0.1 Front matter

title: “Лабораторная работа №2” subtitle: “Основы информационной безопасности” author: “Пинега Белла Александровна”

0.2 Generic otions

lang: ru-RU toc-title: “Содержание”

0.3 Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

0.4 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs: name: english ## I18n babel babel-lang: russian babel-otherlangs: english ## Fonts mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9 ## Biblatex biblatex: true biblio-style: “gost-numeric” biblatexoptions: - parentracker=true - backend=biber - hyperref=auto - language=auto - autolang=other* - citestyle=gost-numeric ## Pandoc-crossref LaTeX customization figureTitle: “Рис.” tableTitle: “Таблица” listingTitle: “Листинг” lofTitle: “Список иллюстраций” lotTitle: “Список таблиц” lolTitle: “Листинги” ## Misc options indent: true header-includes: -

keep figures where there are in the text

- ### # keep figures where there are in the text

1 Цель работы

Получение практических навыков работы в консоли с атрибутами фай- лов, закрепление теоретических основ дискреционного разграничения до- ступа в современных системах с открытым кодом на базе ОС Linux

2 Задание

Постарайтесь последовательно выполнить все пункты, занося ваши от- веты на поставленные вопросы и замечания в отчёт. 1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (ис- пользую 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. Срав- ните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директо- рию. 5. Уточните имя вашего пользователя командой whoami. 6. Уточните имя вашего пользователя, его группу, а также группы, куда вхо- дит пользователь, командой id. Выведенные значения uid, gid и др. за- помните. Сравните вывод id с выводом команды groups. 7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. 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 получен- ными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клави- шу shift, нажимайте page up и page down) либо программу grep вкачестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: cat /etc/passwd | grep guest 9. Определите существующие в системе директории командой ls -l /home/ Удалось ли вам получить список поддиректорий директории /home? Ка- кие права установлены на директориях? 10. Проверьте, какие расширенные атрибуты установлены на поддиректо- риях, находящихся в директории /home, командой: lsattr /home Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? 11. Создайте в домашней директории поддиректорию dir1 командой mkdir dir1 Определите командами ls -l и lsattr, какие права доступа и расши- ренные атрибуты были выставлены на директорию dir1. 12. Снимите с директории dir1 все атрибуты командой chmod 000 dir1 и проверьте с её помощью правильность выполнения команды ls -l 13. Попытайтесь создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 Объясните, почему вы получили отказ в выполнении операции по созда- нию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Про- верьте командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1. 14. Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (фай- лов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разре- шена, знак «-». Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибу- ты файлов и директорий, а лишь «первые три»: r, w, x, для «владельца». Остальные атрибуты также важны (особенно при использовании досту- па 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 пользовате- лей: 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 24 Кулябов Д. С., Королькова А. В., Геворкян М. Н. разделить

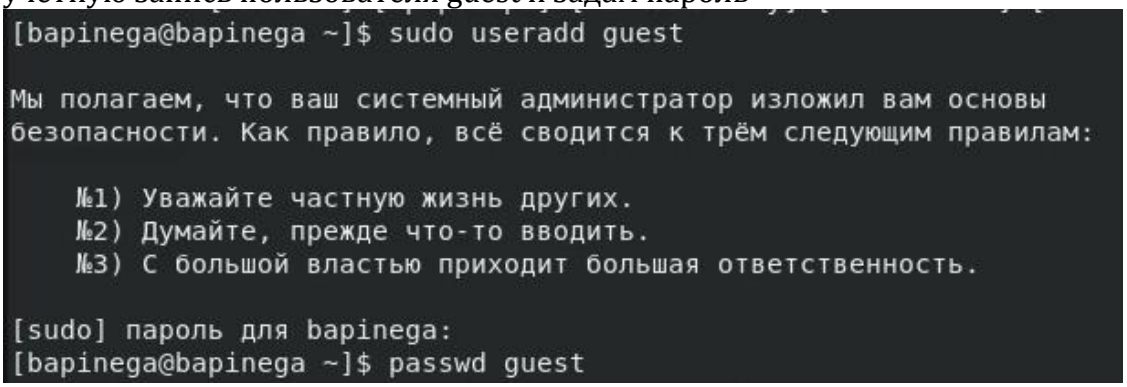
большую таблицу на несколько малых независимых таблиц. В данном примере предлагается рассмотреть 3 + 3 атрибута, т.е. 26 = 64 варианта. Замечание 2: в ряде действий при выполнении команды удаления файла вы можете столкнуться с вопросом: «удалить защищённый от записи пу- стой обычный файл dir1/file1?» Обратите внимание, что наличие этого вопроса не позволяет сделать правильный вывод о том, что файл мож- но удалить. В ряде случаев, при ответе «у» (да) на указанный вопрос, возможно получить другое сообщение: «невозможно удалить dirl /file1: Отказано в доступе». 15. На основании заполненной таблицы определите те или иные минималь- но необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2.

3 Теоретическое введение

1.2.1. Техническое обеспечение Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (https://www.virtualbox.org/) операционной системы Linux (дистрибутив Rocky (https://rockylinux.org/)). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими ха- рактеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (http://www.gentoo.ru/); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: /afs/dk.sci.pfu.edu.ru/common/files/iso/. 1.2.2. Соглашения об именовании При выполнении работ следует придерживаться следующих правил име- нования: имя виртуальной машины, имя хоста вашей виртуальной машины, пользователь внутри виртуальной машины должны совпадать с логином студента, выполняющего лабораторную работу. Вы можете посмотреть ваш логин, набрав в терминале ОС типа Linux команду id -un.

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной ОС создам учётную запись пользователя guest и задам пароль



2. Войду в систему от имени пользователя guest и увижу где я нахожусь
```
[bapinega@bapinega guest]$ pwd
/home/guest
```
Я нахожусь не в домашней директории
3. Имя моего пользователя bapinega
```
[bapinega@bapinega guest]$ whoami
bapinega
```
4. На фото указано имя моего пользователя, его группа, а также группы, куда входит пользователь
```
[bapinega@bapinega guest]$ id
uid=1000(bapinega) gid=1000(bapinega) группы=1000(bapinega),10(wheel) контекст=u
nconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```
Сравню с выводом команды ниже
```
[bapinega@bapinega guest]$ groups
bapinega wheel
```
5. Просмотрю файл /etc/passwd. Я нашла в нем свою учетную запись
```
bapinega:x:1000:1000:bapinega:/home/bapinega:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
```
Можно заметить что значения совпадают с значениями с фото 4.
6. Мне удалось получить список поддиректорий директории /home. Директории можно читать, редактировать, исполнять.
```
[bapinega@bapinega ~]$ ls -l /home/
итого 4
drwx------. 15 bapinega bapinega 4096 фев 15 20:51 bapinega
drwx------.  3 guest    guest      78 фев 15 20:44 guest
```
7. Создам в домашней директории поддиректорию dir1.На директорию dir1 установлены права чтения, исполнения, редактирования. Сниму с директории dir1 все атрибуты. Далее создам в директории dir1 файл file1, но тк я сняла с директории все атрибуты я получаю отказ.
```
[bapinega@bapinega guest]$ mkdir dir1
mkdir: невозможно создать каталог «dir1»: Отказано в доступе
[bapinega@bapinega guest]$ sudo chmod 777 /home/guest
[bapinega@bapinega guest]$ mkdir dir1
[bapinega@bapinega guest]$ ls -l
итого 0
drwxrwxr-x. 2 bapinega bapinega 6 фев 15 21:26 dir1
[bapinega@bapinega guest]$ lsattr
------------------- ./dir1
[bapinega@bapinega guest]$ chmod 000 dir1
[bapinega@bapinega guest]$ ls -l
итого 0
d---------. 2 bapinega bapinega 6 фев 15 21:26 dir1
[bapinega@bapinega guest]$ echo  "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[bapinega@bapinega guest]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
```
Теперь у меня нет прав на создание файла.
8. Заполню таблицу «Установленные права и разрешённые действия» 1 - Создание файла 2- Удаление файла 3- Запись в файл 4- Чтение файла 5- Смена

директории 6- Просмотр файлов в директории 7 - Переименование файла 8- Смена атрибутов файла

Table 1: Установленные права и разрешённые действия

Права директории	Права файла	1	2	3	4	5	6	7	8
d---------(000)	----------(000)	-	-	-	-	-	-	-	-
d--x------(100)	----------(000)	-	-	-	-	+	-	-	+
d-w-------(200)	----------(000)	-	-	-	-	-	-	-	-
d-wx------(300)	----------(000)	+	+	-	-	+	-	+	+
dr--------(400)	----------(000)	-	-	-	-	-	-	-	-
dr-x------(500)	----------(000)	-	-	-	-	+	+	-	+
drw-------(600)	----------(000)	-	-	-	-	-	-	-	-
drwx------(700)	----------(000)	+	+	-	-	+	+	+	+
d---------(000)	---x------(100)	-	-	-	-	-	-	-	-
d--x------(100)	---x------(100)	-	-	-	-	+	-	-	+
d-w-------(200)	---x------(100)	-	-	-	-	-	-	-	-
d-wx------(300)	---x------(100)	+	+	-	-	+	-	+	+
dr--------(400)	---x------(100)	-	-	-	-	-	-	-	-
dr-x------(500)	---x------(100)	-	-	-	-	+	+	-	+
drw-------(600)	---x------(100)	-	-	-	-	-	-	-	-
drwx------(700)	---x------(100)	+	+	-	-	+	+	+	+
d---------(000)	--w-------(200)	-	-	-	-	-	-	-	-
d--x------(100)	--w-------(200)	-	-	+	-	+	-	-	+
d-w-------(200)	--w-------(200)	-	-	-	-	-	-	-	-
d-wx------(300)	--w-------(200)	+	+	+	-	+	-	+	+
dr--------(400)	--w-------(200)	-	-	-	-	-	-	-	-
dr-x------(500)	--w-------(200)	-	-	+	-	+	+	-	+
drw-------(600)	--w-------(200)	-	-	-	-	-	-	-	-
drwx------(700)	--w-------(200)	+	+	+	-	+	+	+	+
d---------(000)	--wx------(300)	-	-	-	-	-	-	-	-
d--x------(100)	--wx------(300)	-	-	+	-	+	-	-	+
d-w-------(200)	--wx------(300)	-	-	-	-	-	-	-	-
d-wx------(300)	--wx------(300)	+	+	+	-	+	-	+	+
dr--------(400)	--wx------(300)	-	-	-	-	-	-	-	-
dr-x------(500)	--wx------(300)	-	-	+	-	+	+	-	+
drw-------(600)	--wx------(300)	-	-	-	-	-	-	-	-
drwx------(700)	--wx------(300)	+	+	+	-	+	+	+	+

Права директории	Права файла	1	2	3	4	5	6	7	8
d---------(000)	-r--------(400)	-	-	-	-	-	-	-	-
d--x------(100)	-r--------(400)	-	-	-	+	+	-	-	+
d-w-------(200)	-r--------(400)	-	-	-	-	-	-	-	-
d-wx------(300)	-r--------(400)	+	+	-	+	+	-	+	+
dr--------(400)	-r--------(400)	-	-	-	-	-	-	-	-
dr-x------(500)	-r--------(400)	-	-	-	+	+	+	-	+
drw-------(600)	-r--------(400)	-	-	-	-	-	-	-	-
drwx------(700)	-r--------(400)	+	+	-	+	+	+	+	+
d---------(000)	-r-x------(500)	-	-	-	-	-	-	-	-
d--x------(100)	-r-x------(500)	-	-	-	+	+	-	-	+
d-w-------(200)	-r-x------(500)	-	-	-	-	-	-	-	-
d-wx------(300)	-r-x------(500)	+	+	-	+	+	-	+	+
dr--------(400)	-r-x------(500)	-	-	-	-	-	-	-	-
dr-x------(500)	-r-x------(500)	-	-	-	+	+	+	-	+
drw-------(600)	-r-x------(500)	-	-	-	-	-	-	-	-
drwx------(700)	-r-x------(500)	+	+	-	+	+	+	+	+
d---------(000)	-rw-------(600)	-	-	-	-	-	-	-	-
d--x------(100)	-rw-------(600)	-	-	+	+	+	-	-	+
d-w-------(200)	-rw-------(600)	-	-	-	-	-	-	-	-
d-wx------(300)	-rw-------(600)	+	+	+	+	+	-	+	+
dr--------(400)	-rw-------(600)	-	-	-	-	-	-	-	-
dr-x------(500)	-rw-------(600)	-	-	+	+	+	+	-	+
drw-------(600)	-rw-------(600)	-	-	-	-	-	-	-	-
drwx------(700)	-rw-------(600)	+	+	+	+	+	+	+	+
d---------(000)	-rwx------(700)	-	-	-	-	-	-	-	-
d--x------(100)	-rwx------(700)	-	-	+	+	+	-	-	+
d-w-------(200)	-rwx------(700)	-	-	-	-	-	-	-	-
d-wx------(300)	-rwx------(700)	+	+	+	+	+	-	+	+
dr--------(400)	-rwx------(700)	-	-	-	-	-	-	-	-
dr-x------(500)	-rwx------(700)	-	-	+	+	+	+	-	+
drw-------(600)	-rwx------(700)	-	-	-	-	-	-	-	-
drwx------(700)	-rwx------(700)	+	+	+	+	+	+	+	+

На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу {#tbl:min-rig} .

Для заполнения последних двух строк опытным путем проверили минимальные права.

Table 2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d-wx------ (300)	---------- (000)
Удаление файла	d-wx------ (300)	---------- (000)
Чтение файла	d--x------ (100)	-r-------- (400)
Запись в файл	d--x------ (100)	--w------- (200)
Переименование файла	d-wx------ (300)	----------(000)
Создание поддиректории	d-wx------ (300)	---------- (000)
Удаление поддиректории	d-wx------ (300)	---------- (000)

5 Выводы

Я приобрела практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы