

Лабораторная работа № 2. Установка и конфигурация операционной системы на виртуальную машину

Малахихин Максим НПИбд 01-20

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.

Ход работы

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

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

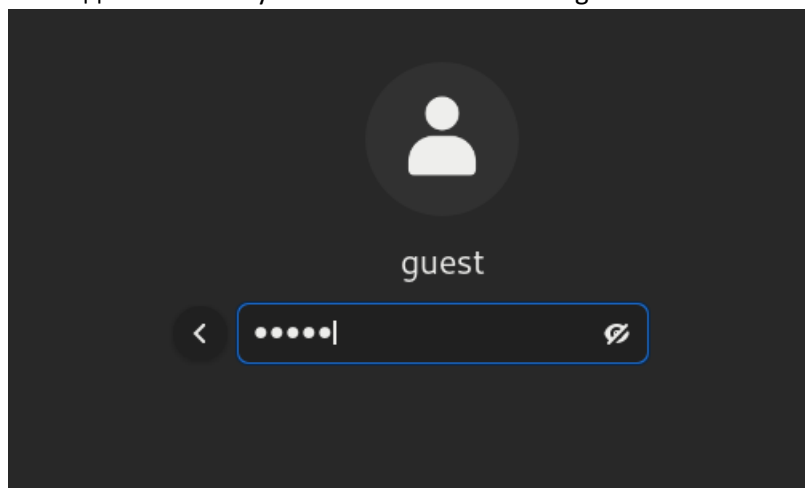
`useradd guest`

2. Задайте пароль для пользователя guest (используя учётную запись администратора):

`passwd guest`

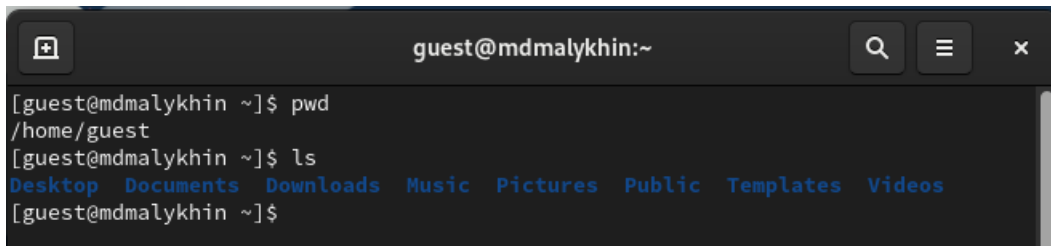
```
[mdmalykhin@mdmalykhin ~]$ su -
Password:
[root@mdmalykhin ~]# useradd guest
[root@mdmalykhin ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@mdmalykhin ~]#
```

3. Войдите в систему от имени пользователя guest.



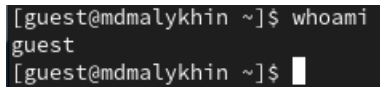
4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.

****Да, является****

A terminal window titled 'guest@mdmalykhin:~' with search, menu, and close buttons. It shows the execution of 'pwd' resulting in '/home/guest' and 'ls' showing a list of directories: Desktop, Documents, Downloads, Music, Pictures, Public, Templates, Videos.

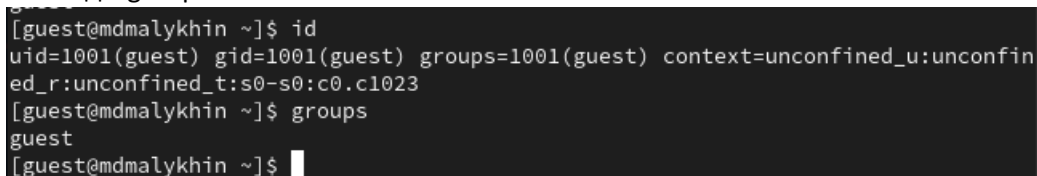
```
[guest@mdmalykhin ~]$ pwd
/home/guest
[guest@mdmalykhin ~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[guest@mdmalykhin ~]$
```

5. Уточните имя вашего пользователя командой whoami.

A terminal window showing the 'whoami' command being executed, which returns the username 'guest'.

```
[guest@mdmalykhin ~]$ whoami
guest
[guest@mdmalykhin ~]$
```

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.

A terminal window showing the 'id' and 'groups' commands. 'id' outputs user and group IDs and context, while 'groups' lists the user's primary and secondary groups.

```
[guest@mdmalykhin ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mdmalykhin ~]$ groups
guest
[guest@mdmalykhin ~]$
```

****groups выдает группы, id выдает gid, groups, context****

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.

****Сходится.****

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`

```
[guest@mdmalykhin ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979:/:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
mdmalykhin:x:1000:1000:mdmalykhin:/home/mdmalykhin:/bin/bash
vboxadd:x:977:1:/:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/:/home/guest:/bin/bash
```

```
[guest@mdmalykhin ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@mdmalykhin ~]$
```

****guest:uid:gid****

9. Определите существующие в системе директории командой

`ls -l /home/`

Удалось ли вам получить список поддиректорий директории `/home`? Какие права установлены на директориях?

```
[guest@mdmalykhin ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Sep 16 15:04 guest
drwx-----. 14 mdmalykhin mdmalykhin 4096 Sep 16 15:04 mdmalykhin
[guest@mdmalykhin ~]$
```

****Сущетсвуют**

directory read+write+execute**

10. 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 других пользователей?

```
[guest@mdmalykhin ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/mdmalykhin
----- /home/guest
[guest@mdmalykhin ~]$ lsattr /home/guest
----- /home/guest/Desktop
----- /home/guest/Downloads
----- /home/guest/Templates
----- /home/guest/Public
----- /home/guest/Documents
----- /home/guest/Music
----- /home/guest/Pictures
----- /home/guest/Videos
[guest@mdmalykhin ~]$
```

****Не удалось****

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.

12. Снимите с директории dir1 все атрибуты командой

chmod 000 dir1

и проверьте с её помощью правильность выполнения команды

ls -l

```
[guest@mdmalykhin ~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[guest@mdmalykhin ~]$ mkdir dir1
[guest@mdmalykhin ~]$ ls
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos
[guest@mdmalykhin ~]$ ls -l dir1
total 0
[guest@mdmalykhin ~]$ lsattr dir1
[guest@mdmalykhin ~]$ lsattr /dir1
lsattr: No such file or directory while trying to stat /dir1
[guest@mdmalykhin ~]$ chmod 000 dir1
[guest@mdmalykhin ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Desktop
d------. 2 guest guest 6 Sep 16 15:24 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 14:57 Videos
[guest@mdmalykhin ~]$
```

13. Попробуйте 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.

```
[guest@mdmalykhin ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@mdmalykhin ~]$
```

****Нет разрешения на запись. Кроме того, нет разрешения на чтение.****

14. Заполните таблицу «Установленные права и разрешённые действия»

(см. табл. 2.1), 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. 2

6 = 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 dir1 /file1:

Отказано в доступе».

30	dr-----(400)	-wx-----(300)	нет	нет	нет	нет	нет	нет	нет	нет
31	dr-x-----(500)	-wx-----(300)	нет	нет	да	нет	нет	да	нет	да
32	drwx-----(600)	-wx-----(300)	да	да	нет	нет	нет	да	нет	нет
33	drwx-----(700)	-wx-----(300)	да	да	да	нет	да	да	да	да
34	d-----(000)	r------(400)	нет	нет	нет	нет	нет	нет	нет	нет
35	d-x-----(100)	r------(400)	нет	нет	нет	да	да	нет	нет	да
36	d-w-----(200)	r------(400)	нет	нет	нет	нет	нет	нет	нет	нет
37	d-wx-----(300)	r------(400)	да	да	нет	да	нет	нет	нет	нет
38	dr------(400)	r------(400)	нет	нет	нет	нет	нет	нет	нет	нет
39	dr-x------(500)	r------(400)	нет	нет	нет	да	да	да	нет	да
40	drw------(600)	r------(400)	да	да	нет	нет	нет	да	нет	нет
41	drwx------(700)	r------(400)	да	да	нет	да	да	да	да	да
42	d------(000)	r-x------(500)	нет	нет	нет	нет	нет	нет	нет	нет
43	d-x------(100)	r-x------(500)	нет	нет	нет	да	да	нет	нет	да
44	d-w------(200)	r-x------(500)	нет	нет	нет	нет	нет	нет	нет	нет
45	d-wx------(300)	r-x------(500)	да	да	нет	да	нет	нет	нет	нет
46	dr------(400)	r-x------(500)	нет	нет	нет	нет	нет	нет	нет	нет
47	dr-x------(500)	r-x------(500)	нет	нет	нет	да	да	да	нет	да
48	drw------(600)	r-x------(500)	да	да	нет	нет	нет	да	нет	нет
49	drwx------(700)	r-x------(500)	да	да	нет	да	да	да	да	да
50	d------(000)	rw------(600)	нет	нет	нет	нет	нет	нет	нет	нет
51	d-x------(100)	rw------(600)	нет	нет	да	да	да	нет	нет	да
52	d-w------(200)	rw------(600)	нет	нет	нет	нет	нет	нет	нет	нет
53	d-wx------(300)	rw------(600)	да	да	да	да	нет	нет	нет	нет
54	dr------(400)	rw------(600)	нет	нет	нет	нет	нет	нет	нет	нет
55	dr-x------(500)	rw------(600)	нет	нет	да	да	да	да	нет	да
56	drw------(600)	rw------(600)	да	да	нет	нет	да	да	нет	нет
1	Права директории	Права файла	Создание файла	Удаление файла	Запись	Чтение	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
2	d------(000)	------(000)	нет	нет	нет	нет	нет	нет	нет	нет
3	d-x------(100)	------(000)	нет	нет	нет	нет	да	нет	нет	да
4	d-w------(200)	------(000)	нет	нет	нет	нет	нет	нет	нет	нет
5	d-wx------(300)	------(000)	да	да	нет	нет	нет	нет	нет	нет
6	dr------(400)	------(000)	нет	нет	нет	нет	нет	нет	нет	нет
7	dr-x------(500)	------(000)	нет	нет	нет	нет	да	да	нет	да
8	drw------(600)	------(000)	да	да	нет	нет	нет	да	нет	нет
9	drwx------(700)	------(000)	да	да	нет	да	да	да	да	да
10	d------(000)	--x------(100)	нет	нет	нет	нет	нет	нет	нет	нет
11	d-x------(100)	--x------(100)	нет	нет	нет	нет	да	нет	нет	да
12	d-w------(200)	--x------(100)	нет	нет	нет	нет	нет	нет	нет	нет
13	d-wx------(300)	--x------(100)	да	да	нет	нет	нет	нет	нет	нет
14	dr------(400)	--x------(100)	нет	нет	нет	нет	нет	нет	нет	нет
15	dr-x------(500)	--x------(100)	нет	нет	нет	нет	да	да	нет	да
16	drw------(600)	--x------(100)	да	да	нет	нет	нет	да	нет	нет
17	drwx------(700)	--x------(100)	да	да	нет	да	да	да	да	да
18	d------(000)	-w------(200)	нет	нет	нет	нет	нет	нет	нет	нет
19	d-x------(100)	-w------(200)	нет	нет	да	нет	да	нет	нет	да
20	d-w------(200)	-w------(200)	нет	нет	нет	нет	нет	нет	нет	нет
21	d-wx------(300)	-w------(200)	да	да	да	нет	нет	нет	нет	нет
22	dr------(400)	-w------(200)	нет	нет	нет	нет	нет	нет	нет	нет
23	dr-x------(500)	-w------(200)	нет	нет	да	нет	нет	да	нет	да
24	drw------(600)	-w------(200)	да	да	нет	нет	нет	да	нет	нет
25	drwx------(700)	-w------(200)	да	да	да	нет	да	да	да	да
26	d------(000)	-wx------(300)	нет	нет	нет	нет	нет	нет	нет	нет
27	d-x------(100)	-wx------(300)	нет	нет	да	нет	да	нет	нет	да
28	d-w------(200)	-wx------(300)	нет	нет	нет	нет	нет	нет	нет	нет
29	d-wx------(300)	-wx------(300)	да	да	да	нет	нет	нет	нет	нет

57	drwx-----(700)	rw-----(600)	да	да	да	да	да	да	да	да
58	d----- (000)	rwX----- (700)	нет	нет	нет	нет	нет	нет	нет	нет
59	d-x----- (100)	rwX----- (700)	нет	нет	да	да	да	нет	нет	да
60	d-w----- (200)	rwX----- (700)	нет	нет	нет	нет	нет	нет	нет	нет
61	d-wx----- (300)	rwX----- (700)	да	да	да	да	нет	нет	нет	нет
62	dr----- (400)	rwX----- (700)	нет	нет	нет	нет	нет	нет	нет	нет
63	dr-x----- (500)	rwX----- (700)	нет	нет	да	да	да	да	нет	да
64	drw----- (600)	rwX----- (700)	да	да	нет	нет	да	да	нет	нет
65	drwx----- (700)	rwX----- (700)	да	да	да	да	да	да	да	да

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

Операция	Мин права директории	Мин права файла
Создание файла	wx	-
Удаление файла	wx	-
Запись	x	w
Чтение	x	r
Смена директории	x	-
Просмотр файлов в директории	r	-
Переименование файла	x	w
Смена атрибутов файла	x	w

Вывод

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.