Отчёт по лабораторной работе №2

Дисциплина: Информационная безопасность

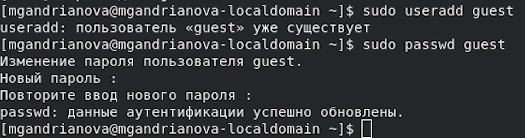
Андрианова Марина Георгиевна

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.

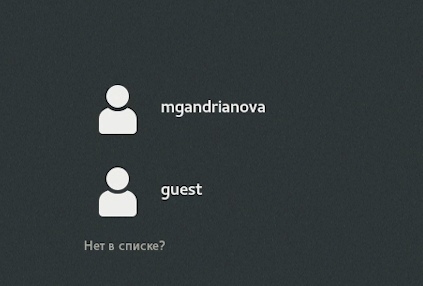
Выполнение лабораторной работы

В установленной при выполнении лабораторной работы ОС создала учётную запись пользователя guest с помощью команды “sudo useradd guest” и задала пароль для этого пользователя командой “sudo passwd guest” (рис.1)

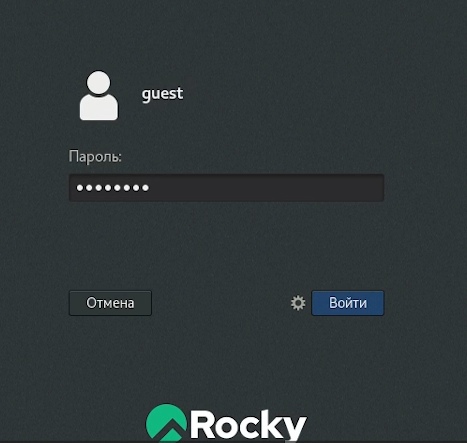


|  |
| --- |
| Рис.1:Создание пользователя |

Вошла в систему от имени пользователя guest (рис.2, рис.3).

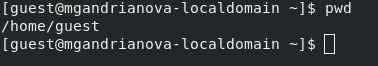


|  |
| --- |
| Рис.2:Вход в систему |



|  |
| --- |
| Рис.3:Вход в систему |

Определила директорию (/home/guest), в которой я нахожусь, командой “pwd”. Сравнила её с приглашением командной строки: они совпадают. Определила, что она является моей домашней директорией (рис.4).



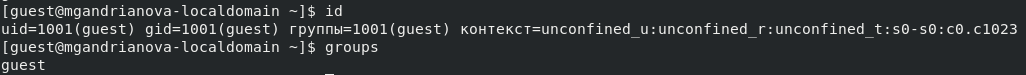
|  |
| --- |
| Рис.4:Команда pwd |

Уточнила имя своего пользователя командой “whoami” и получила вывод: guest (рис.5).



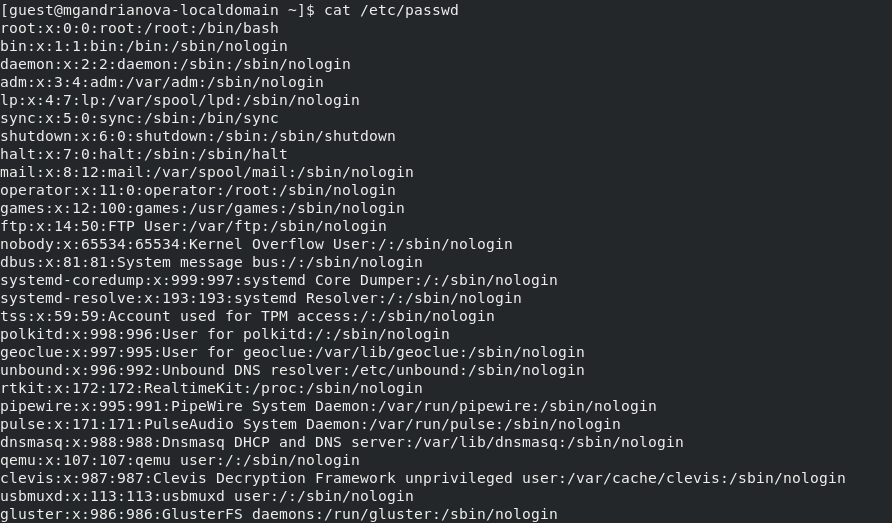
|  |
| --- |
| Рис.5:Команда whoami |

С помощью команды “id” определила имя своего пользователя (guest), uid=1001, gid=1001. Сравнила полученную информацию с выводом команды “groups”, которая вывела “guest”. Мой пользователь входит только в одну группу, состоящую из него самого, поэтому вывод обеих команд (“id” и “groups”) совпадает (рис.6). Данные, выводимые в приглашении командной строки, совпадают с полученной информацией.



|  |
| --- |
| Рис.6:Команды id и groups |

Просмотрела файл /etc/passwd командой “cat /etc/passwd” (рис.7)



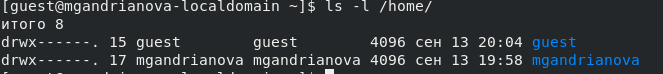
|  |
| --- |
| Рис.7:Команда cat /etc/passwd |

Найшла в нём свою учётную запись (в самом конце) (рис.8). Uid = 1001, gid = 1001, то есть они совпадают с тем, что мы получили ранее.



|  |
| --- |
| Рис.8:Содержание файла /etc/passwd |

Определила существующие в системе директории командой “ls -l /home/” (рис.9). Список поддиректорий директории /home получить удалось. На директориях установлены права чтения, записи и выполнения для самого пользователя (для группы и остальных пользователей никаких прав доступа не установлено).



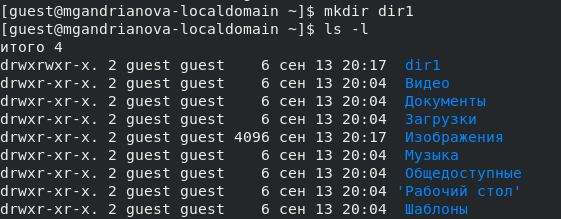
|  |
| --- |
| Рис.9:Существующие в системе директории |

Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой “lsattr /home” (рис.10). Удалось увидеть расширенные атрибуты только директории того пользователя, от имени которого я нахожусь в системе.

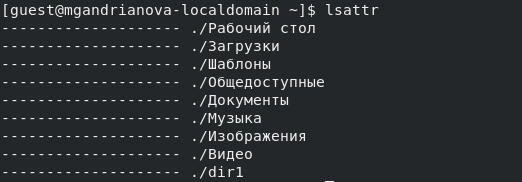


|  |
| --- |
| Рис.10:Расширенные атрибуты |

Создала в домашней директории поддиректорию dir1 командой “mkdir dir1” (рис.11) и определила, какие права доступа и расширенные атрибуты были на неё выставлены: чтение, запись и выполнение доступны только для самого пользователя и для группы, для остальных - только чтение и выполнение, расширенных атрибутов не установлено (рис.12)

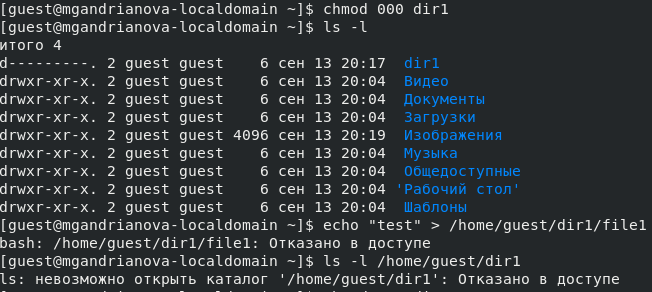


|  |
| --- |
| Рис.11:Создание поддиректории |

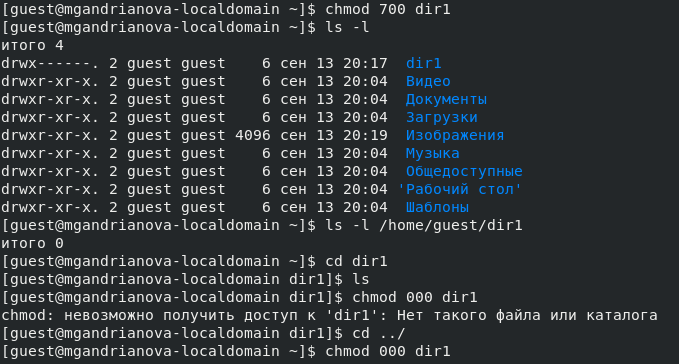


|  |
| --- |
| Рис.12:Команда lsattr |

Сняла с директории dir1 все атрибуты командой “chmod 000 dir1” и проверила с её помощью правильность выполнения команды “ls -l”. Все атрибуты были сняты (рис.13). Попыталась создать в директории dir1 файл file1 командой “echo”test” > /home/guest/dir1/file1” (рис.13). Я получила отказ в выполнении операции по созданию файла, так как предыдущим действием мы убрали право доступа на запись в директории. В итоге файл не был создан; открыть директорию с помощью команды “ls -l /home/guest/dir1” изначально тоже не удалось по той же причине, поэтому я поменяла права доступа (рис.14) и снова воспользовалась этой командой, и тогда смогла просмотреть содержимое директории, убедившись, что файл не был создан.



|  |
| --- |
| Рис.13:Попытка создать файл в директории |



|  |
| --- |
| Рис.14:Создание файла в директории |

Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов). Если операция разрешена, занесём в таблицу знак «+», если не разрешена, знак «-». Создание файла: “echo”text” > /home/guest/dir1/file2”. Удаление файла: “rm -r /home/guest/dir1/file1”. Запись в файл: “echo”textnew” > /home/guest/dir1/file1”. Чтение файла: “cat /home/guest/dir1/file1”. Смена директории: “cd /home/guest/dir1”. Просмотр файлов в директории: “ls /home/guest/dir1”. Переименование файла: “mv /home/guest/dir1/file1 filenew”. Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”.

| 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 (000) | (000) | - | - | - | - | - | - | - | - |
| d –x (100) | (000) | - | - | - | - | + | - | - | - |
| d -w- (200) | (000) | - | - | - | - | - | - | - | - |
| d -wx (300) | (000) | + | + | - | - | + | - | + | - |
| d r– (400) | (000) | - | - | - | - | - | + | - | - |
| d r-x (500) | (000) | - | - | - | - | + | + | - | - |
| d rw- (600) | (000) | - | - | - | - | - | + | - | - |
| d rwx (700) | (000) | + | + | - | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (100) | - | - | - | - | - | - | - | - |
| d –x (100) | (100) | - | - | - | - | + | - | - | - |
| d -w- (200) | (100) | - | - | - | - | - | - | - | - |
| d -wx (300) | (100) | + | + | - | - | + | - | + | - |
| d r– (400) | (100) | - | - | - | - | - | + | - | - |
| d r-x (500) | (100) | - | - | - | - | + | + | - | - |
| d rw- (600) | (100) | - | - | - | - | - | + | - | - |
| d rwx (700) | (100) | + | + | - | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (200) | - | - | - | - | - | - | - | - |
| d –x (100) | (200) | - | - | + | - | + | - | - | - |
| d -w- (200) | (020) | - | - | - | - | - | - | - | - |
| d -wx (300) | (200) | + | + | + | - | + | - | + | - |
| d r– (400) | (200) | - | - | - | - | - | + | - | - |
| d r-x (500) | (200) | - | - | + | - | + | + | - | - |
| d rw- (600) | (200) | - | - | - | - | - | + | - | - |
| d rwx (700) | (200) | + | + | + | - | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (300) | - | - | - | - | - | - | - | - |
| d –x (100) | (300) | - | - | + | - | + | - | - | - |
| d -w- (200) | (300) | - | - | - | - | - | - | - | - |
| d -wx (300) | (300) | + | + | + | + | + | - | + | - |
| d r– (400) | (300) | - | - | - | - | - | + | - | - |
| d r-x (500) | (300) | - | - | + | - | + | + | - | - |
| d rw- (600) | (300) | - | - | - | - | - | + | - | - |
| d rwx (700) | (300) | + | + | + | + | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (400) | - | - | - | - | - | - | - | - |
| d –x (100) | (400) | - | - | - | + | + | - | - | - |
| d -w- (200) | (400) | - | - | - | - | - | - | - | - |
| d -wx (300) | (400) | + | + | - | + | + | - | + | - |
| d r– (400) | (400) | - | - | - | - | - | + | - | - |
| d r-x (500) | (400) | - | - | - | + | + | + | - | - |
| d rw- (600) | (400) | - | - | - | - | - | + | - | - |
| d rwx (700) | (400) | + | + | - | + | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (500) | - | - | - | - | - | - | - | - |
| d –x (100) | (500) | - | - | - | + | + | - | - | - |
| d -w- (200) | (500) | - | - | - | - | - | - | - | - |
| d -wx (300) | (500) | + | + | - | + | + | - | + | - |
| d r– (400) | (500) | - | - | - | - | - | + | - | - |
| d r-x (500) | (500) | - | - | - | + | + | + | - | - |
| d rw- (600) | (500) | - | - | - | - | - | + | - | - |
| d rwx (700) | (500) | + | + | - | + | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (600) | - | - | - | - | - | - | - | - |
| d –x (100) | (600) | - | - | + | + | + | - | - | - |
| d -w- (200) | (600) | - | - | - | - | - | - | - | - |
| d -wx (300) | (600) | + | + | + | + | + | - | + | - |
| d r– (400) | (600) | - | - | - | - | - | + | - | - |
| d r-x (500) | (600) | - | - | + | + | + | + | - | - |
| d rw- (600) | (600) | - | - | - | - | - | + | - | - |
| d rwx (700) | (600) | + | + | + | + | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |
| d (000) | (700) | - | - | - | - | - | - | - | - |
| d –x (100) | (700) | - | - | + | + | + | - | - | - |
| d -w- (200) | (700) | - | - | - | - | - | - | - | - |
| d -wx (300) | (700) | + | + | + | + | + | - | + | - |
| d r– (400) | (700) | - | - | - | - | - | + | - | - |
| d r-x (500) | (700) | - | - | + | + | + | + | - | - |
| d rw- (600) | (700) | - | - | - | - | - | + | - | - |
| d rwx (700) | (700) | + | + | + | + | + | + | + | - |
| —————— | ————- | —————- | —————- | ————— | ————– | —————— | —————————— | ———————- | ———————– |

Сравнивая полученную таблицу с таблицей из прошлой лабораторной работы, приходим к выводу, что изменился только последний столбец, позволяющий изменять атрибуты у файла: теперь это сделать невозможно, т.к. у владельца файла и директории нет на это прав (во всех случаях в первой позиции стоят 0). При определенном наборе прав остальные действия выполняются или не выполняются аналогично предыдущей таблице, но теперь как для владельца, так и для группы.

Заполним таблицу «Минимально необходимые права для выполнения операций внутри директории».

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d -wx (300) | (000) |
| Удаление файла | d -wx (300) | (000) |
| Чтение файла | d –x (100) | (040) |
| Запись в файл | d –x (100) | (020) |
| Переименование файла | d -wx (300) | (000) |
| Создание поддиректории | d -wx (300) | (000) |
| Удаление поддиректории | d -wx (300) | (000) |

Выводы

В ходе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

* Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: https://losst.ru/prava-dostupa-k-fajlam-v-linux.