Информационная безопасность. Отчет по лабораторной работе № 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Горбунова Ярослава Михайловна

Содержание

# 1 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].

# 2 Выполнение лабораторной работы

Постарайтесь последовательно выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт [2].

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

Figure 1: Создание учётной записи пользователя guest

Figure 1: Создание учётной записи пользователя guest

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

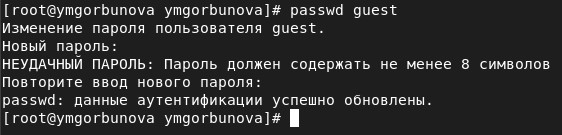


Figure 2: Задание пароля для пользователя guest

1. Войдите в систему от имени пользователя guest (fig. 3).
2. 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 (fig. 3). –Дирректория, в которой мы находимся совпадает с приглашением командной строки, но не является домашней дирректорией, поэтому переходим в домашний каталог.

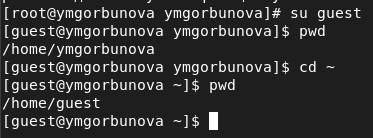


Figure 3: Вход в систему от имени пользователя guest. Определение текущей дирректории. Переход в домашний каталог

1. Уточните имя вашего пользователя командой whoami (fig. 4).
2. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gidи др. запомните. Сравните вывод idс выводом команды groups (fig. 4). – Вывод команды id дает больше информации о пользователе, в то время как команда groups дает информацию только о группах.

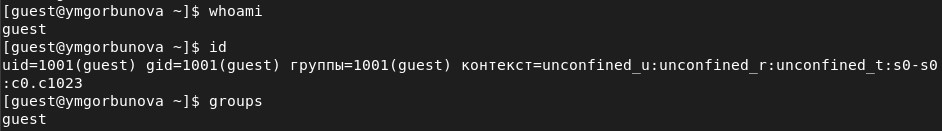


Figure 4: Имя, группа пользователя, группы, куда входит пользователь (команды id, groups)

1. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. – В приглашении командной строки фигурирует то же имя пользователя, которое получено при просмотре вывода команды id.
2. 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 (fig. 5). – Найденные значения полностью совпадают с полученными на предыдущих шагах.

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

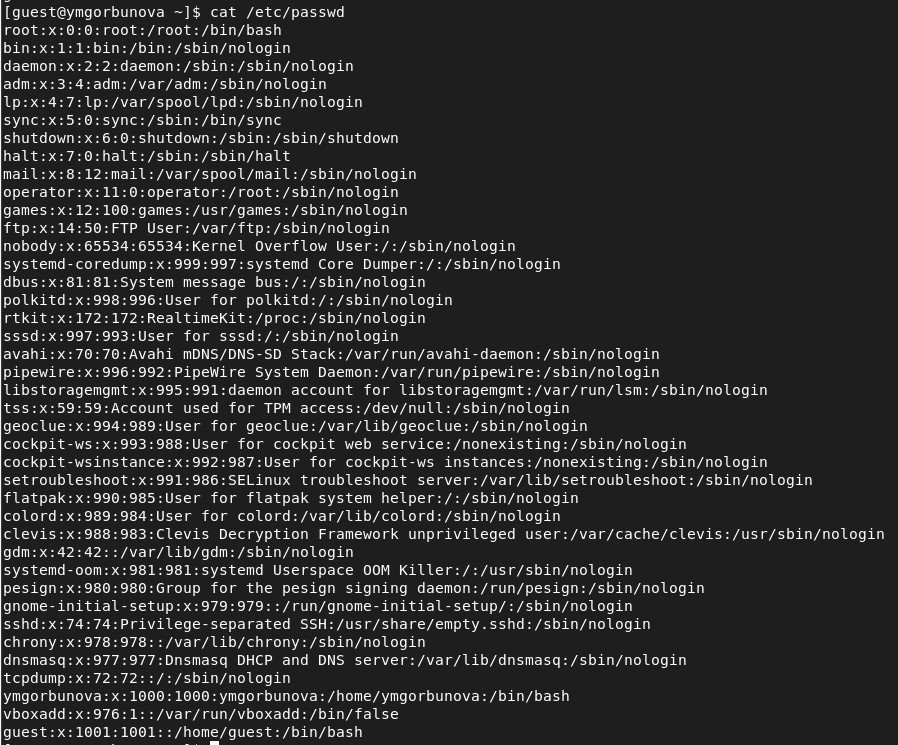


Figure 5: Просмотр файла /etc/passwd

1. Определите существующие в системе директории командой (fig. 6)

ls -l /home/

Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях? – Удалось получить список поддиректорий. На обеих установлены полные права для пользователя, не установлены права для остальных пользователей.

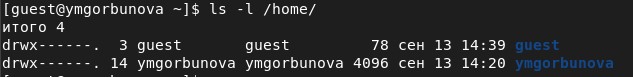


Figure 6: Существующие в системе поддиректорий директории /home/

1. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home (fig. 7), командой:

lsattr /home

Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? – Есть возможность увидеть расширенные атрибуты директории guest, но не удается увидеть расширенные атрибуты директорий других пользователей.

Figure 7: Существующие в системе поддиректорий директории /home/

Figure 7: Существующие в системе поддиректорий директории /home/

1. 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 (fig. 8). – На дирректорию были выставлены полные права доступа для пользователя и членов группы и права на чтение, исполнение для остальных пользователей. Никакие расширенные атрибуты не были выставлены.

1. Снимите с директории dir1 все атрибуты командой

chmod 000 dir1

и проверьте с её помощью правильность выполнения команды (fig. 8)

ls -l

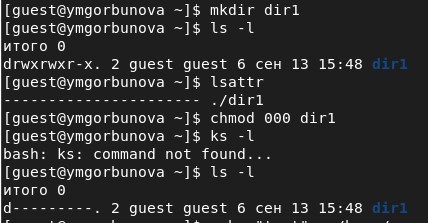


Figure 8: Права доступа и расширенные атрибуты для dir1. Снятие всех атрибутов с дирректории dir1

1. Попытайтесь создать в директории dir1 файл file1 командой

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? – Отказ получен в силу того, что всем пользователям, даже обладателя, ограничены действия по чтению, записи, исполнению с дирректорией. Файл действительно не был создан.

Проверьте командой

ls -l /home/guest/dir1

действительно ли файл file1 не находится внутри директории dir1 (fig. 9).

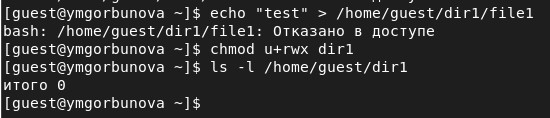


Figure 9: Попытка создания в директории dir1 файла file1. Проверка

1. Заполните таблицу 2.1 «Установленные права и разрешённые действия», 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 «-» (fig. 10 - fig. 12).

Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибуты файлов и директорий, а лишь «первые три»: г, w, х, 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 «y» (да) на указанный вопрос, возможно получить другое сообщение: «невозможно удалить dirl /file1: Отказано в доступе».

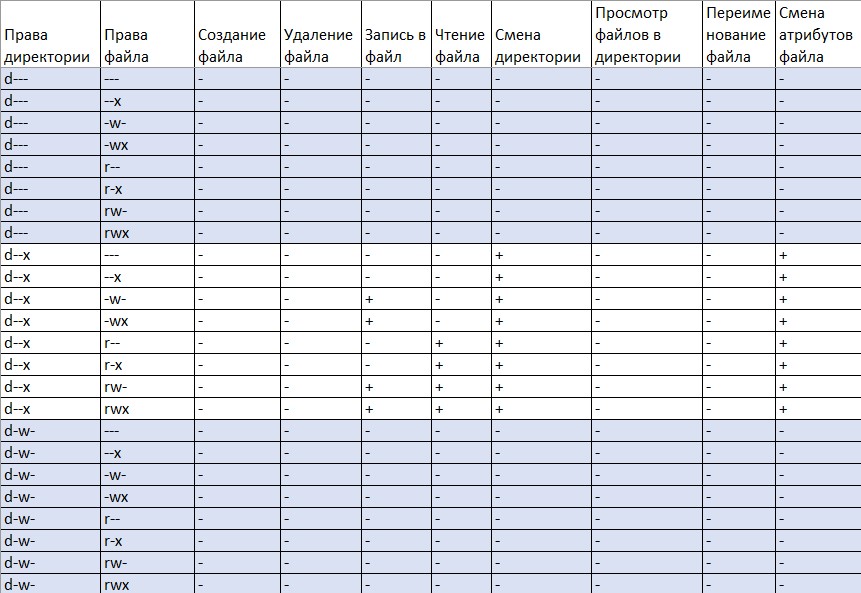


Figure 10: Таблица 2.1. Установленные права и разрешённые действия (часть 1)

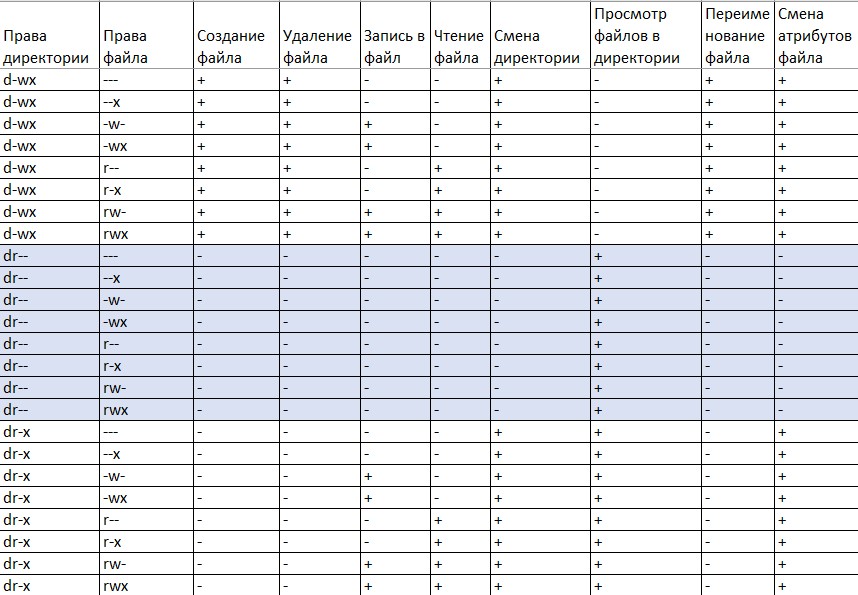


Figure 11: Таблица 2.1. Установленные права и разрешённые действия (часть 2)



Figure 12: Таблица 2.1. Установленные права и разрешённые действия (часть 3)

1. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2 (fig. 13).

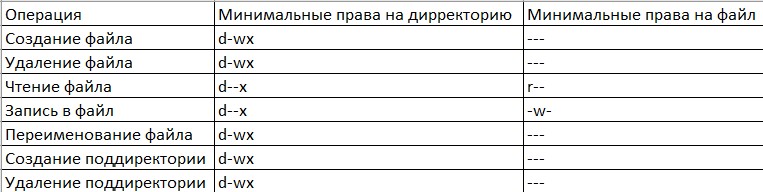


Figure 13: Таблица 2.2. Минимальные права для совершения операций

# 3 Выводы

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

# 4 Список литературы

1. Задание к лабораторной работе № 2
2. Методические материалы курса