Отчет по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Лебедев Ярослав Борисович

Содержание

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux [1].

Выполнение лабораторной работы

Работу выполял с помощью VirtualBox.

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (использую учётную запись администратора): useradd guest (Рис.1)

2. Задайте пароль для пользователя guest (использую учётную запись администратора): passwd guest (Рис.1)

3. Войдите в систему от имени пользователя guest (Рис.1).

4. Определите директорию, в которой вы находитесь, командой pwd. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию (Рис.1).

5. Уточните имя вашего пользователя командой whoami (Рис.1).

6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gidи др. запомните. Сравните вывод idc выводом команды groups (Рис.1).

```
[yblebedev@yblebedev ~]$ su
Пароль:
[root@yblebedev yblebedev]# useradd guest
[root@yblebedev yblebedev]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@yblebedev yblebedev]# su guest
[guest@yblebedev yblebedev]$ pwd
/home/yblebedev
[guest@yblebedev yblebedev]$ cd ~
[guest@yblebedev ~]$ whoami
guest
[guest@yblebedev ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0
:c0.c1023
[guest@yblebedev ~]$ groups
guest
```

Рис.1. Пункты 1-6

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Данные guest и дамашней дирректории различаются.

8. Просмотрите файл /etc/passwd командой cat /etc/passwd. Найдите в нём свою учётную запись. Определите uid пользователя. Определите gid пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу shift, нажимайте page up и page down) либо программу grep в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: cat /etc/passwd | grep guest (Рис.2).

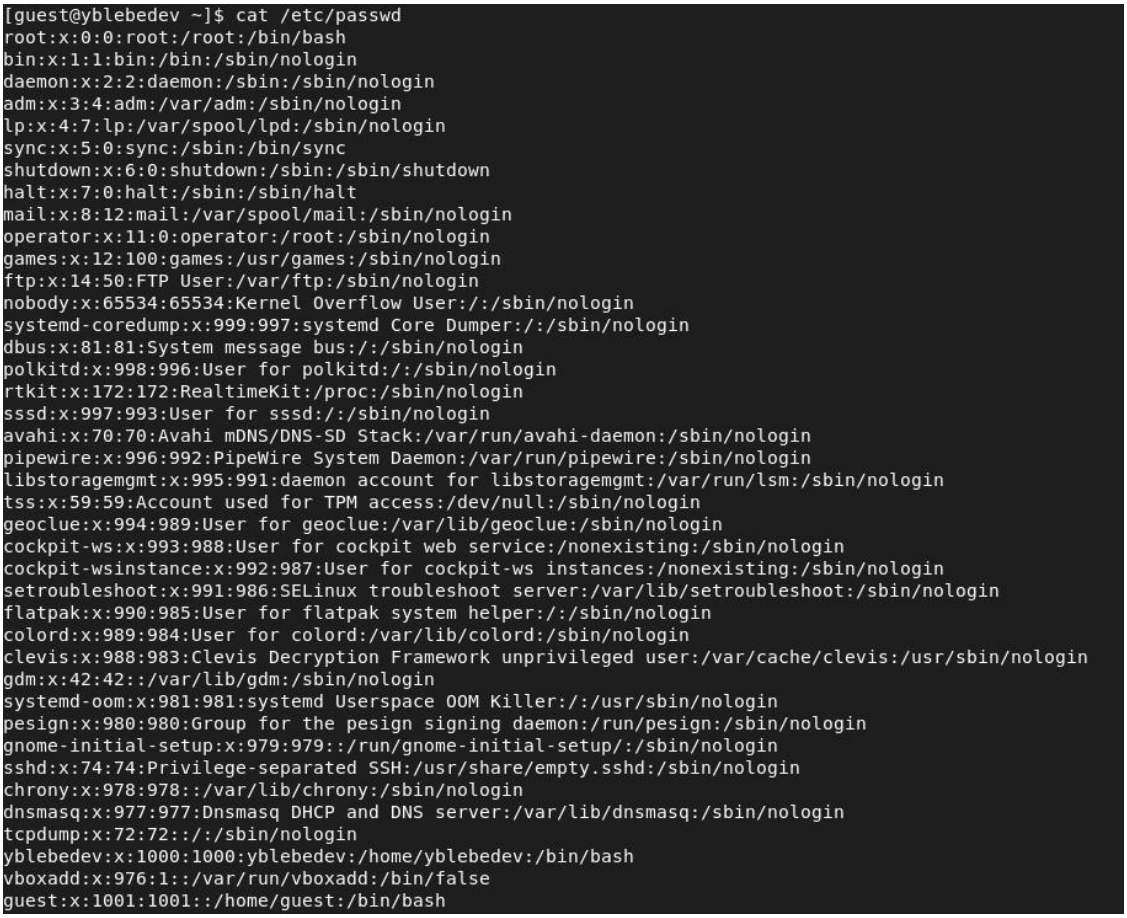

Рис.2. Пункт 8

9. Определите существующие в системе директории командой ls -l /home/ Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях? Удалось, установлены полные права для пользователя (Рис.3).

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой (Рис.3): lsattr /home Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? Удалось, но для других пользователей у меня нет доступа к просмотру.

11. Создайте в домашней директории поддиректорию dir1 командой mkdir dir1 Определите командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (Рис.3).

12. Снимите с директории dir1 все атрибуты (Рис.3) командой chmod 000 dir1 и проверьте с её помощью правильность выполнения команды ls -l

13. Попытайтесь создать в директории dir1 файл file1 командой (Рис.3) echo “test” > /home/guest/dir1/file1 Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на

создании файла? Проверьте командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1.

Получен отказ, так как мы сняли все права доступа на дирректорию.

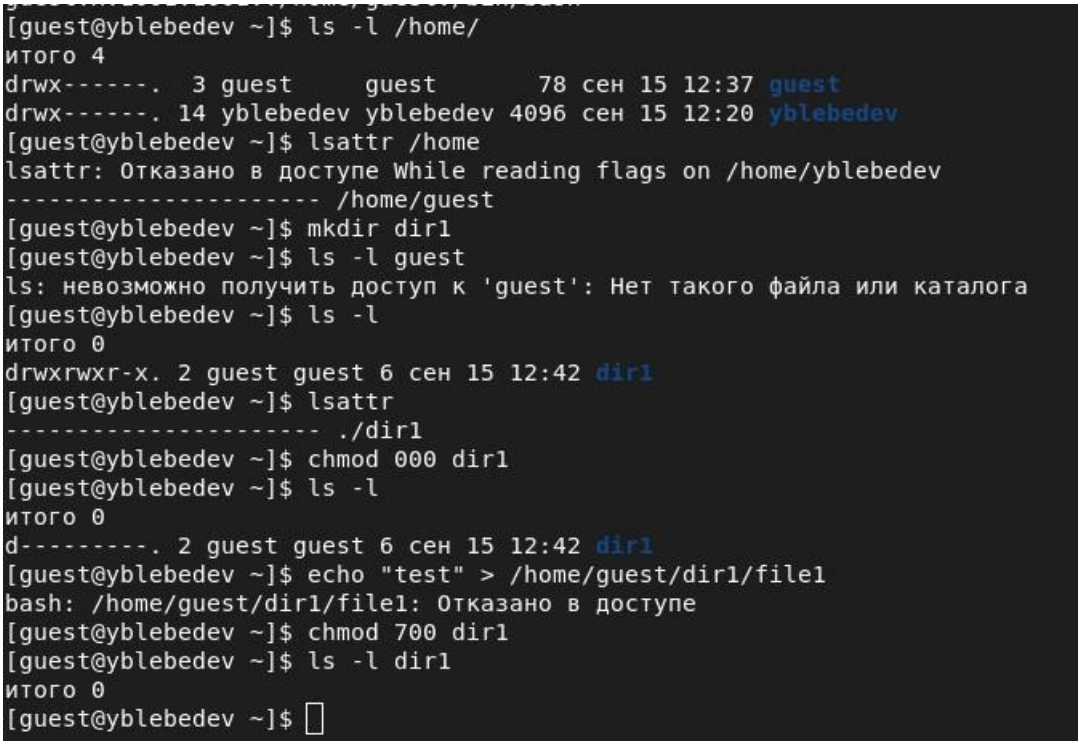

Рис.3. Пункты 9-13

14. Заполните таблицу «Установленные права и разрешённые действия» (Рис. 4-6), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибуты файлов и директорий, а лишь «первые три»: r, w, x, для «владельца». Остальные атрибуты также важны (особенно при использовании доступа от имени разных пользователей, входящих в те или иные группы). Проверка всех атрибутов при всех условиях значительно увеличила бы таблицу: так 9 атрибутов на директорию и 9 атрибутов на файл дают 218 строк без учёта дополнительных атрибутов, плюс таблица была бы расширена по количеству столбцов, так как все приведённые операции необходимо было бы повторить ещё как минимум для двух пользователей: входящего в группу владельца файла и не входящего в неё. После полного заполнения табл. 2.1 и анализа полученных данных нам удалось бы выяснить, что заполнение её в таком виде излишне. Можно разделить большую таблицу на несколько малых независимых таблиц. В данном примере предлагается рассмотреть 3+3атрибута, т.е. 26 = 64 варианта. Замечание 2: в ряде действий при выполнении команды удаления файла вы можете столкнуться с вопросом: «удалить защищённый от записи пустой обычный файл dir1/file1?» Обратите внимание, что наличие этого вопроса не позволяет сделать правильный вывод о том, что файл можно удалить. В ряде случаев, при ответе

«у» (да) на указанный вопрос, возможно получить другое сообщение: «невозможно удалить dirl /file1: Отказано в доступе».

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d---	---	-	-	-	-	-	-	-	-
d---	--x	-	-	-	-	-	-	-	-
d---	-w-	-	-	-	-	-	-	-	-
d---	-wx	-	-	-	-	-	-	-	-
d---	r--	-	-	-	-	-	-	-	-
d---	r-x	-	-	-	-	-	-	-	-
d---	rw-	-	-	-	-	-	-	-	-
d---	rwx	-	-	-	-	-	-	-	-
d--x	---	-	-	-	-	+	-	-	+
d--x	--x	-	-	-	-	+	-	-	+
d--x	-w-	-	-	+	-	+	-	-	+
d--x	-wx	-	-	+	-	+	-	-	+
d--x	r--	-	-	-	+	+	-	-	+
d--x	r-x	-	-	-	+	+	-	-	+
d--x	rw-	-	-	+	+	+	-	-	+
d--x	rwx	-	-	+	+	+	-	-	+
d-w-	---	-	-	-	-	-	-	-	-
d-w-	--x	-	-	-	-	-	-	-	-
d-w-	-w-	-	-	-	-	-	-	-	-
d-w-	-wx	-	-	-	-	-	-	-	-
d-w-	r--	-	-	-	-	-	-	-	-
d-w-	r-x	-	-	-	-	-	-	-	-
d-w-	rw-	-	-	-	-	-	-	-	-
d-w-	rwx	-	-	-	-	-	-	-	-

Рис.4. Таблица 2.1 «Установленные права и разрешённые действия»

d-wx	---	+	+	-	-	+	-	+	+
d-wx	--x	+	+	-	-	+	-	+	+
d-wx	-w-	+	+	+	-	+	-	+	+
d-wx	-wx	+	+	+	-	+	-	+	+
d-wx	r--	+	+	-	+	+	-	+	+
d-wx	r-x	+	+	-	+	+	-	+	+
d-wx	rw-	+	+	+	+	+	-	+	+
d-wx	rwx	+	+	+	+	+	-	+	+
dr--	---	-	-	-	-	-	+	-	-
dr--	--x	-	-	-	-	-	+	-	-
dr--	-w-	-	-	-	-	-	+	-	-
dr--	-wx	-	-	-	-	-	+	-	-
dr--	r--	-	-	-	-	-	+	-	-
dr--	r-x	-	-	-	-	-	+	-	-
dr--	rw-	-	-	-	-	-	+	-	-
dr--	rwx	-	-	-	-	-	+	-	-
dr-x	---	-	-	-	-	+	+	-	+
dr-x	--x	-	-	-	-	+	+	-	+
dr-x	-w-	-	-	+	-	+	+	-	+
dr-x	-wx	-	-	+	-	+	+	-	+
dr-x	r--	-	-	-	+	+	+	-	+
dr-x	r-x	-	-	-	+	+	+	-	+
dr-x	rw-	-	-	+	+	+	+	-	+
dr-x	rwx	-	-	+	+	+	+	-	+

Рис.5. Таблица 2.1 «Установленные права и разрешённые действия»

drw-	---	-	-	-	-	-	+	-	-
drw-	--x	-	-	-	-	-	+	-	-
drw-	-w-	-	-	-	-	-	+	-	-
drw-	-wx	-	-	-	-	-	+	-	-
drw-	r--	-	-	-	-	-	+	-	-
drw-	r-x	-	-	-	-	-	+	-	-
drw-	rw-	-	-	-	-	-	+	-	-
drw-	rwx	-	-	-	-	-	+	-	-
drwx	---	+	+	-	-	+	+	+	+
drwx	--x	+	+	-	-	+	+	+	+
drwx	-w-	+	+	+	-	+	+	+	+
drwx	-wx	+	+	+	-	+	+	+	+
drwx	r--	+	+	-	+	+	+	+	+
drwx	r-x	+	+	-	+	+	+	+	+
drwx	rw-	+	+	+	+	+	+	+	+
drwx	rwx	+	+	+	+	+	+	+	+

Рис.6. Таблица 2.1 «Установленные права и разрешённые действия»

15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2 (Рис. 7).

Операция	Минимальные права на дирректорию	Минимальные права на файл
Создание файла	d-wx	---
Удаление файла	d-wx	---
Чтение файла	d--x	r--
Запись в файл	d--x	-w-
Переименование файла	d-wx	---
Создание поддиректории	d-wx	---
Удаление поддиректории	d-wx	---

Рис.7. Таблица 2.2 «Минимальные права для совершения операций»

Выводы

Получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Методические материалы курса