Лабораторная работа №2

Основы информационной безопасности

Волгин Иван Алексеевич

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 Linux1

# 2 Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (использую учётную запись администратора): useradd guest
2. Задайте пароль для пользователя guest (использую учётную запись администратора):passwd guest
3. Войдите в систему от имени пользователя guest.
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.
5. Уточните имя вашего пользователя командой whoami.
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. запомните. Сравните вывод id с выводом команды groups.
7. 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
8. Определите существующие в системе директории командой ls -l /home/ Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?
9. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий другихпользователей?
10. 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.
11. Снимите с директории dir1 все атрибуты командой chmod 000 dir1 и проверьте с её помощью правильность выполнения команды ls -l
12. 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? Проверьте командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1
13. Заполните таблицу «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 «-». 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 + 3 атрибута, 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».
14. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1.

# 3 Выполнение лабораторной работы

1. Создаю учетную запись пользователя guest (рис. 1).

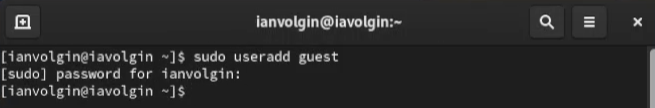


Рис. 1: создание пользователя guest

1. Далее задаю пароль для пользователя guest (рис. 2).

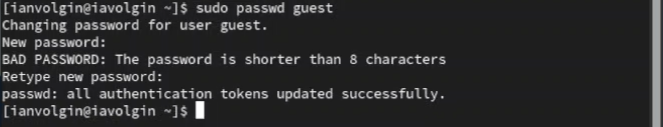


Рис. 2: создание пароля для пользователя guest

1. Затем вхожу в систему под пользователем guest (рис. 3).

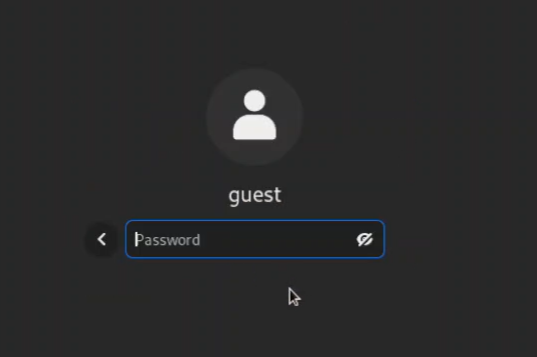


Рис. 3: вход в систему под новым пользователем

1. После этого нужно было проверить в какой директории я нахожусь с помощью команды pwd (рис. 4).

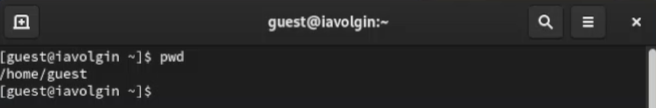


Рис. 4: проверка текущей директории

1. Далее уточняю имя пользователя, используя команду whoami (рис. 5).

Рис. 5: имя пользователя

Рис. 5: имя пользователя

1. Затем с помощью команды id eточняю имя моего пользователя, его группу, а также группы, куда он входит (рис. 6) и сравниваю с выводом команды groups (рис. 7). Команда groups выводит только имя пользователя в то время, как команда id дает более расширенную информацию о нем.

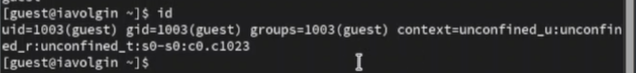


Рис. 6: информация команды id

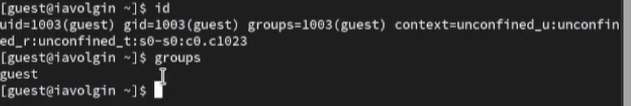


Рис. 7: информация команды groups

1. Далее нужно было просмотреть файл /etc/passwd командой cat /etc/passwd (рис. 8) и найти там информацию о моей учетной записи, я сделал это с помощью команды cat /etc/passwd | grep guest (рис. 9). uid и gid пользователя совпадают с теми, что я получил в прошлых пунктах.

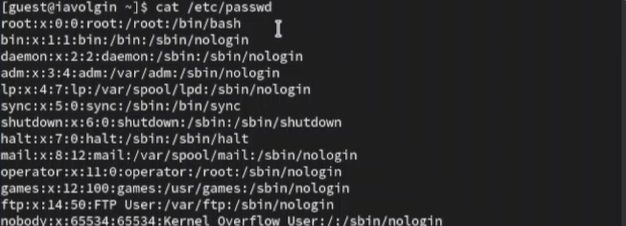


Рис. 8: просмотр файла /etc/passwd

Рис. 9: информация о пользователе

Рис. 9: информация о пользователе

1. После этого нужно было определить существующие в системе директории командой ls -l /home/ (рис. 10)

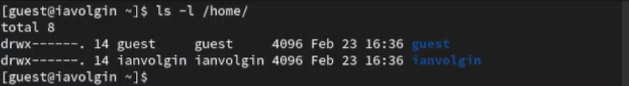


Рис. 10: существующие в системе директории

1. Затем я проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home (рис. 11).

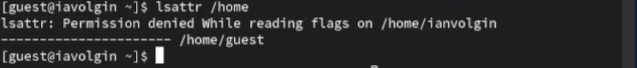


Рис. 11: расширенные атрибуты установлены поддиректорий

1. Далее я создаю домашней директории поддиректорию dir1 командой mkdir dir1 (рис. 12) и определяю командами ls -l (рис. 13) и lsattr (рис. 14), какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

Рис. 12: создание директории dir1

Рис. 12: создание директории dir1

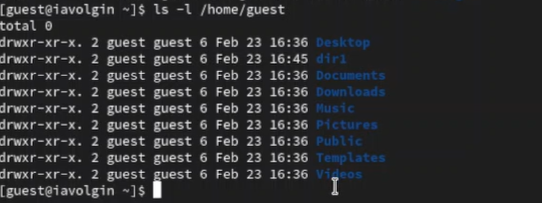


Рис. 13: права доступа директории dir1

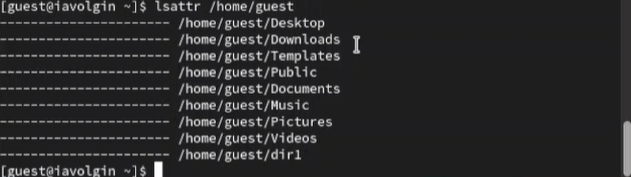


Рис. 14: разрешенные атрибудты директории dir1

1. Затем я снимаю с директории dir1 все атрибуты командой chmod 000 dir1 и проверяю с её помощью правильность выполнения команды ls -l (рис. 15)

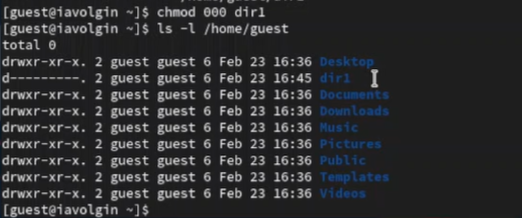


Рис. 15: снятие прав доступа с dir1

1. После этого я пытаюсь создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 (должно быть отказано в доступе) (рис. 16) и проверяю командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1 (тоже отказано в доступе) (рис. 17)

Рис. 16: попытка создания файла file1

Рис. 16: попытка создания файла file1

Рис. 17: проверка его нахождения в dir1

Рис. 17: проверка его нахождения в dir1

1. Заполняю таблицу «Установленные права и разрешённые действия» (рис. 18) (рис. 19) (рис. 20) (рис. 21)

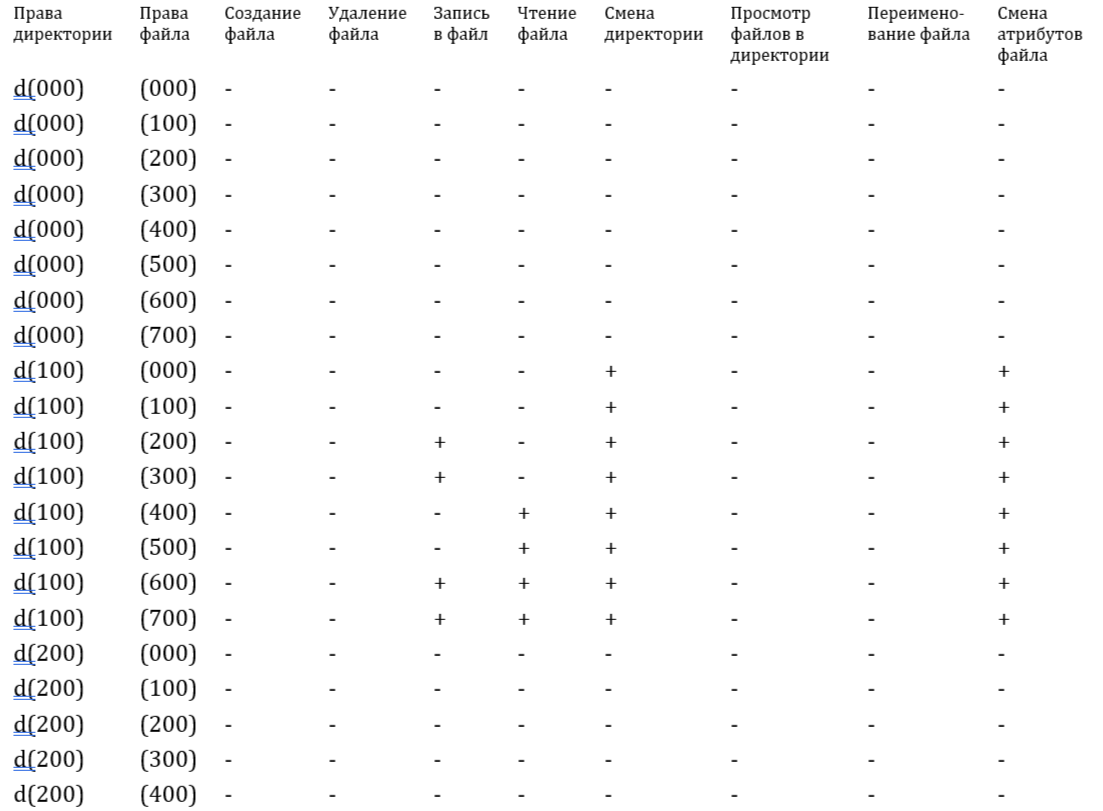


Рис. 18: Таблицу «Установленные права и разрешённые действия» ч.1

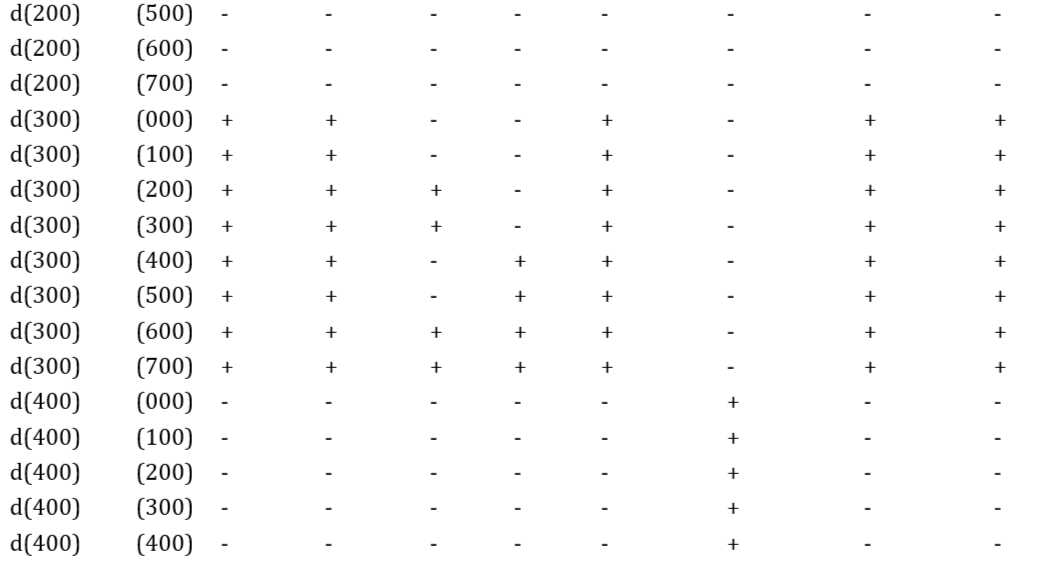


Рис. 19: Таблицу «Установленные права и разрешённые действия» ч.2

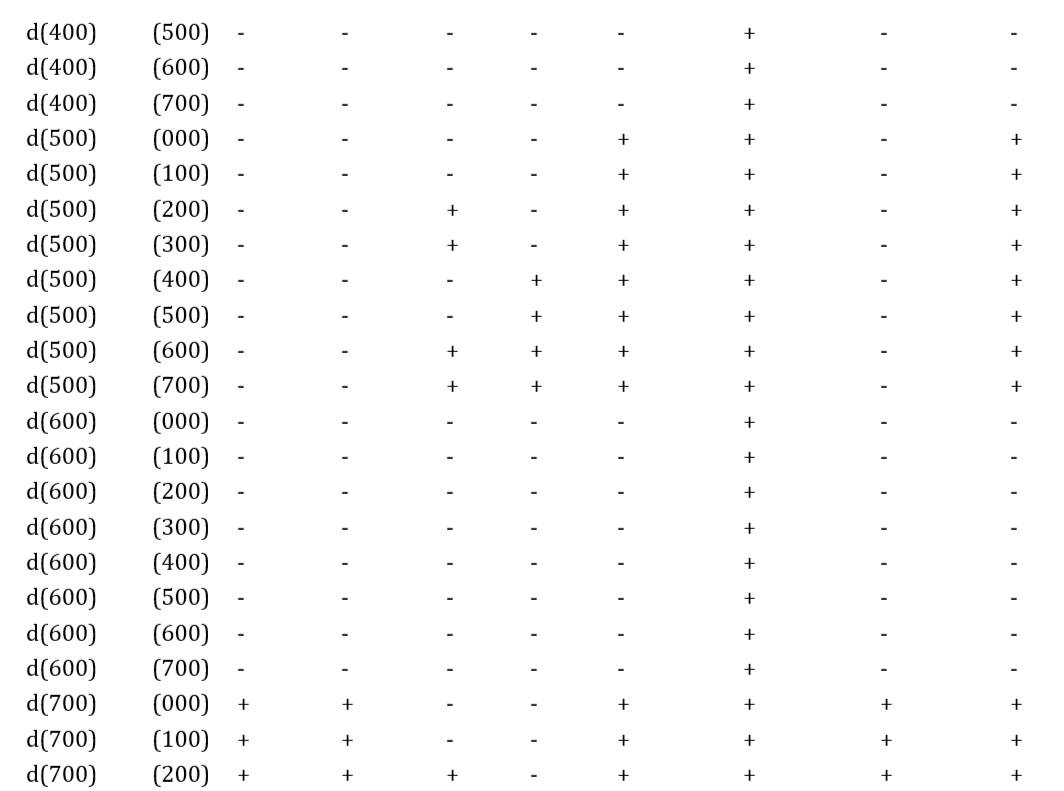


Рис. 20: Таблицу «Установленные права и разрешённые действия» ч.3

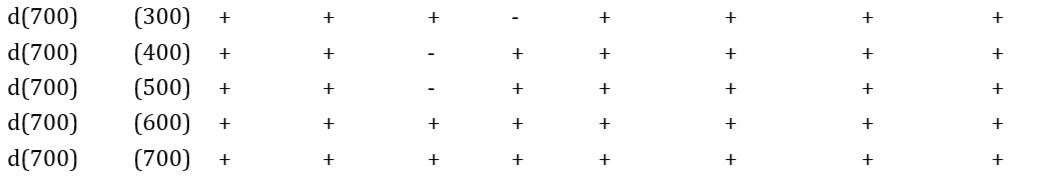


Рис. 21: Таблицу «Установленные права и разрешённые действия» ч.4

1. Затем на основании заполненной таблицы определяю те или иные минимально необходимые права для выполнения операций внутри директории dir1 (рис. 22)

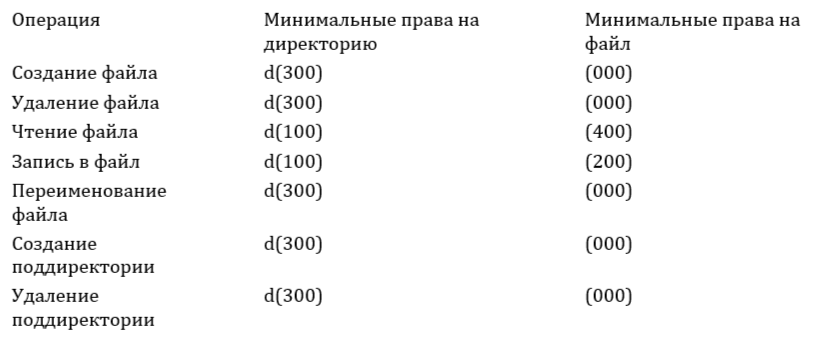


Рис. 22: Таблица минимально необходимых прав для выполнения операций внутри директории dir1

# 4 Выводы

В ходе выполнения данной лабораторной работы я 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.