

Отчёт по лабораторной работе № 2

Основы информационной безопасности

Луангсуваннавонг Сайпхачан, НКАбд-01-24

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
3.1 Работа с атрибутами файлов	7
3.2 Заполнение таблицы 2.1	12
3.3 Заполнение таблицы 2.2	15
4 Выводы	17
Список литературы	18

Список иллюстраций

3.1	Создание учетной записи guest	7
3.2	Вход в пользователь guest	8
3.3	Получение информации о пользователе	9
3.4	Получение информации о пользователе	9
3.5	Получение информации о пользователе	10
3.6	Получение списка подкаталогов и их атрибутов	10
3.7	Получение списка подкаталогов и их атрибутов	10
3.8	Создание подкаталога и получение его атрибутов	11
3.9	Настройка атрибутов	11
3.10	Проверка и тестирование атрибутов	12
3.11	Заполнение таблицы 2.1	15
3.12	Заполнение таблицы 2.2	16

Список таблиц

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

2 Задание

1. Работа с атрибутами файлов
2. Заполнение таблицы «Установленные права и разрешённые действия» (табл. 2.1)
3. Заполнение таблицы «Минимальные права для совершения операций» (табл. 2.2)

3 Выполнение лабораторной работы

3.1 Работа с атрибутами файлов

Я открываю терминал в операционной системе Rocky Linux, затем перехожу в учётную запись администратора с помощью sudo -i, после чего создаю новую учётную запись guest. (рис. 3.1)

```
sayprachanhlsvnv@sayprachanhlsvnv:~$ sudo -i
[sudo] password for sayprachanhlsvnv:
Sorry, try again.
[sudo] password for sayprachanhlsvnv:
root@sayprachanhlsvnv:~# useradd guest
root@sayprachanhlsvnv:~# passwd guest
New password:
Retype new password:
passwd: password updated successfully
root@sayprachanhlsvnv:~#
```

Рисунок 3.1: Создание учетной записи guest

Затем я перезагружаю виртуальную машину, чтобы войти как пользователь guest. (рис. 3.2)

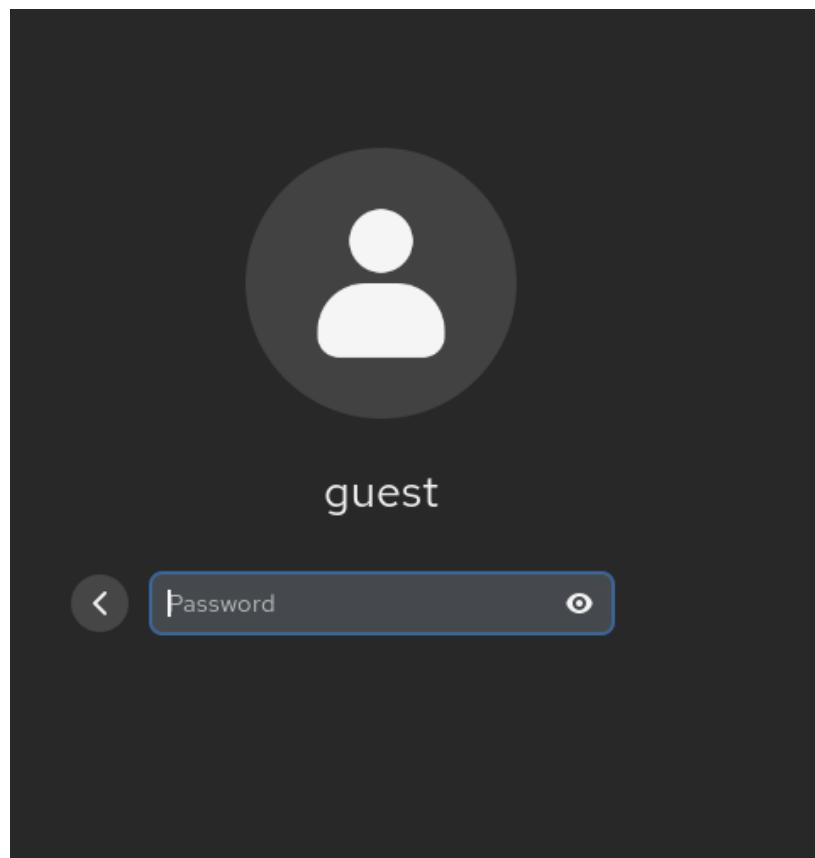
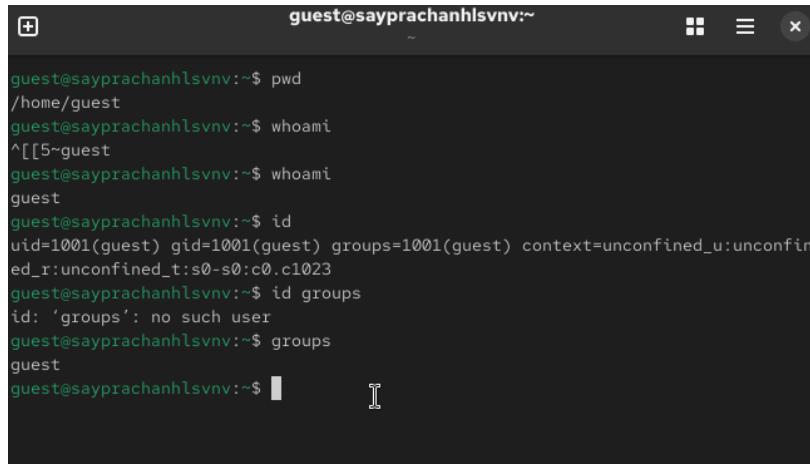


Рисунок 3.2: Вход в пользователь guest

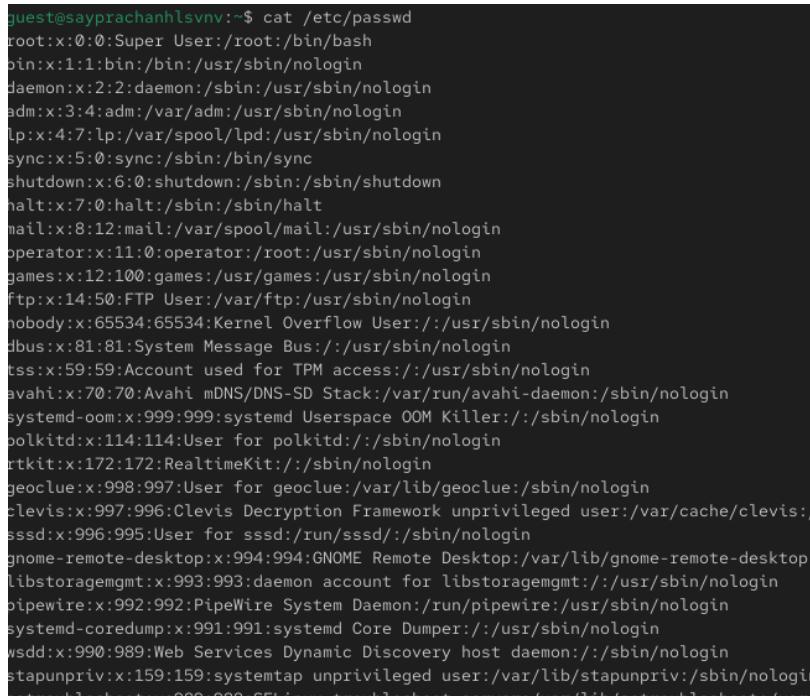
С помощью команды `pwd` я отображаю текущую директорию - это домашняя директория, затем определяю имя своего пользователя командой `whoami`. Используя команду `id`, я получаю информацию об имени пользователя, имени группы, а также о группах, в которые входит пользователь; если использовать команду `groups`, она отобразит только информацию о пользователе `guest`. Затем я сверяю полученную информацию с именем моего пользователя — она совпадает. (рис. 3.3)



```
guest@sayprachanhlsvnv:~$ pwd
/home/guest
guest@sayprachanhlsvnv:~$ whoami
^[[5~guest
guest@sayprachanhlsvnv:~$ whoami
guest
guest@sayprachanhlsvnv:~$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
guest@sayprachanhlsvnv:~$ id groups
id: 'groups': no such user
guest@sayprachanhlsvnv:~$ groups
guest
guest@sayprachanhlsvnv:~$
```

Рисунок 3.3: Получение информации о пользователе

Я просматриваю основную информацию об учётных записях пользователей в файле /etc/passwd. (рис. 3.4)



```
guest@sayprachanhlsvnv:~$ cat /etc/passwd
root:x:0:0:Super User:/root:/bin/bash
bin:x:1:1:bin:/bin:/usr/sbin/nologin
daemon:x:2:2:daemon:/sbin:/usr/sbin/nologin
adm:x:3:4:adm:/var/adm:/usr/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/usr/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:/usr/sbin/nologin
operator:x:11:0:operator:/root:/usr/sbin/nologin
games:x:12:100:games:/usr/games:/usr/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/usr/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/usr/sbin/nologin
dbus:x:81:81:System Message Bus:/:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access://:/usr/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
systemd-oom:x:999:999:systemd Userspace OOM Killer://:/sbin/nologin
polkitd:x:114:114:User for polkitd:/:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/:/sbin/nologin
geoclue:x:998:997:User for geoclue:/var/lib/geoclue:/sbin/nologin
clevis:x:997:996:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/_
sssd:x:996:995:User for sssd:/run/sssd:/sbin/nologin
gnome-remote-desktop:x:994:994:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:
libstoragemgmt:x:993:993:daemon account for libstoragemgmt:/:/usr/sbin/nologin
pipewire:x:992:992:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
systemd-coredump:x:991:991:systemd Core Dumper:/:/usr/sbin/nologin
wsdd:x:990:989:Web Services Dynamic Discovery host daemon:/:/sbin/nologin
stapunpriv:x:159:159:systemtap unprivileged user:/var/lib/stapunpriv:/sbin/nologin
```

Рисунок 3.4: Получение информации о пользователе

Затем я запрашиваю информацию о конкретном пользователе с помощью команды grep и имени пользователя. (рис. 3.5)

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

Рисунок 3.5: Получение информации о пользователе

Используя команду ls -l, я получаю список поддиректорий внутри /home/ и это верно: как у sayprachanhlsvnv, так и у guest одинаковые права: drwx-- (рис. 3.6)

```
guest@sayprachanhlsvnv:~$ ls -l /home/
total 8
drwx----- 14 guest           guest          4096 Feb 13 13:57 guest
drwx----- 20 sayprachanhlsvnv sayprachanhlsvnv 4096 Feb 13 00:01 sayprachanhlsvnv
guest@sayprachanhlsvnv:~$
```

Рисунок 3.6: Получение списка подкаталогов и их атрибутов

Я попытался проверить расширенные атрибуты поддиректорий, находящихся в директории /home, но это не удалось — информация об атрибутах не отображается. (рис. 3.7)

```
guest@sayprachanhlsvnv:~$ lsattr /home
lsattr: Permission denied While reading flags on /home/sayprachanhlsvnv
----- /home/guest
guest@sayprachanhlsvnv:~$
```

Рисунок 3.7: Получение списка подкаталогов и их атрибутов

Я создаю поддиректорию dir1, затем с помощью ls -l проверяю список его поддиректорий (он пуст), после чего просматриваю расширенные атрибуты командой lsattr, но они не отобразились; используя команду ls -la, видно, что атрибуты: drwxr-xr-x. (рис. 3.8)

```

guest@sayprachanhlsvnv:~$ mkdir dir1
guest@sayprachanhlsvnv:~$ ls -l dir1
total 0
guest@sayprachanhlsvnv:~$ lsattr dir1
guest@sayprachanhlsvnv:~$ ls -la
total 24
drwx----- 15 guest guest 4096 Feb 13 13:41 .
drwxr-xr-x  4 root  root   43 Feb 13 13:35 ..
-rw-r--r--  1 guest guest  18 Oct 29 2024 .bash_logout
-rw-r--r--  1 guest guest 144 Oct 29 2024 .bash_profile
-rw-r--r--  1 guest guest 522 Oct 29 2024 .bashrc
drwx-----  9 guest guest 4096 Feb 13 13:37 .cache
drwx-----  8 guest guest 4096 Feb 13 13:37 .config
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Desktop
drwxr-xr-x  2 guest guest   6 Feb 13 13:41 dir1
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Documents
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Downloads
drwx-----  4 guest guest  32 Feb 13 13:37 .local
drwxr-xr-x  4 guest guest  39 Feb 10 21:15 .mozilla
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Music
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Pictures
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Public
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Templates
drwxr-xr-x  2 guest guest   6 Feb 13 13:37 Videos
guest@sayprachanhlsvnv:~$ 

```

Рисунок 3.8: Создание подкаталога и получение его атрибутов

Я назначаю поддиректории dir1 новые атрибуты с помощью команды chmod, установив значение 000, затем при выполнении ls -l в домашней директории отображается, что поддиректория имеет атрибут 0. (рис. 3.9)

```

guest@sayprachanhlsvnv:~$ chmod 000 dir1
guest@sayprachanhlsvnv:~$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Desktop
d-----. 2 guest guest 6 Feb 13 13:41 dir1
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Documents
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Music
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Public
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Templates
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Videos
guest@sayprachanhlsvnv:~$ ls -l dir1
ls: cannot open directory 'dir1': Permission denied
guest@sayprachanhlsvnv:~$ 

```

Рисунок 3.9: Настройка атрибутов

Я пытаюсь создать файл в этой поддиректории — получаю отказ в доступе (permission denied), аналогично с командой ls -l, так как мы установили атрибуты в 000, то есть владелец, группа и остальные не могут ничего с ней делать.

И поскольку команда создания файла не удалась, в поддиректории dir1 файл file1 отсутствует. (рис. 3.10)

```
guest@sayprachanhlsvnv:~$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
guest@sayprachanhlsvnv:~$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
guest@sayprachanhlsvnv:~$
```

Рисунок 3.10: Проверка и тестирование атрибутов

3.2 Заполнение таблицы 2.1

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов	Переименование файла	Изменение атрибутов
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+

d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-

d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Таблица «Установленные права и разрешённые действия» (табл. 2.1)(рис. 3.11)

```

mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
guest@sayprachanhlsvnv:~$ chmod 500 dir1/file1
guest@sayprachanhlsvnv:~$ echo test > dir1/file1
bash: dir1/file1: Permission denied
guest@sayprachanhlsvnv:~$ echo test > dir1/file2
bash: dir1/file2: Permission denied
guest@sayprachanhlsvnv:~$ echo test >> dir1/file1
bash: dir1/file1: Permission denied
guest@sayprachanhlsvnv:~$ rm dir1/file1
rm: remove write-protected regular file 'dir1/file1'? y
rm: cannot remove 'dir1/file1': Permission denied
guest@sayprachanhlsvnv:~$ cat dir1/file1
test
test
guest@sayprachanhlsvnv:~$ cd dir1
guest@sayprachanhlsvnv:~/dir1$ cd
guest@sayprachanhlsvnv:~$ ls -l dir1
ls: cannot open directory 'dir1': Permission denied
guest@sayprachanhlsvnv:~$ mv dir1/file1 dir1/file2
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
guest@sayprachanhlsvnv:~$ chmod 600 dir1/file1
guest@sayprachanhlsvnv:~$ echo test > dir1/file2
bash: dir1/file2: Permission denied
guest@sayprachanhlsvnv:~$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
guest@sayprachanhlsvnv:~$ echo test >> dir1/file1
guest@sayprachanhlsvnv:~$ cat dir1/file1
test
test
test
guest@sayprachanhlsvnv:~$ cd dir1
guest@sayprachanhlsvnv:~/dir1$ cd
guest@sayprachanhlsvnv:~$ ls -l dir1/file1
-rw-----. 1 guest guest 15 Feb 13 14:09 dir1/file1
guest@sayprachanhlsvnv:~$ ls -l dir1

```

Рисунок 3.11: Заполнение таблицы 2.1

3.3 Заполнение таблицы 2.2

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	-

Удаление	d(300)	-
файла		
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование	d(300)	(000)
файла		
Создание	d(300)	-
поддиректории		
Удаление	d(300)	-
поддиректории		

Таблица «Минимальные права для совершения операций» (табл. 2.2)(рис. 3.12)

```
guest@sayprachanhlsvnv:~$ chmod 000 dir1
guest@sayprachanhlsvnv:~$ mkdir a dir1/
mkdir: cannot create directory 'dir1/': File exists
guest@sayprachanhlsvnv:~$ mkdir dir1/a
mkdir: cannot create directory 'dir1/a': Permission denied
guest@sayprachanhlsvnv:~$ chmod 100 dir1
guest@sayprachanhlsvnv:~$ mkdir dir1/a
mkdir: cannot create directory 'dir1/a': Permission denied
guest@sayprachanhlsvnv:~$ chmod 200 dir1
guest@sayprachanhlsvnv:~$ mkdir dir1/a
mkdir: cannot create directory 'dir1/a': Permission denied
guest@sayprachanhlsvnv:~$ chmod 300 dir1
guest@sayprachanhlsvnv:~$ mkdir dir1/a
guest@sayprachanhlsvnv:~$ rmdir dir1/a
guest@sayprachanhlsvnv:~$ mkdir dir1/a
guest@sayprachanhlsvnv:~$ chmod 200 dir1
guest@sayprachanhlsvnv:~$ rmdir dir1/a
rmdir: failed to remove 'dir1/a': Permission denied
guest@sayprachanhlsvnv:~$ █
```

Рисунок 3.12: Заполнение таблицы 2.2

4 Выводы

Я получил практические навыки работы в консоли с атрибутами файлов и закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

Атрибуты Linux chmod: <https://opensource.com/article/19/8/linux-chmod-command>