УДК 004.451

Шайкова А.А., студент, 3 курс, кафедра прикладной информатики и информационных технологий, Белгородский государственный национальный исследовательский университет, РФ, г. Белгород

Научный руководитель: Резниченко Олег Сергеевич ст. преподаватель кафедры прикладной информатики и информационных технологий, Белгородский государственный национальны исследовательский университет, РФ, г. Белгород

ОБЗОР ИНСТРУМЕНТАРИЯ ЗАЩИТЫ ОТ СБОЕВ И ВОССТАНОВЛЕНИЯ ОС СЕМЕЙСТВА LINUX

Аннотация: *Считается что ОС семейства Linux одни из самых защищенных, но даже при работе с ними могут возникать ошибки и сбои. В данной статье рассматриваются средства, помогающие свести шанс их появления к минимуму.*

Ключевые слова: *Linux, сбои, восстановление, защита, данные.*

Annotation: *It is believed that the Linux OS family is one of the most secure, but even when working with them, errors and failures can occur. This article discusses means that help reduce the chance of their occurrence to a minimum.*

Keywords: *Linux, failures, recovery, protection, data.*

Основные особенности защиты Linux заключаются в: многоуровневой архитектуре безопасности; системе прав доступа и разрешений; постоянном обновлении безопасности с помощью активного сообщества разработчиков, инструментах, позволяющих администратору отслеживать системные процессы и многих других.

Особое внимание стоить уделить обширной системе разграничения прав доступа, основанной на принципе наименьших привилегий, то есть предоставлении пользователю или процессу лишь тех прав, которые необходимы для осуществления предполагаемых действий. За соблюдением этого принципа в ОС следит SELinux – система принудительного контроля доступа, реализованная на уровне ядра, когда применение контроля производится администраторами и системой. Ее компонентами являются: Policy Enforcement Server – механизм организации контроля доступа; БД политик безопасности; Взаимодействие с перехватчиком событий LSM и др. Она может работать в одном из трех режимов: Enforcing – строгое соблюдение политик безопасности; Permissive – допускается нарушение ограничений; Disabled – политики безопасности не действуют.

Контролировать нарушение политик безопасности и преодоление ограничений помогает Pluggable Authentication Modules – модульная система аутентификации, которая используется везде, где требуется аутентификация пользователя или проверка его прав, в том числе при превышении привилегий через команду sudo [1]. Также в Linux относительно недавно появилась система реализующая разграничение прав доступа к файлам на основе их атрибутов – POSIX ACL [2]. Если до ее появления права доступа Linux предоставляли очень мало возможностей и настроить их было сложно, то теперь данная система позволяет точно указать права конкретных пользователей и групп.

Кроме всего вышеперечисленного существует также AppArmor – система упреждающей защиты, основанная на политиках безопасности (профилях). Данная система используется LSM–модуль ядра, который при запуске приложения проверяет наличие его профиля, и если профиль существует, то ограничивает выполнение системных вызовов в соответствии с ним [3].

Таким образом ОС семейства Linux обладают множеством функций и возможностей, которые делают их надежными и безопасными. Однако, безопасность зависит не только от операционной системы, но и от правильной настройки, управления и использования системы. К средствам и методам обеспечения безопасности и минимизации сбоев и ошибок можно отнести следующие [4]:

1. Своевременное обновление безопасности и установка стабильных версий системы. Так как код систем Linux является открытым, над его улучшением работает не только компания, но и активное сообщество разработчиков. Такие обновления часто помогают исправить сбои и уязвимости. Для обновления ОС достаточно зайти в настройки системы или ввести соответствующую конкретной ОС команду в терминал: для Ubuntu и Debian: «sudo apt– get update» и «sudo apt– get upgrade», для Fedora и Centos: «yum update».

2. Ограничение доступа к внешним сервисам. Для этого достаточно отредактировать файлы /etc/hosts.allow и /etc/hosts.deny.

3. Подключение к серверам от имени пользователя с ограниченными правами. Чтобы создать такого пользователя нужно ввести в терминале команду: для Ubuntu и Debian: «adduser», для CentOS и Fedora «useradd && passwd», и внести запрашиваемую системой информацию. Далее необходимо добавить пользователя в его группу.

4. Настройки прав доступа для пользователей. В Linux можно устанавливать права доступа на файлы и директории, обычно это права на запуск, чтение и изменение файла. В Linux типы такого доступа помечаются с помощью двух видов нотаций: алфавитной и восьмеричной. В алфавитной нотации разрешения отмечены буквами: r – чтение, w – изменение, x – запуск. В восьмеричной системе счисления уровень доступа к файлам определяется числами от 0 до 7, где 0 означает отсутствие доступа, а 7 означает полный

доступ на изменение, чтение и выполнение: 4 – чтение, 2 – изменение, 1 – запуск. Для этого можно использовать команду «chmod».

5. Ограничение терминалов. Для защиты консоли можно ограничить права администратора на использование определенных терминалов, указав используемые в /etc/securetty.

6. Изменение пароля. Пароль пользователя системой, а особенно администратора должен быть надежным и периодически изменятся. Для изменения пароля можно использовать команды: для Ubuntu и Debian: «passwd». Кроме того, можно установить период устаревания пароля: «chage – M … – m … – W … ИмяПользователя».

7. Оповещения при использовании команды «sudo». Администратор может запретить пользователям использовать команды администратора или поставить дополнительную защиту в виде уведомлений на почту во время использования «sudo». Для этого в конец файла конфигурации «sudo» нужно добавить две строки вида: «mailto yourname@yourdomain.com mail_always on».

8. Мониторинг файловой системы. Для отслеживания изменений файлов в системе можно использовать как встроенные средства, например, утилиту strace или сторонние инструменты такие как Tripwire [5].

9. Использование антивируса. Хотя количество вредоносных программ, нацеленных на Linux, меньше, они все равно существуют. Антивирусы, предназначенные для семейства Linux, могут помочь защитить систему от вредоносных угроз и, кроме того, могут быть полезны для предотвращения распространения вредоносного кода при работе в среде смешанной системы [6]. Так отечественными антивирусными ПО для Linux являются Dr.Web и Kaspersky Endpoint Security. А к наиболее популярному бесплатно распространяемому ПО можно отнести ClamTK.

В системах семейства Linux есть средства и дополнительные утилиты восстановления информации в случаях если все же произошел сбой или

некорректное действие со стороны пользователя, приведшие к потере информации или повреждению системы.

Для начала стоит рассмотреть режим восстановления – особый режим загрузки операционной системы Linux, который предназначен для решения проблем с загрузкой и работой системы в штатном режиме. При запуске данного режима загружается и работает минимум необходимых сервисов, и вся работа происходит в консольном режиме. Войти в него можно через меню Grub, выбрав «Дополнительные параметры для…» и в представленном списке нажав на строку, которая содержит надпись "(recovery mode)" [7].

К встроенным средствам восстановления можно отнести инструмент командной строки dd, который входит в установленную ОС. К минусам можно отнести избыточность копирования и необходимость отдельного физического устройства, но она весьма удобна для полного копирования дисков и создания загрузочных накопителей. Вызвать ее можно командой «sudo dd if=раздел диска of=файл копии bs=Размер», где if – имя входного файла. Если оно пропущено, то считается как стандартный ввод. Of – имя выходного файла. Bs – размер блока.

Также, существует инструмент командной строки tar, который в основном применяется для копирования данных в пределах одного компьютера. Например, для копирования полного дерева файловых объектов можно ввести в командную строку команду «sudo tar – – xattrs – – acls – czf название архива \ – – exclude=/название исключенного из архива файла \ /». С помощью этого инструмента можно заранее архивировать всю систему, а затем восстановить ее при повреждении. Также, очень часто для восстановления пользовательских файлов используют такие дополнительные утилиты как testdisk, photorec и многие другие [8].

Для восстановления системных файлов пользователь может применить служебную программу командной строки fsck, которая позволяет проверять целостность системных файлов и восстанавливать их. Синтаксис утилиты

выглядит следующим образом: «$ fsck [опции] [опции_файловой_системы] [раздел_диска]».

Для создания точек восстановления и резервных копий системы можно использовать различные утилиты и приложения, одним из популярных вариантов является Systemback. Для этого достаточно открыть приложение и воспользоваться его интерфейсом. Также популярностью пользуются программы TimeShift, TestDisk и SystemRescue CD.

Таким образом помимо встроенных систем защиты в ОС Linux, существуют различные средства и утилиты для предотвращения сбоев и восстановления. К ним относятся: средства профилактики – система обновлений и антивирусное ПО, системы ограничения и разделения прав пользователя, а также утилиты восстановления утерянных данных, как пользовательских файлов, так и всей системы в целом.

Использованные источники:

1. Механизмы безопасности в Linux: краткий ликбез [Электронный ресурс]. URL: https://otus.ru/nest/post/823/

2. POSIX ACL [Электронный ресурс]. URL: https://www.kryukov.biz/soderzhanie/sistema– bezopasnosti/posix– acl/

3. Как обезопасить Linux– систему: 10 советов [Электронный ресурс]. URL: https://habr.com/ru/companies/1cloud/articles/309696/

4. Базовая безопасность в Linux [Электронный ресурс]. URL: https://serverspace.ru/support/help/bazovaya– bezopasnost– linux/

5. Базовая настройка безопасности Linux– систем [Электронный ресурс]. URL: https://1cloud.ru/help/linux/linux_security_basics

6. Антивирус для Linux: необходимость или избыточность? [Электронный ресурс]. URL: https://uchet– jkh.ru/i/antivirus– dlya– linux– neobxodimost– ili– izbytocnost)

7. Linux: Как зайти в Recovery Mode (Режим восстановления) [Электронный ресурс]. URL: https://pc.ru/articles/linux– kak– zajti– v– recovery– mode– rezhim– vosstanovleniya

8. 12 инструментов для восстановления Linux [Электронный ресурс]. URL: https://blog.sedicomm.com/2017/03/23/12– instrumentov– dlya– vosstanovleniya– linux/