МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__» _____2016 г.

ЛАБОРАТОРНАЯ РАБОТА № 2
«Реализация политики разграничения доступа средствами ОС Linux»

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных систем», «Администрирование вычислительных сетей» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01.

Курск 2016

УДК 004
Составители: В.В. Гефнер, И.В. Калуцкий

Рецензент
Кандидат технических наук, доцент кафедры
защиты информации и систем связи *А.Г. Спеваков*

Реализация политики разграничения доступа средствами ОС Linux: методические указания к выполнению лабораторных и практических работ по дисциплинам: «Администрирование вычислительных систем», «Администрирование вычислительных сетей» / Юго-Зап. гос. ун-т; сост.: В.В. Гефнер, И.В. Калуцкий, Курск, 2016. 88 с.: ил. нет, Библиогр.: с. 88

Содержат сведения по вопросам реализации политик разграничения доступа средствами ОС GNU/Linux.

Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Комплексная защита объектов информатизации», «Информационная безопасность», «Информационная безопасность автоматизированных систем».

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных систем», «Администрирование вычислительных сетей» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01 дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать . 31.05.16 Формат 60x84 1/16.
Усл. печ. л. 5,1 . Уч. –изд.л. 4,6 . Тираж 30 экз. Заказ 588 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

Цель работы 4
Порядок выполнения работы 4
Содержание отчёта 4
Выполнение работы 5
Временная нейтрализация парольной защиты 19
Контрольные вопросы 22
Библиографический список 23

Цель работы

Цель лабораторной работы – знакомство и получение практических навыков реализации разграничения доступа средствами операционной системы GNU/Linux.

Порядок выполнения работы

1. Изучить теоретическую часть.
2. Выполнить задания, поставленные в данном методическом указании.
3. Сделать вывод по проделанной работе.

Содержание отчёта

1. Титульный лист.
2. Задание на лабораторную работу.
3. Ход выполнения лабораторной работы со скриншотами.
4. Вывод по лабораторной работе.

Выполнение работы

1. Изучите теоретический материал, изложенный в методических указаниях к лабораторной работе №1 «Исследование файловых объектов с правами пользователя».
2. Зарегистрируйтесь в системе с правами суперпользователя.
3. С помощью команды **cat /etc/group** откройте для просмотра файл групп. *Файл представляет собой таблицу, каждая строка которой является отдельной учетной записью, состоящей из 4 полей, разделенных двоеточиями. Первое и третье поле соответственно – имя и номер (GID) группы, второе – обычно отсутствующий групповой пароль, четвертое – имена пользователей, включенных в данную группу дополнительно. Они обладают групповыми правами на файлы владельцев, входящих в данную основную группу.*
4. С помощью команды **cat /etc/passwd** откройте для просмотра файл учетных записей. *Файл представляет собой таблицу, каждая строка которой является отдельной учетной записью, состоящей из 7 полей. Обратите внимание на характерные разделители полей (регистрационное имя, признак пароля,*

идентификатор пользователя, идентификатор группы, дополнительная информация, домашний каталог, имя командного процессора) в виде двоеточия. Символ ***x*** *в поле признака пароля указывает на то, что хэшированный пароль находится в другом файле –* **/etc/shadow**.

5. Аналогично изучите содержимое «теневого» файла паролей **/etc/shadow**. *Он также представляет собой таблицу, каждая строка которой состоит из 9 полей, разделенных двоеточиями (регистрационное имя, хэшированный пароль, контрольные сроки в днях, среди которых:*

- *число дней с 01.01.70 до дня последнего изменения пароля,*
- *минимальное число дней действия пароля со дня его последнего изменения,*
- *максимальное число дней действия пароля,*
- *число дней до устаревания пароля, за которые система начнет выдавать предупреждения,*
- *число дней со времени обязательной смены пароля до блокировки учетной записи,*
- *день блокировки учетной записи).*

Последнее, девятое, поле зарезервировано и не используется.

5. Запустите утилиту **pwck** и проверьте с ее помощью файлы учетных записей **/etc/passwd** и **/etc/shadow** на отсутствие ошибок. Разберитесь в обнаруженных ошибках и, если они представляют угрозу, покажите их преподавателю. Самостоятельное

редактирование парольных файлов, не предусмотренное настоящим заданием, запрещено.

6. С помощью команды **groupadd omega** создайте новую группу без указания ее числового идентификатора. Откройте для просмотра файл групп и найдите в нем созданную запись. Обратите внимание на номер созданной группы и запишите его.

7. С помощью команды **useradd –m john** зарегистрируйте в системе нового пользователя. Аргумент **–m** указывает на необходимость создания домашнего каталога пользователя с его именем. После успешной регистрации, не назначая пользователю пароль, посмотрите содержимое текстовых файлов **/etc/passwd** и **/etc/shadow**. Обратите внимание на заполнение второго поля в созданной учетной записи, которая будет располагаться в конце каждого из файлов. Проверьте наличие и содержимое домашнего каталога пользователя, включая «скрытые» файлы. В какую группу по умолчанию включен зарегистрированный пользователь?

8. Командой **passwd john** присвойте новому пользователю какой-либо простой пароль (например, 12345). Программа напомнит вам о том, что пароль слишком простой, но администратор может с этим мнением не считаться. После завершения процедуры регистрации вновь откройте теневой файл паролей **/etc/shadow**. Что изменилось в учетной записи этого пользователя?

9. С помощью **Alt+F2** перейдите во вторую консоль и зарегистрируйтесь с именем и паролем вновь созданного

пользователя. Чем отличаются символы в приглашениях ввода команд для администратора и обычного пользователя?

10. С правами пользователя **john** создайте в его домашнем каталоге текстовый файл с содержимым, позволяющим его идентифицировать (например, **echo 'my name' john > /home/john/j**). Затем установите права доступа 0750 на каталог **/home/john** и 0640 на созданный текстовый файл.

11. Аналогично предыдущим пунктам создайте учетную запись второго пользователя **useradd –m –g omega braun**. Присвойте ему такой же пароль. Затем посмотрите содержимое теневого файла **/etc/shadow**. Сравните учетные записи созданных пользователей и попытайтесь объяснить, почему при одинаковых паролях их хэшированные функции различаются?

12. С помощью **Alt+F1** перейдите в первую консоль и правами **root** создайте командой **touch /etc/nologin** пустой файл, запрещающий регистрацию в системе новых пользователей. Перейдите в третью консоль (**Alt+F3**) и попытайтесь зарегистрироваться там. Убедитесь в бесполезности таких попыток.

13. Из первой консоли удалите правами **root** созданный файл **/etc/nologin**, переключитесь в третью консоль и повторите попытку входа в систему пользователем **braun**. На этот раз попытка входа должна закончиться удачно.

14. С правами пользователя **braun** создайте в его домашнем каталоге текстовый файл с содержимым, позволяющим его идентифицировать (например, **echo my name braun >**

/home/braun/b). Затем установите права доступа 0750 на каталог **/home/braun** и 0640 на созданный текстовый файл.

15. С правами пользователя **braun** попытайтесь войти в домашний каталог пользователя **john** и прочитать его файл. Сделайте выводы.

16. С помощью **Alt+F2** перейдите во вторую консоль и с правами пользователя **john** попытайтесь войти в домашний каталог пользователя **braun**
и прочитать его файл. Сделайте выводы.

17. Перейдите в первую консоль и с правами администратора командой **usermod –G omega john** включите названного пользователя в дополнительную группу. Откройте для просмотра файл **/etc/group** и зафиксируйте изменения.

18. Правами пользователей **john** и **braun** из соответствующих консолей повторите попытки доступа к чужим каталогам и файлам. Объясните произошедшие изменения.

19. С помощью команд **who** и **w** посмотрите список пользователей, которые сейчас работают в системе. Какую информацию вам удалось из этого извлечь? Чем отличаются результаты, выведенные командами **who** и **w**?

20. Не выходя из консоли администратора, запустите редактор **mcedit** с именем файла учетных записей **/etc/passwd** в качестве аргумента. В учетной записи пользователя **john** вместо символа **x** во втором поле поставьте символ восклицательного знака. Сохраните (F2) изменения в файле и выйдите из редактора.

21. Перейдите (**Alt+F2**) во вторую консоль и командой **exit** завершите сеанс работы пользователя **john**. Попытайтесь вновь зарегистрироваться в системе с этим именем. Почему вам это не удалось?

22. Вернитесь в консоль администратора (**Alt+F1**) и с помощью редактора **mcedit** разблокируйте учетную запись пользователя **john**. Вновь из второй консоли войдите в систему с его именем.

23. Вернитесь в консоль администратора (**Alt+F1**) и попытайтесь удалить учетную запись пользователя **john** командой **userdel –r john** (аргумент **–r** позволяет удалить с учетной записью и домашний каталог пользователя **/home/john**). Почему система не позволяет удалить эту учетную запись?

24. С помощью команды **ps –elf** выведите на экран список процессов, исполняющихся в системе. В последних строках файла найдите процесс командной оболочки, закрепленной за пользователем **john**. Прочитайте во втором столбце числовой идентификатор этого процесса (PID) и «убейте» его командой **kill -9 PID**. Перейдите во вторую консоль и убедитесь в том, что сеанс пользователя **john** завершен. Теперь учетную запись можно удалить (но сейчас это лучше не делать).

25. Попытайтесь присвоить пользователю **braun** нулевой идентификатор (это можно сделать командой **usermod –u 0 braun**). Почему администратору в такой попытке было отказано?

26. Вновь с правами администратора запустите **mcedit** и откройте в нем файл **/etc/passwd**. Найдите учетную запись пользователя **braun** и замените его числовой идентификатор **UID** на **0**. Сохраните изменения в файле (F2) и завершите редактирование.

27. Перейдите в третью консоль и попытайтесь прочитать теневой файл паролей (**cat /etc/shadow**). Почему пользователю в этом было отказано? Командой **exit** завершите сеанс пользователя **braun**, а затем вновь зарегистрируйтесь с этим именем. Почему изменился символ в строке приглашения? Вновь попытайтесь прочитать файл паролей. Почему на этот раз все получилось? Какую информацию о пользователях на этот раз выдает команда **who**?

28. Из третьей консоли запустите редактор и верните в исходное состояние учетную запись пользователя **braun**. Сделайте выводы о роли учетных записей пользователей.

29. Из консоли администратора просмотрите текстовые файлы в каталоге **/var/log** и найдите записи аудита, в которых зафиксированы входы в систему администратора и пользователей. Имеется ли доступ к файлам аудита у обычных пользователей?

30. Вам необходимо создать учетные записи и определить права доступа для десяти (10) сотрудников: **w_gromov, n_kalinina, e_ivanova, r_klinova, b_rebrov, k_beglov, i_frolov, d_lavrov, m_kruglov, t_uporov**, работающих в одном подразделении и занятых созданием и редактированием текстовых документов различного уровня конфиденциальности. Разграничение доступа к информации должно быть произведено на основании следующих требований:

- допуск к секретным сведениям имеют четыре пользователя: **w_gromov, n_kalinina, b_rebrov, k_beglov;**
- три пользователя: **n_kalinina, b_rebrov, k_beglov** работают над созданием секретных документов, каждый по своему профилю. Их домашние каталоги и файлы должны быть полностью недоступными как друг для друга, так и для всех остальных, исключая **w_gromov;**
- три пользователя: **i_frolov, d_lavrov, e_ivanova** имеют допуск к конфиденциальной информации и работают над документами с соответствующим грифом. Они имеют право читать файлы с конфиденциальной информацией, созданные своими коллегами, без права их модификации;
- все секретоносители имеют право знакомиться с конфиденциальными файлами;
- три пользователя: **r_klinova, m_kruglov, t_uporov** могут работать только с открытой информацией. Их файлы должны быть доступны для чтения каждому сотруднику подразделения без права модификации;
- **w_gromov** является редактором подразделения и имеет право читать и копировать файлы всех сотрудников и всех уровней конфиденциальности. Завершенные документы копируются пользователем **w_gromov** в его домашний каталог, который должен быть недоступен для всех остальных сотрудников подразделения;

- всем сотрудникам, включая редактора, запрещается вносить изменения и удалять документы других пользователей, независимо от уровня конфиденциальности.

31. Укажите в отчете, какие коллизии вы усматриваете в сформулированных требованиях? Как реализовать указанные требования таким образом, чтобы пользователи не могли по своему усмотрению изменять установленный порядок?

32. С помощью команды **groupadd** создайте четыре пользовательских группы: **alfa, beta, nabla, sigma.** Формат команды **groupadd -g GID group_name.** Идентификатор группы **GID** можно назначать произвольно, начиная с номера 100 (например**, groupadd – g 101 alfa).**

33. Создайте учетные записи для вышеуказанных десяти новых пользователей. Регистрационные данные (кроме паролей и групп) сведены в табл. 2. Пароли назначайте произвольно, длиной не менее 8 символов, не забывая фиксировать их в черновике отчета. Для пользователей **e_ivanova, r_klinova** задайте одинаковые пароли. Распределите сотрудников по группам таким образом, чтобы удовлетворить вышеперечисленным требованиям. Изобразите в отчете наглядную схему, поясняющую разграничение доступа сотрудников подразделения к компьютерной информации. Заполните требуемыми правами доступа ячейки табл. 3.

Таблица 2- Регистрационные данные

Пользователь	**UID**	**Пароль**	**Группа**	**Домашний каталог**	**Дата удаления учетной записи**
i_frolov	2001			/home/i_frolov	T+ 10 дней
m_kruglov	2002			/home/m_kruglov	T+ 30 дней
b_rebrov	2003			/home/b_rebrov	T+ 12 дней
d_lavrov	2004			/home/d_lavrov	T+ 60 дней
e_ivanova	2005			/home/e_ivanova	T+ 30 дней
t_uporov	2006			/home/t_uporov	T+ 15 дней
k_beglov	2007			/home/k_beglov	T+ 45 дней
n_kalinina	2008			/home/n_kalinina	T+ 30 дней
r_klinova	2009			/home/r_klinova	T+ 90 дней
w_gromov	2010			/home/w_gromov	не удалять

Таблица 3 – Таблица для заполнения

Пользователь	**Права доступа к объектам ФС**					
	Файл редактора	**Файлы «С»**			**Файлы «К»**	**Файлы «Н»**
		С1	**С2**	**С3**		
i_frolov						
m_kruglov						
b_rebrov						
d_lavrov						
e_ivanova						
t_uporov						
k_beglov						
n_kalinina						
r_klinova						
w_gromov						

34. Пять первых пользователей (**w_gromov, n_kalinina, e_ivanova, r_klinova, b_rebrov)** зарегистрируйте с помощью команды **useradd.** Например, **useradd –u 501 –g sigma –d /home/n_kalinina –p v5g7K2S4 –e 2010-01-07 n_kalinina**. Параметр **-m** обеспечивает создание домашнего каталога пользователя, если он еще не существует. Прочие параметры команды можно не указывать. Идентификаторы пользователей **UID** назначать, начиная с 2001. Дату удаления учетной записи пользователя вводить в формате ГГГГ-ММ-ДД.

35. Пять последних пользователей зарегистрируйте с помощью командного файла **adduser**, которая запрашивает значения в интерактивном режиме. При вводе данных ориентируйтесь на подсказки системы [в квадратных скобках]. Все параметры, кроме имени пользователя, его идентификатора, имени группы, пароля и домашнего каталога, можно игнорировать. Для ввода параметра по умолчанию вводить **Enter**. В некоторых дистрибутивах ОС Linux командный файл **adduser** отсутствует, и в этом случае регистрацию остальных пользователей следует произвести аналогично предыдущему пункту. При использовании **adduser** символ подчеркивания в имени пользователя может не восприниматься. Если это так, замените этот символ в именах пользователей на символ дефиса.

36. Зарегистрировавшись администратором во вспомогательной консоли, отслеживайте из нее изменения,

происходящие в файлах **/etc/passwd** и **/etc/shadow** по мере создания новых учетных записей.

37. Обратите внимание на то, что утилита **useradd** записывает пароли в файл **/etc/shadow** в открытом виде. Поскольку система воспринимает эту запись в качестве хэш-функции пароля, у пользователя с подобной учетной записью нет никаких шансов войти в систему. Правами администратора установите пользователям требуемые пароли с помощью команды **passwd.**

38. Регистрируясь в системе от имени пользователей **w_gromov**, **b_rebrov**, **d_lavrov** и **m_kruglov**, создайте их правами и в их домашних каталогах по одному текстовому файлу. Путем пробного доступа к этим файлам на чтение и запись от имени иных пользователей проверьте, удалось ли вам реализовать требуемую политику безопасности.

39. Правами администратора с помощью команды **usermod** по своему усмотрению измените основную группу пользователю **d_lavrov**. Проверьте, как изменились его права доступа к файлам иных пользователей.

40. Из первой консоли с помощью команды **su** измените права администратора на права пользователя **w_gromov**. Почему система не запрашивает пароль? С помощью команды **exit** верните себе права администратора. Был ли запрошен пароль? Почему?

41. Пользователь **d_lavrov** уволен за дисциплинарный проступок. С помощью команды **userdel d_lavrov** удалите его

учетную запись. Кто теперь стал владельцем его домашнего каталога?

42. Зарегистрируйте вместо уволенного пользователя нового сотрудника **f_mironov** с предоставлением ему аналогичных прав (пароль должен быть новым!). Приобрел ли новый пользователь права на каталог ранее удаленного сотрудника? Для того чтобы подобное не происходило, при удалении учетных записей администратору необходимо вначале скопировать в недоступную для других директорию файлы пользователя, представляющие ценность для организации, а затем удалить учетную запись пользователя вместе с каталогом.

43. Пользователь **r_klinova** убыла в командировку сроком на две недели.

Заблокируйте ее учетную запись любым из известных вам способов. Попытайтесь зарегистрироваться во второй консоли с правами **r_klinova** и убедитесь в том, что для этого пользователя система недоступна.

44. Зарегистрируйтесь во второй консоли с правами пользователя **k_beglov,** вызовите команду **passwd** и измените свой пароль. В качестве нового пароля введите **qwerty**.

45. Перейдите в консоль администратора и назначьте пользователю **k_beglov** новый пароль **zxcvbnm.** Затем с помощью команды **chage** (change aging – изменить информацию об устаревании) установите для этого пользователя минимальное время

действия паролей, равное 5 дням. С какой целью устанавливается минимальный срок действия пароля?

46. Вспомните теоретический материал, связанный с файлом **/etc/sudoers.** Отредактируйте его таким образом, чтобы предоставить следующим пользователям дополнительные права за счет использования команды **sudo**:

- пользователю **e_ivanova** – право монтировать файловые системы типа **iso9660** на оптических дисках на своем компьютере,
- пользователю **b_rebrov** – право изменения владельца файлов на всех компьютерах локальной сети,
- пользователю **f_mironov** – право изменения учетных записей пользователей на своем компьютере без обязательного ввода пароля.

47. Из второй консоли с правами пользователя **f_mironov** создайте файл **cal 2011 > /home/f_mironov/cal2011**. С помощью команды **su** переключите консоль на пользователя **b_rebrov** и с помощью временно предоставленных ему привилегий передайте права на созданный **f_mironov** файл другому владельцу **n_kalinina.** Каким еще путем можно предоставить подобные права пользователям, не передавая им «опасных» полномочий администратора?

48. Просмотрите с правами администратора системные журналы в каталоге **/var/log** и убедитесь, что система зафиксировала факты присвоения полномочий администратора.

Временная нейтрализация парольной защиты

49. Отработайте вариант временной нейтрализации пароля администратора (например, для случая его утраты). Получите у преподавателя загрузочный оптический диск с ядром и минимальным набором утилит ОС Linux. Загрузите компьютер со сменного носителя. При необходимости измените порядок загрузки с использованием настроек в Setup BIOS. По завершении загрузки вы должны увидеть символ # и приглашение для ввода команды.

50. Введите команду **fdisk –lu** для отображения информации о разделах фиксированных и пристыкованных машинных носителях и установленных на них файловых системах. Найдите название файла блочного устройства, на котором установлен корневой раздел Linux (например, **/dev/sda6**).

51. Примонтируйте файловую систему Linux (предположительно это ФС **ext2fs** или **ext3fs**) на разделе HDD с помощью команды **mount – t ext2 /dev/hda6 /mnt**.

52. В случае успешного монтирования откройте файл учетных записей в смонтированной системе с помощью команды **vi /mnt/etc/passwd**. Текстовый редактор **vi** отобразит требуемый файл с мигающим курсором под первым символом учетной записи **root**. С

помощью клавиш управления курсором переместите его под первый символ справа от двоеточия после слова **root**. Затем с помощью клавиши **x** требуется удалить все символы между первым и вторым двоеточием. В результате начало первой строки редактируемого файла должно выглядеть так: **root::0:0:**

53. Переключитесь в режим ввода команд редактора с помощью клавиши с двоеточием. После того как двоеточие и мигающий курсор после него появятся в последней строке, введите команду на сохранение изменений и выход из редактора **wq <Enter>**. Если вы ошиблись и удалили лишние символы, проще перейти в режим команд и выйти из редактора без сохранения изменений с помощью **q! <Enter>** (затем следует повторить попытку редактирования).

54. При наличии в операционной системе встроенного редактора **Midnight Commander** процесс модификации учетной записи можно сделать более удобным. Файл открывается командой **mcedit /etc/passwd**, а результаты сохраняются функциональной клавишей F2.

55. Введите команду **reboot** для перезагрузки компьютера и извлеките компакт-диск. После загрузки Linux с жесткого диска на

запрос об авторизации введите имя **root** и система зарегистрирует вас своим администратором без пароля. После завершения доступа требуется либо сменить пароль администратора с помощью команды **passwd,** либо восстановить удаленный признак пароля (по умолчанию это символ **x** между первым и вторым двоеточием в учетной записи **root** файла **/etc/passwd**). Редактирование файла паролей можно произвести встроенным редактором (F4) файлового менеджера **Midnight Commander**. Можно не использовать целиком файловый менеджер, ограничившись запуском его редактора **mcedit /etc/passwd**. Сохраните изменения (F2) и закройте программу.

56. Найдите в каталоге **/var/log** файл аудита, в котором зафиксирован вход в систему администратора без пароля.

Контрольные вопросы

1. Достаточно ли трех базовых прав доступа к файлам для реализации в ОС Linux требуемой политики безопасности?
2. Какие изъяны вы усматриваете в использованных утилитах регистрации учетных записей пользователей?
3. Может ли пользователь закрыть для себя доступ к собственному файлу? Каким образом? Почему система не соотносит владельца файла ни с его группой, ни со всеми остальными?
4. Существуют ли способы ограничения доступа суперпользователя к некоторым конфиденциальным файлам?
5. Какие дополнительные права администратор может предоставить пользователям с помощью утилиты **sudo** и регистрационного файла **/etc/sudoers**?

Библиографический список

1. Техническая электронная документация по операционной системе Linux.

2. Береснев А.Л. Администрирование GNU/Linux с нуля./А.Л. Береснев –СПб.: БВХ-Петербург, 2010 – 576 с.

3. Блум, Ричард, Бреснахэн, Кристина. Командная строка Linux и сценарии оболочки. Библия пользователя/ Ричард Блум, Кристина Бреснахэн -М. : ООО “И.Д. Вильямс”, 2012. — 784 с.

4. В.В. Бакланов Защитные механизмы операционной системы Linux: учебное пособие / В.В. Бакланов. под ред. Н.А. Гайдамакина. Екатеринбург: УрФУ, 2011. 354 с.