

Лабораторная работа № 2

Дискреционное разграничение прав в Linux. Основные атрибуты

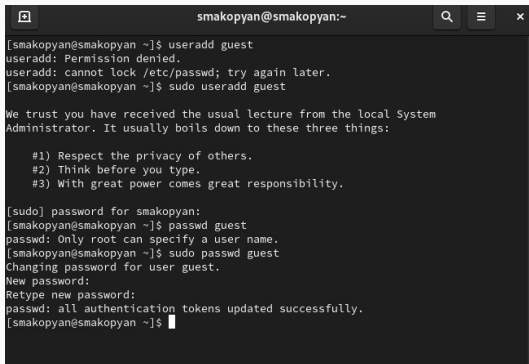
Акопян Сатеник

Российский университет дружбы народов, Москва, Россия

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

Выполнение лабораторной работы

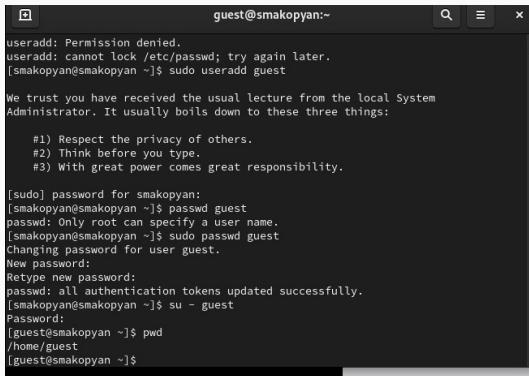
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора). Задайте пароль для пользователя guest (используя учётную запись администратора):

A terminal window titled 'smakopyan@smakopyan:~' with search, menu, and close icons. It shows the execution of 'useradd guest' which fails with 'Permission denied' and 'cannot lock /etc/passwd'. Then 'sudo useradd guest' is run, followed by a system message about the local system administrator. A list of three principles is displayed: 1) Respect the privacy of others, 2) Think before you type, 3) With great power comes great responsibility. Then 'sudo password for smakopyan:' is entered, followed by 'passwd guest' which fails with 'Only root can specify a user name.'. Finally, 'sudo passwd guest' is run, prompting for a new password and its confirmation, and ending with 'passwd: all authentication tokens updated successfully.' and a new prompt.

```
smakopyan@smakopyan:~  
[smakopyan@smakopyan ~]$ useradd guest  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[smakopyan@smakopyan ~]$ sudo useradd guest  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for smakopyan:  
[smakopyan@smakopyan ~]$ passwd guest  
passwd: Only root can specify a user name.  
[smakopyan@smakopyan ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[smakopyan@smakopyan ~]$
```

Выполнение лабораторной работы

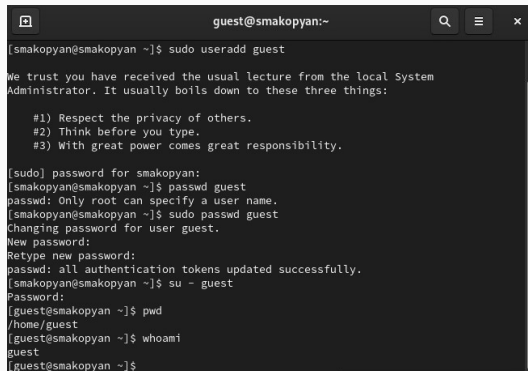
- Войдите в систему от имени пользователя guest (команда su). Определите директорию, в которой вы находитесь, командой pwd.



```
guest@smakopyan:~  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[smakopyan@smakopyan ~]$ sudo useradd guest  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for smakopyan:  
[smakopyan@smakopyan ~]$ passwd guest  
passwd: Only root can specify a user name.  
[smakopyan@smakopyan ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[smakopyan@smakopyan ~]$ su - guest  
Password:  
[guest@smakopyan ~]$ pwd  
/home/guest  
[guest@smakopyan ~]$
```

Рис. 2: рисунок 2

3. Уточните имя вашего пользователя командой whoami

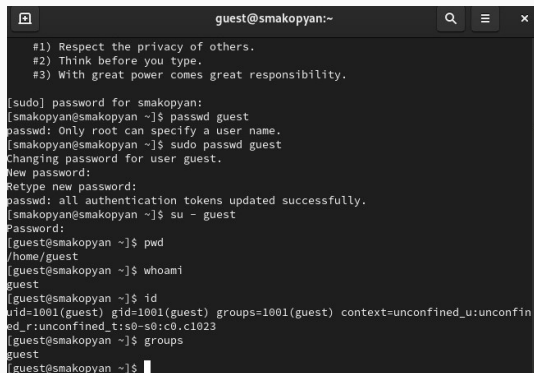


```
guest@smakopyan:~  
[smakopyan@smakopyan ~]$ sudo useradd guest  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for smakopyan:  
[smakopyan@smakopyan ~]$ passwd guest  
passwd: Only root can specify a user name.  
[smakopyan@smakopyan ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[smakopyan@smakopyan ~]$ su - guest  
Password:  
[guest@smakopyan ~]$ pwd  
/home/guest  
[guest@smakopyan ~]$ whoami  
guest  
[guest@smakopyan ~]$
```

Рис. 3: рисунок 3

Выполнение лабораторной работы

4. 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`.

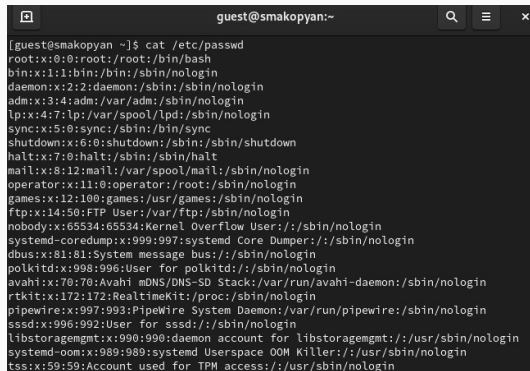


```
guest@smakopyan:~  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for smakopyan:  
[smakopyan@smakopyan ~]$ passwd guest  
passwd: Only root can specify a user name.  
[smakopyan@smakopyan ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[smakopyan@smakopyan ~]$ su - guest  
Password:  
[guest@smakopyan ~]$ pwd  
/home/guest  
[guest@smakopyan ~]$ whoami  
guest  
[guest@smakopyan ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@smakopyan ~]$ groups  
guest  
[guest@smakopyan ~]$
```

Рис. 4: рисунок 4

Выполнение лабораторной работы

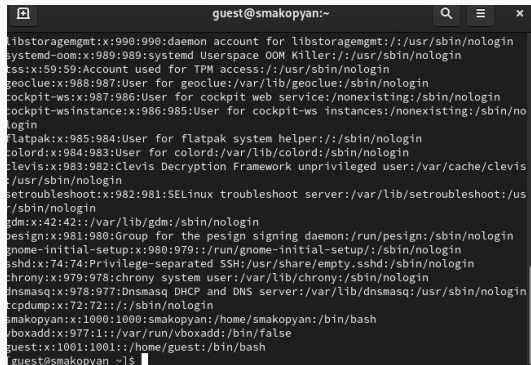
5. Просмотрите файл /etc/passwd командой cat /etc/passwd



```
guest@smakopyan:~$ 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
pipewire:x:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/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:/usr/sbin/nologin
```

Рис. 5: рисунок 5

Выполнение лабораторной работы



```
guest@smakopyan:~  
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:/usr/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:/usr/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
design:x:981:980:Group for the design signing daemon:/run/design:/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:/usr/sbin/nologin  
tcpdump:x:72:72:/sbin/nologin  
smakopyan:x:1000:1000:smakopyan:/home/smakopyan:/bin/bash  
vboxadd:x:977:1:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
guest@smakopyan ~]$
```

Рис. 6: рисунок 6

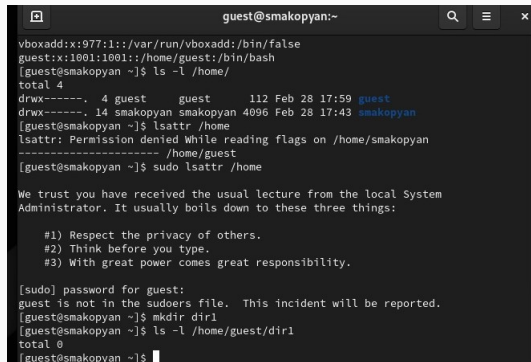
Выполнение лабораторной работы

6. Определите существующие в системе директории командой `ls -l /home/`
Удалось ли вам получить список поддиректорий директории `/home`? (да) Ка-
кие права установлены на директориях? (Создание файла, Удаление файла,
запись в файл, чтение файла, смена директории, просмотр файлов в
директории, переименование файла, смена атрибутов файла)

```
guest@smakopyan:~  
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/no  
login  
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:/us  
r/sbin/nologin  
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin  
design:x:981:980:Group for the design signing daemon:/run/design:/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:/usr/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
smakopyan:x:1000:1000:smakopyan:/home/smakopyan:/bin/bash  
vboxadd:x:977:1:/:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/:/home/guest:/bin/bash  
[guest@smakopyan ~]$ ls -l /home/  
total 4  
drwx-----. 4 guest guest 112 Feb 28 17:59 guest  
drwx-----. 14 smakopyan smakopyan 4096 Feb 28 17:43 smakopyan
```

7. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` Удалось ли вам увидеть расширенные атрибуты директории (нет)? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей (нет)

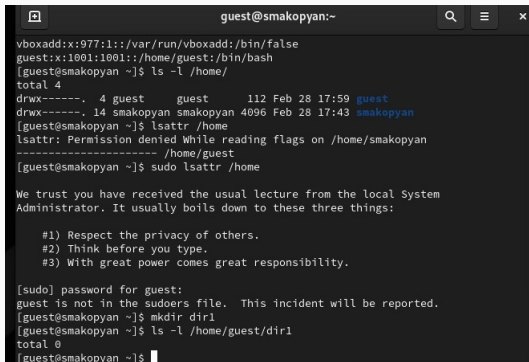
Выполнение лабораторной работы



```
guest@smakopyan:~  
vboxadd:x:977:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@smakopyan ~]$ ls -l /home/  
total 4  
drwx-----. 4 guest      guest      112 Feb 28 17:59 guest  
drwx-----. 14 smakopyan smakopyan 4096 Feb 28 17:43 smakopyan  
[guest@smakopyan ~]$ lsattr /home  
lsattr: Permission denied while reading flags on /home/smakopyan  
----- /home/guest  
[guest@smakopyan ~]$ sudo lsattr /home  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for guest:  
guest is not in the sudoers file. This incident will be reported.  
[guest@smakopyan ~]$ mkdir dir1  
[guest@smakopyan ~]$ ls -l /home/guest/dir1  
total 0  
[guest@smakopyan ~]$
```

Рис. 8: рисунок 8

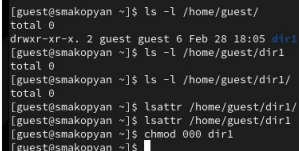
8. Создайте в домашней директории поддиректорию dir1 командой mkdir dir1



```
guest@smakopyan:~  
vboxadd:x:977:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@smakopyan ~]$ ls -l /home/  
total 4  
drwx-----. 4 guest      guest      112 Feb 28 17:59 guest  
drwx-----. 14 smakopyan smakopyan 4096 Feb 28 17:43 smakopyan  
[guest@smakopyan ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/smakopyan  
----- /home/guest  
[guest@smakopyan ~]$ sudo lsattr /home  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for guest:  
guest is not in the sudoers file. This incident will be reported.  
[guest@smakopyan ~]$ mkdir dir1  
[guest@smakopyan ~]$ ls -l /home/guest/dir1  
total 0  
[guest@smakopyan ~]$
```

Рис. 9: рисунок 9

9. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`



```
[guest@smakopyan ~]$ ls -l /home/guest/  
total 0  
drwxr-xr-x. 2 guest guest 6 Feb 28 18:05 dir1  
[guest@smakopyan ~]$ ls -l /home/guest/dir1  
total 0  
[guest@smakopyan ~]$ ls -l /home/guest/dir1/  
total 0  
[guest@smakopyan ~]$ lsattr /home/guest/dir1/  
[guest@smakopyan ~]$ lsattr /home/guest/dir1  
[guest@smakopyan ~]$ chmod 000 dir1  
[guest@smakopyan ~]$
```

Рис. 10: рисунок 10

Выполнение лабораторной работы

10. 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 (так как на предыдущем этапе сняли все атрибуты с директории)? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой (файл не создавался)

```
guest@smakopyan:~  
thentication.  
[guest@smakopyan ~]$ ls -l /home/guest/  
total 0  
drwxr-xr-x. 2 guest guest 6 Feb 28 18:05 dir1  
[guest@smakopyan ~]$ ls -l /home/guest/dir1  
total 0  
[guest@smakopyan ~]$ ls -l /home/guest/dir1/  
total 0  
[guest@smakopyan ~]$ lsattr /home/guest/dir1/  
[guest@smakopyan ~]$ lsattr /home/guest/dir1  
[guest@smakopyan ~]$ chmod 000 dir1  
[guest@smakopyan ~]$ ls -l  
total 0  
d-----, 2 guest guest 6 Feb 28 18:05 dir1  
[guest@smakopyan ~]$ ls -l /home/guest/dir1/  
ls: cannot open directory '/home/guest/dir1/': Permission denied  
[guest@smakopyan ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied  
[guest@smakopyan ~]$ echo "test" > /home/guest/dir1/file1  
-bash: /home/guest/dir1/file1: Permission denied  
[guest@smakopyan ~]$ ls -l /home/guest/dir1  
ls: cannot open directory '/home/guest/dir1': Permission denied  
[guest@smakopyan ~]$
```

В результате 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