Тюленева Евгения Михайловна
ФГБОУ ВО «Курганский государственный университет»,
студентка кафедры «Безопасность информационных и автоматизированных систем»,
evgeniya.tyulenyova.98@mail.ru, Курган, Россия
Ревняков Евгений Николаевич
ФГБОУ ВО «Курганский государственный университет»,
канд. техн. наук, доцент кафедры «Безопасность информационных и автоматизированных систем»,
aphaline@mail.ru, Курган, Россия
Змызгова Татьяна Рудольфовна
ФГБОУ ВО «Курганский государственный университет»,
канд. техн. наук, доцент кафедры «Программное обеспечение автоматизированных систем»,
tr.zmyzgova@gmail.com, Курган, Россия

МЕТОДИКА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОС GNU/LINUX

УДК 004.056.53

Аннотация. GNU/Linux – широко используемая система, и задача по обеспечению ее безопасности сейчас довольно актуальна. В данной статье приводится минимальный набор средств для обеспечения безопасности операционной системы GNU/Linux, подходящий для широкого круга пользователей.
Ключевые слова: программное обеспечение, GNU/Linux, несанкционированный доступ.

Abstract. GNU/Linux is a widely used system, and the task of ensuring its security is quite relevant now. This article provides a minimal set of security tools for the GNU/Linux operating system, suitable for a wide range of users.
Keywords: software, GNU/Linux, unauthorized access.

В течение последнего десятилетия все больше компаний переходят на Linux-системы, что позволяет им экономить на стоимости программного обеспечения. Кроме того, в России из-за импортозамещения госорганы переходят на отечественные операционные системы, в том числе созданные на базе Linux. И не только Россия, так, например, власти Южной Кореи в 2020-ом году запланировали перевод всех госструктур на южнокорейские дистрибутивы Linux [4]. Из этого следует, что сейчас перед многими стоит задача в обеспечении безопасности Linux-систем.

Безопасность операционной системы – это комплексная задача. Для нее не существует определенных алгоритмов и абсолютно верных решений. Следовательно, количество комбинаций методов огромно. В данной статье мы ограничимся небольшим списком программ и рекомендаций для Linux-систем. Для удобства, все средства будут разбиты на три категории: аутентификация, файловая защита и сетевая защита.

Для начала рассмотрим блок аутентификации.

Каждому пользователю необходим пароль. Считается, что пароль надежный, если содержит в себе от 8 до 12 символов разного регистра, а также цифры. Для генерации паролей в Linux можно использовать утилиту OpenSSL, набрав в терминале следующую команду:

$ openssl rand –base64 8,

где 8 – количество сгенерированных символов, а затем закодированных base64.

Следует защититься и от брутфорс-атак, для чего подойдет утилита Fail2ban. Она ищет в лог-файлах следы попыток подбора пароля и блокирует IP-адреса, с которых они осуществлялись. Файлы конфигурации находятся в каталоге /etc/fail2ban.

Установка:

$ sudo apt-get install fail2ban

Перезапуск после изменения файла конфигурации:

$ sudo /etc/init.d/fail2ban restart

Перейдем к файловой защите.

Самое первое, что нужно сделать в файловой системе, – это отделить системные файлы от пользовательских. Папки usr, home, var, var/tmp и tmp должны располагаться на отдельных логических разделах диска [3]. Необходимо шифрование. Но вместо того, чтобы зашифровать целый диск, лучше ограничиться домашним каталогом и своп-файлом, так как обычно

именно в них хранится конфиденциальная информация. Для этих целей подойдет утилита ecrypts.

Установка:

```
$ sudo apt-get install ecryptfs-utils
```

Шифрование своп-файла:

```
$ sudo ecryptfs-setup-swap
```

Создание каталогов для зашифрованных и расшифрованных файлов:

```
$ ecryptfs-setup-private
```

Шифрование домашнего каталога:

```
# ecryptfs-migrate-home -u <имя пользователя>
```

При удалении файлов с зашифрованных носителей чаще всего в памяти не остается следов, то есть остаточной информации. Но съемные носители, такие как флешки и карты памяти, придется очищать другим способом. Например, утилитой srm, которая удаляет файлы и заполняет оставшиеся блоки данных случайными значениями.

Установка:

```
$ sudo apt-get install secure-delete
```

При удалении можно указать несколько файлов:

```
$ srm <файл1> <файл2>
```

Если необходимо отформатировать носитель полностью, то подойдет утилита dd [6]:

```
# dd if=/dev/zero of=/dev/SpecialDeviceFile,
```

где SpecialDeviceFile – это имя файла устройства.

Ко всему прочему, файлы следует проверять на целостность, что возможно с утилитой Tripwire. Она создает базу эталонных значений контрольных сумм файлов, а при запуске снова вычисляет их и сравнивает со значениями из базы [8].

Теперь рассмотрим средства сетевой защиты.

Сначала ограничим доступ к машине, настроив межсетевой экран. Существует множество способов настройки, но самый простой – это

использовать скрипт ipkungfu, который сам сгенерирует все необходимые правила. Для базовой защиты его будет достаточно. Установка:

```
$ sudo apt-get install ipkungfu
```

Исправим файл конфигурации ipkungfu.conf, расположенный в /etc/ipkungfu. При наличии локальной сети необходимо указать адрес сети вместе с маской, если же нет, то loopback-адрес (127.0.0.1).

```
LOCAL_NET="127.0.0.1"
```

Затем указываем, что данная машина не является шлюзом:

```
GATEWAY=0
```

Закрываем порт 135 (удаленный вызов процедур) и необязательные открытые порты NetBios:

```
FORBIDDEN_PORTS="135 137 139"
```

Блокируем команду ping из внешней сети:

```
BLOCK_PINGS=1
```

Также нужно установить флаг «DROP» для некоторых пакетов и сканирования портов:

```
SUSPECT="DROP"
KNOWN_BAD="DROP"
PORT_SCAN="DROP"
```

Чтобы запустить ipkungfu, необходимо в файле /etc/default/ipkungfu заменить IPKFSTART = 0 на IPKFSTART = 1 и запустить:

```
$ sudo ipkungfu
```

Но межсетевой экран не поможет защититься от руткитов, с помощью которых злоумышленник получает удаленный доступ к машине. Для их обнаружения на Linux существует утилита rkhunter. Она проверяет систему на предмет руткитов и, если такой найдется, укажет его расположение.

Установка и запуск:

```
$ sudo apt-get install rkhunter
$ sudo rkhunter -c --sk
```

Запускать rkhunter рекомендуется ежедневно. Для этого создаем файл /etc/cron.daily/rkhunter.sh и пишем в него следующее:

#!/bin/bash

/usr/bin/rkhunter -c --cronjob 2>&1 | mail -s "RKhunter Scan Results" <адрес электронной почты>

На электронную почту будут приходить результаты сканирования. Теперь нужно разрешить выполнение:

$ sudo chmod +x /etc/cron.daily/rkhunter.sh

Для обновления баз rkhunter используется следующая команда:

$ sudo rkhunter --update

Немаловажно вовремя выявлять вторжения в систему. Наиболее популярным инструментом является Snort. Его преимущество в том, что ничего не нужно конфигурировать, для защиты типовых сервисов хватит и стандартных настроек.

$ sudo apt-get install snort

При установке указываем интерфейс и диапазон адресов сети, в данном случае enp0s3 и 192.168.10.0/24, представлен на рисунке 1.

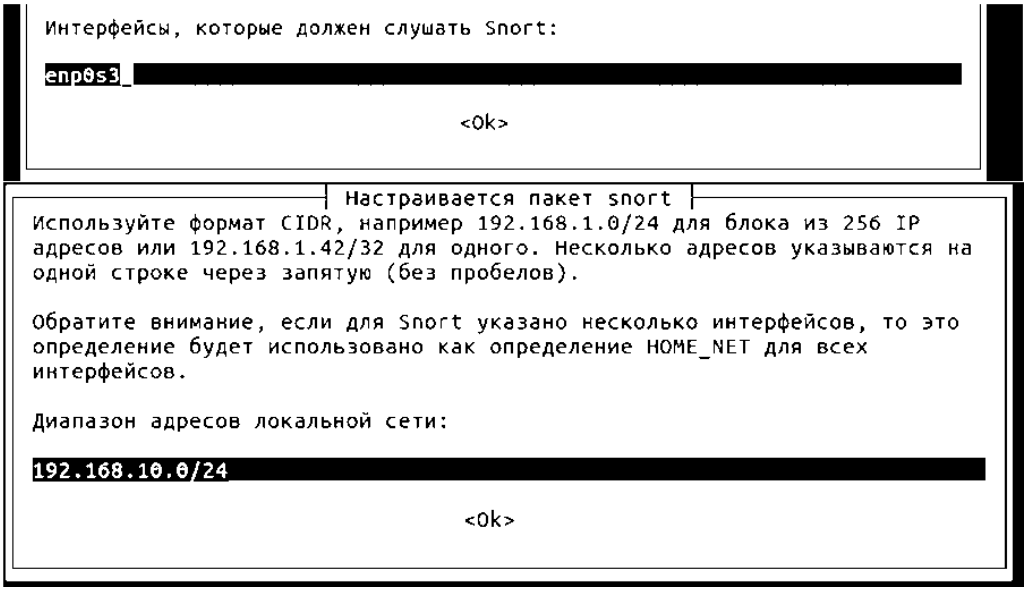

Рис. 1. Настройки snort

Затем вводим команду для работы утилиты в фоновом режиме:

$ snort -D

Впоследствии необходимо периодически проверять лог-файл на предмет вторжений.

В завершение приведем несколько дополнительных советов по защите:

1. своевременно обновлять программное обеспечение, что позволит уменьшить количество уязвимостей;
2. запретить аутентификацию по паролю для FTP и Telnet, а вместо этого использовать ключи ssh [7];
3. устанавливать только необходимое программное обеспечение, потому что чем больше ПО, тем больше уязвимостей у системы;
4. удалить возможность использования учетной записи root, вместо этого использовать sudo;
5. делать резервные копии и хранить их отдельно от системы [1].

Таким образом, мы получили минимальный перечень средств защиты для Linux-системы. Они повысят шансы того, что злоумышленники не доберутся до информации, хранящейся на машине, и не нарушат ее целостность, конфиденциальность, доступность. Данная методика может быть использована пользователями с минимальными знаниями, так что область ее применения является достаточно обширной.

Список использованной литературы

1. Unix и Linux: руководство системного администратора / Немет Эви, Снайдер Гарт, Хейн Трент, Уэйли Бэн. 4-е изд.: Пер. с англ. М.: ООО “ИД Вильямс”, 2012. 1312 с.

2. Полякова Е. Н., Дорофеева А. С. Обзор современных систем разграничения доступа к ресурсам вычислительной системы // Вестник Курганского государственного университета. 2016. № 3 (42). С. 122–127.

3. 40 Linux Server Hardening Security Tips [2019 edition]: сайт. – URL: https://www.cyberciti.biz/tips/linux-security.html (дата обращения: 10.06.2020).

4. Власти Южной Кореи отказываются от Windows и переезжают на Linux: сайт. URL: https://www.cnews.ru/news/top/2020-02-11_yuzhnaya_koreya_perevodit_gosuchrezhdeniya (дата обращения: 29.06.2020).

5. Гайд по обеспечению безопасности Linux-системы: сайт. URL: https://xakep.ru/2014/10/02/paranoid-linuxoid/ (дата обращения: 10.06.2020).

6. Команда dd и все, что с ней связано: сайт. URL: https://habr.com/ru/post/117050/ (дата обращения: 23.06.2020).

7. Памятка пользователям ssh: сайт. URL: https://habr.com/ru/post/122445/ (дата обращения: 26.06.2020).

8. Установка и настройка tripwire для проверки целостности файлов: сайт. URL: https://1cloud.ru/help/security/nastroika-tripwire-dlya-proverki-tselosnosti-failov (дата обращения: 25.06.2020).

Филанович Антон Николаевич
к. ф.-м. н., доцент
ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»,
a.n.filanovich@urfu.ru, Екатеринбург, Россия
Повзнер Александр Александрович
д. ф.-м. н., профессор, заведующий кафедрой,
ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»,
a.a.povzner@urfu.ru, Екатеринбург, Россия

ОБ ИСПОЛЬЗОВАНИИ ВИРТУАЛЬНОГО ЛАБОРАТОРНОГО ПРАКТИКУМА В ДИСТАНЦИОННОМ ПРЕПОДАВАНИИ ФИЗИКИ В ПЕРИОД ПАНДЕМИИ

УДК 372.853

Аннотация. В работе рассматривается опыт использования виртуальных лабораторных работ как вынужденной замены натурного практикума по физике. Обсуждаются преимущества и недостатки ранее разработанного комплекса виртуальных лабораторных работ, а также общие проблемы замещения натурного практикума виртуальным. Сформулировано направление дальнейшего развития виртуального практикума.

Ключевые слова: виртуальный практикум, физический практикум, технологии дистанционного образования.

Absrtact. The paper considers the experience of using virtual laboratory work as a compelled replacement for real laboratory classes in physics. The advantages and disadvantages of the developed complex of virtual labs are discussed, as well as the general problems of replacing a