Т. 10. №2. 2024
https://doi.org/10.33619/2414-2948/99

УДК 004.056 https://doi.org/10.33619/2414-2948/99/39

ОСНОВНЫЕ МЕХАНИЗМЫ БЕЗОПАСНОСТИ В LINUX

©Лиманова Н. И., *ORCID: 0000-0003-2924-5602, SPIN-код: 9799-8380, д-р техн. наук, Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия, nataliya.i.limanova@gmail.com*
©Анашкин А. С., *ORCID: 0000-0003-4803-3058, Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия, a_anashkinn@icloud.com*

BASIC SECURITY MECHANISMS IN LINUX

©Limanova N., *ORCID: 0000-0003-2924-5602, SPIN-code: 9799-8380, Dr. habil., Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia, nataliya.i.limanova@gmail.com*
©Anashkin A., *ORCID: 0000-0003-4803-3058, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia, a_anashkinn@icloud.com*

Аннотация. Статья представляет обзор ключевых аспектов обеспечения безопасности в операционной системе Linux. Актуальность данной работы заключается в том, что в свете быстрого развития технологий и повышенных угроз в сфере информационной безопасности, особое внимание уделяется механизмам, обеспечивающим стабильную защиту данных и системных ресурсов. Статья начинается с рассмотрения основных принципов безопасности, таких как принцип наименьших привилегий и обеспечение доступа по принципу необходимости. Далее рассматриваются современные механизмы аутентификации и авторизации, включая роль Pluggable Authentication Modules и многопользовательские правила Security-Enhanced Linux. Особое внимание уделяется системам контроля доступа, включая механизмы управления правами доступа к файлам через избирательное управление доступом (DAC) и мандатное управление доступом (MAC). Анализируются брандмауэры iptables и firewalld, как ключевые инструменты для обеспечения безопасности сетевого взаимодействия. Статья также охватывает современные тенденции и вызовы в области безопасности Linux, а также обзор последних обновлений ядра и программного обеспечения. В итоге читатель получит комплексное представление о механизмах безопасности в Linux, что позволит ему принимать информированные решения для эффективной защиты своих систем и данных.

Abstract. The article provides an overview of the key security aspects of the Linux operating system. The relevance of this work lies in the fact that in light of the rapid development of technology and increased threats in the field of information security, special attention is paid to mechanisms that ensure stable protection of data and system resources. The article begins by reviewing basic security principles such as the principle of least privilege and need-based access. Next, we look at modern authentication and authorization mechanisms, including the role of Pluggable Authentication Modules (PAM) and Security-Enhanced Linux (SELinux) multi-user rules. Particular attention is paid to access control systems, including mechanisms for managing access rights to files through the Discretionary Access Control (DAC) and Mandatory Access Control (MAC). The iptables and firewalld firewalls are analyzed as key tools for ensuring the security of network interactions. The article also covers current Linux security trends and challenges, as well as an overview of the latest kernel and software updates. Ultimately, the reader

Т. 10. №2. 2024
https://doi.org/10.33619/2414-2948/99

will gain a comprehensive understanding of Linux security mechanisms, allowing him to make informed decisions to effectively protect his systems and data.

Ключевые слова: информационная безопасность, механизмы безопасности, механизмы аутентификации и авторизации, избирательное управление доступом, мандатное управление доступом.

Keywords: information security, security mechanisms, authentication and authorization mechanisms, discretionary access control, mandate access management.

Linux, как открытая операционная система, привлекает внимание многих пользователей своей гибкостью и стабильностью. Однако, чтобы обеспечить полноценную безопасность в сетевом взаимодействии и сохранить целостность данных, необходимо внимательно настраивать механизмы безопасности. В данной статье рассмотрены основные принципы и механизмы, которые способствуют безопасности в Linux. Основополагающими принципами безопасности являются принцип наименьших привилегий и принцип необходимости. Первый предполагает, что пользователи и программы должны иметь только те привилегии, которые необходимы для выполнения своих задач. Второй принцип заключается в обеспечении доступа только к необходимым ресурсам, минимизируя потенциальные уязвимости.

Современные механизмы аутентификации и авторизации в Linux играют ключевую роль в обеспечении безопасности. PAM (Pluggable Authentication Modules) предоставляет стандартизированный способ для приложений проведения аутентификации. SELinux (Security-Enhanced Linux) обеспечивает мандатное управление доступом, ограничивая привилегии программ и пользователя на основе политик безопасности [1, с. 248–250].

Системы контроля доступа в Linux включают механизмы управления правами доступа к файлам через систему прав доступа (DAC) и мандатное управление доступом (MAC). DAC использует владельца файла для определения доступа, в то время как MAC применяет строгие политики, управляющие доступом на основе атрибутов и полномочий [4].

Брандмауэры являются неотъемлемой частью обеспечения безопасности сетевого взаимодействия в Linux. Iptables — классический инструмент для настройки правил фильтрации пакетов. Firewalld предоставляет более удобный интерфейс, позволяя администраторам управлять правилами брандмауэра динамически [3].

Сегодня безопасность Linux сталкивается с постоянными вызовами и требует постоянного совершенствования. Современные тенденции включают в себя разработку новых механизмов безопасности, обновление ядра и программного обеспечения. Новые вызовы включают в себя угрозы виртуализации, атаки на уровне аппаратного обеспечения и растущую сложность конфигураций систем [1, с. 815].

Последние обновления ядра и программного обеспечения направлены на закрытие уязвимостей и улучшение средств безопасности. Активное обновление системы, использование инструментов мониторинга и анализа безопасности помогают администраторам оперативно реагировать на новые угрозы и обеспечивать безопасность системы [4].

Криптография играет важную роль в обеспечении безопасности Linux. Шифрование файловых систем, использование протоколов шифрования для защиты сетевого трафика и подпись цифровых сертификатов — все эти методы способствуют укреплению защиты данных от несанкционированного доступа и подделки [1, с. 129].

Системы аудита в Linux предоставляют возможность отслеживать события, связанные с

безопасностью. Аудиторские журналы позволяют администраторам следить за изменениями в системе, анализировать попытки взлома и предпринимать меры в ответ на инциденты безопасности. С увеличением сетевого взаимодействия особое внимание уделяется сетевой безопасности. Механизмы, такие как Virtual Private Networks (VPN), Intrusion Detection Systems (IDS), и Secure Sockets Layer (SSL) помогают защитить передачу данных по сети от несанкционированного доступа и атак [1, с. 173].

Ни одна система безопасности не может быть полностью эффективной без компетентного персонала. Обучение сотрудников по правилам безопасности, проведение тренингов по реагированию на инциденты и следующие за последними тенденциями в области безопасности — все это содействует формированию культуры безопасности в организации [1, с. 468].

Итак, поддержание безопасности в Linux — это постоянный процесс, требующий внимания к деталям и актуальности механизмов безопасности. Соблюдение принципов наименьших привилегий и необходимости, использование современных механизмов аутентификации и авторизации, а также эффективное управление доступом к ресурсам сети и файлов – важные шаги к обеспечению безопасности в среде Linux.

Список литературы:

1. Anderson R. Security engineering: a guide to building dependable distributed systems. – John Wiley & Sons, 2020. https://doi.org/10.1002/9781119644682

2. Love R. Linux system programming: talking directly to the kernel and C library. O'Reilly Media, Inc., 2013.

3. Безопасность в Linux. https://habr.com/ru/companies/slurm/articles/694222/

4. Security. Arch Linux Wiki. https://wiki.archlinux.org/title/Security

References:

1. Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons. https://doi.org/10.1002/9781119644682

2. Love, R. (2013). *Linux system programming: talking directly to the kernel and C library*. O'Reilly Media, Inc. http://hdl.handle.net/10563/52223

3. Security in Linux. https://habr.com/ru/companies/slurm/articles/694222/ (in Russian)

4. Security. Arch Linux Wiki. https://wiki.archlinux.org/title/Security (in Russian)

Работа поступила
в редакцию 16.01.2024 г.

Принята к публикации
24.01.2024 г.

Ссылка для цитирования:

Лиманова Н. И., Анашкин А. С. Основные механизмы безопасности в Linux // Бюллетень науки и практики. 2024. Т. 10. №2. С. 404-406. https://doi.org/10.33619/2414-2948/99/39

Cite as (APA):

Limanova, N., & Anashkin, A. (2024). Basic Security Mechanisms in Linux. *Bulletin of Science and Practice, 10*(2), 404-406. (in Russian). https://doi.org/10.33619/2414-2948/99/39