлились на бізнеси з великими потенціалом для отримування значно більших грошей і, щоб це у цьому переконатись, не потрібно далеко ходити. Наприклад, у 2021 експерти виявили модифікацію троянської програми RansomEXX, яка могла шифрувати дані на машинах Linux. Шкідлива програма була розроблена саме для цілеспрямованих атак на конкретні організації, сам код і повідомлення про викуп налаштовувались для кожної нової цілі [1].

Існують певні міри обережності, які підвищують безпеку в Linux. По-перше, слід використовувати VPN, оскільки VPN дозволяє мати захищене підключення до Інтернету, яке приховує дані. По-друге, уникати завантаження із зовнішніх пристроїв. Зловмисники можуть використовувати зовнішні пристрої для доступу до конфіденційної інформації. По-третє, уникати непотрібного програмного забезпечення. У користувача може виникнути спокуса встановити нове програмне забезпечення, яке додає велику кількість програм на пристрій, що робить його більш сприйнятливим до нових потенційних атак у майбутньому. Важливо регулярно оновлювати програмне забезпечення, адже нові випуски містять усунення проблем та впровадження рішень для нових вразливостей. Необхідним є використання надійних паролів, оскільки, щоб уникнути загроз,

потрібен стійкий пароль, який буде містити принаймні десять символів: цифри, великі та малі літери, спеціальні символи [6].

Але у деяких випадках бюджетних інструментів, що забезпечують базовий захист операційної системи, може бути не достатньо. Великі бізнеси та компанії повинні мати набагато вищий рівень захисту, який буде відбуватись в реальному часі. У такий спосіб пропонуються платні програми, які надають широкий спектр функцій щодо захисту. Нижче наведено топ 3 найпопулярніших засобів для захисту програмного забезпечення під Linux, що включають антивірусний захист [2]. Перелік цих програмних продуктів для Linux такий.

GravityZone Endpoint Security Tool for Linux. Виробником даного продукту є румунська компанія Bitdefender. Програмне забезпечення пропонує широкий спектр функціональних можливостей для захисту Linux-систем. Характеристики і функціональні можливості цієї програми такі [3]:

- захист від шкідливих програм для файлових серверів;
- можливість одночасного захисту (масштабування) до 100 комп'ютерів;
- оцінювання вразливостей;
- сканування не тільки на наявність шкідливих файлів, а й на наявність підозрілих процесів, які програми виконують у мережі.

Security for Linux. Виробником є чеська компанія Avast. Включає такі функціональні можливості [4]:

- сканування та виявляння вірусів;
- надання централізованого пункт управління IT-адміністраторами;
- автоматичне надсилання регулярних оновлень.

VirusScan Enterprise for Linux. Виробником є американська компанія McAfee Antivirus. Програмний засіб надає такі можливості [5]:

- захист в реальному часі;
- автоматичне сканування файлового сервера у фоновому режимі;
- блокування нових шкідливих програм;
- захист брандмауером.

Однією з проблем захисту програмного забезпечення є проблема захисту від несанкціонованого дослідження та дампінгу, тобто, від зняття програм з пам'яті. До антидампінгових програм під Linux можна віднести такі.

Armadillo. Країна-розробник – Німеччина. Програма має такі особливості [7]:

- вільний доступ та відкритий код, що робить програму гарним вибором для користувачів, які шукають доступні антидампінгові рішення;
- проста і зручна у використанні;
- ефективний захист коду. Програма може ефективно захищати виконувані файли від зворотної інженерії та інших втручань в код;
- підтримує декілька форматів файлів. Програма може захищати широкий спектр виконуваних файлів, включаючи ELF, PE32, Mach-O.

MPRESS. Країна-розробник – США. Програма має такі особливості і функції [8]:

- безкоштовний та відкритий код;
- підтримка багатьох форматів файлів;
- потужні можливості ущільнення, тобто зменшення розміру виконуваних файлів;
- функції безпеки, такі як шифрування та обфускація. Програма може шифрувати виконувані файли, щоб захистити їх від несанкціонованого доступу, а також обфускувати код, щоб ускладнити його розуміння та злам зловмисниками.

ExeGuard. Країна: Країна-розробник – США. Програма має такі особливості і функції [9]:

- призначена для захисту виконуваних файлів від реверсивного інжинірингу – саме для цього вона і розроблялась;
- запобігає зловмисникам змінювати код виконуваних файлів, тобто реалізує захист від зламу;
- програма реалізує обфускацію коду, захист від несанкціонованого налагодження та захист від копіювання;
- підтримує багато різних форматів файлів.

Висновок

Linux – це потужна та гнучка операційна система, яка використовується в широкому спектрі застосувань. Однак, як і будь-яка інша операційна система, Linux є вразливою до шкідливого програмного забезпечення та інших загроз, таких, як несанкціоноване копіювання, дослідження, злам та дампінг. Для захисту системи Linux від цих загроз необхідно використовувати програмні інструменти для забезпечення безпеки, наприклад, антивірусні програми, брандмауери, файерволи та інші захисні механізми. У деяких випадках бюджетні інструменти щодо забезпечення захисту операційної системи, які надають базовий захист, не є достатніми. Тому необхідно використовувати додаткові інструменти захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pozhogin A. Does Linux need protecting? [Електронний ресурс]. Режим доступу: URL : https://www.kaspersky.com/blog/linux-security-hybrid-cloud/41259/ (дата останнього доступу 14.11.2023).
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=10000360 7&utm_content=13156052&couponfield=yes&cjevent=902c4b0ed3485c3df27d63d51903c8d1e7c01874 b51c27b9e&trafficSource=affiliate&partnerid=100003607&programtype=CJ&clickID=7714a65b830711 ee81c100760a18ba73#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=UFJVdb2KjxyP W6vSiK0Vt3rWUkFVvqTucy571w0&csrc=LQ&csrcl2=1377816&sharedid=&adid=74047&ccstype=par tnerlinks&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/

Туржанська Ірина Дмитрівна – студентка групи 2БС-22Б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: turzhanskayaryna@gmail.com

Науковий керівник – Каплун Валентина Аполінаріївна

Turzhanska Iryna Dmitrievna – student of group 2BS-22B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: turzhanskayaryna@gmail.com

Supervisor – Kalpun Valentyna