

Защита лабораторной работы №2

Информационная безопасность

Докладчик

Петрова Мария Евгеньевна



Студентка группы НФИбд-02-21



Студ. билет 1032216450



Российский университет дружбы народов

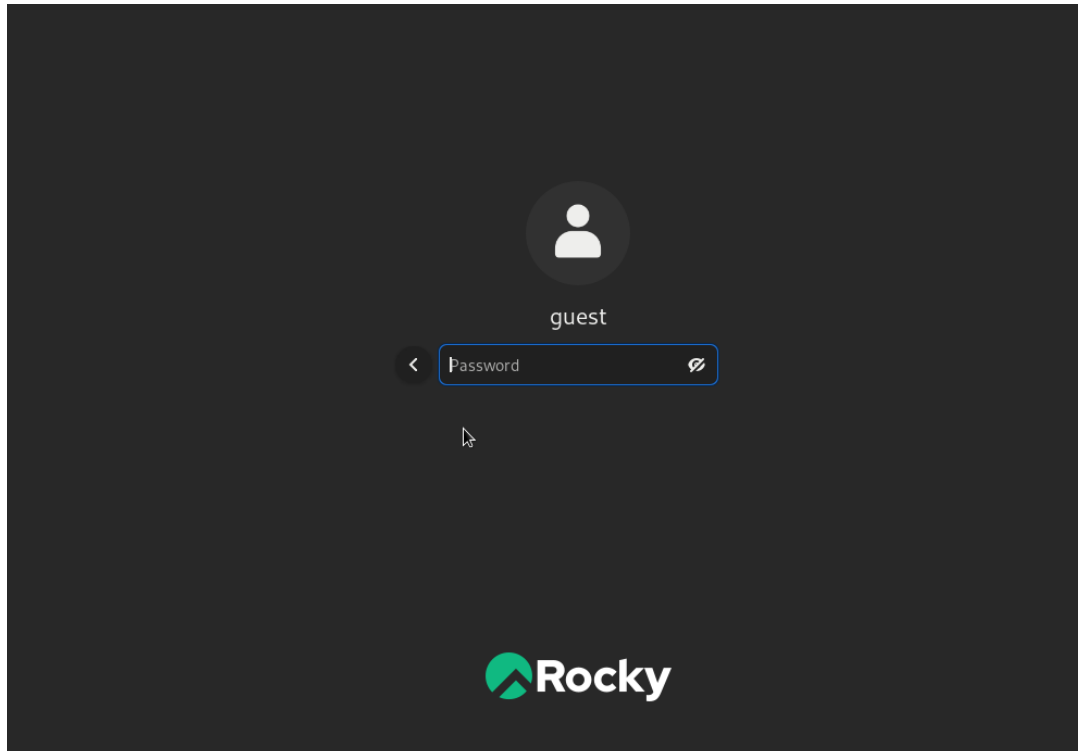
Цель лабораторной работы

- 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[1].

Теоретическое введение

- Программа VirtualBox предоставляет широкий спектр возможностей для работы с виртуальными машинами. Это решение подходит для тестирования новых операционных систем, запуска старых приложений или изоляции потенциально опасного программного обеспечения. Благодаря интуитивно понятному интерфейсу и богатому функционалу, VirtualBox стал выбором многих пользователей по всему миру.

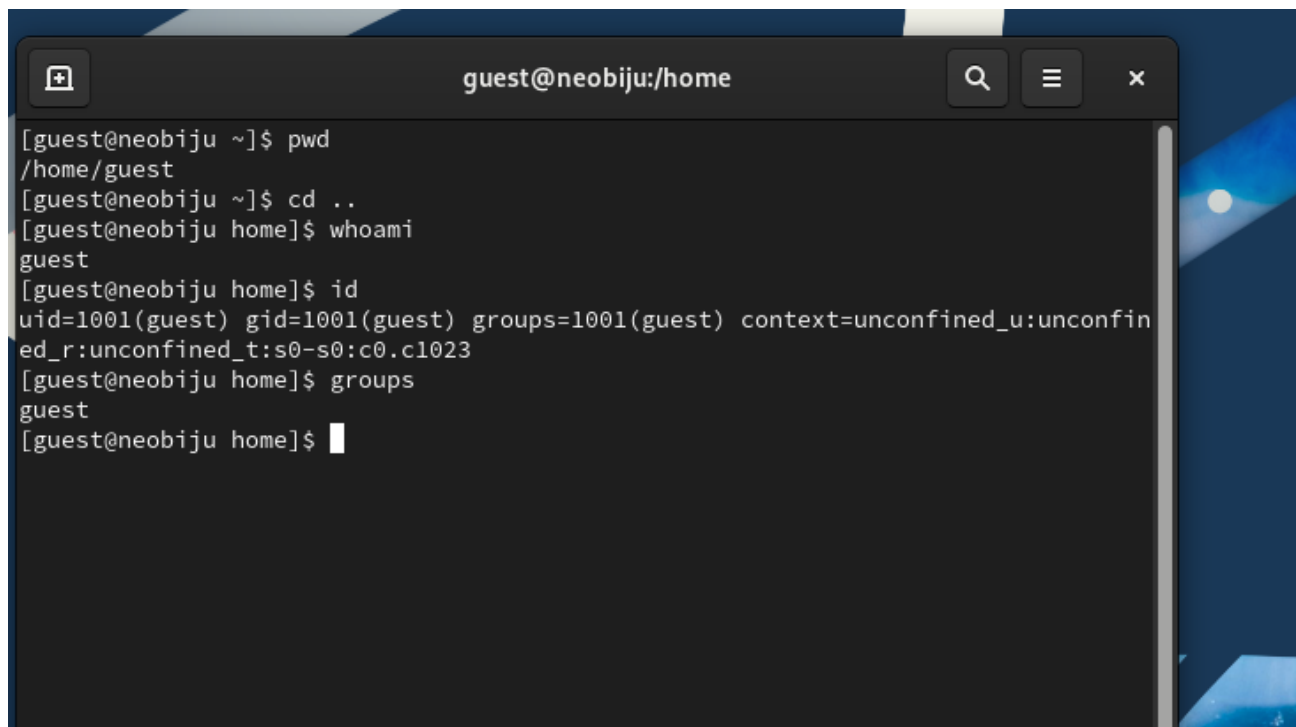
В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора):



```
root@neobiju:~  
[neobiju@neobiju ~]$ useradd guest  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[neobiju@neobiju ~]$ su -  
Password:  
[root@neobiju ~]# useradd guest  
[root@neobiju ~]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@neobiju ~]#
```

Учетная запись guest

*Домашняя директория И Проверка имени пользователя
Также Команды id, groups и Сравнение имени пользователя*



```
guest@neobiju:/home
[guest@neobiju ~]$ pwd
/home/guest
[guest@neobiju ~]$ cd ..
[guest@neobiju home]$ whoami
guest
[guest@neobiju home]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@neobiju home]$ groups
guest
[guest@neobiju home]$
```

```
[guest@neobiju home]$ groups
guest
[guest@neobiju home]$ 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:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
neobiju:x:1000:1000:neobiju:/home/neobiju:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@neobiju home]$
```

guest@neobiju:~

```
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
neobiju:x:1000:1000:neobiju:/home/neobiju:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@neobiju home]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@neobiju home]$ ls -l /home/
total 8
drwx-----. 14 guest  guest  4096 Sep 14 15:29 guest
drwx-----. 14 neobiju neobiju 4096 Sep  7 17:57 neobiju
[guest@neobiju home]$ lsattr /home
lsattr: Permission denied While reading flags on /home/neobiju
----- /home/guest
[guest@neobiju home]$ cd guest
[guest@neobiju ~]$ mkdir dir1
[guest@neobiju ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 14 15:49 dir1
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Music
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Public
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Videos
[guest@neobiju ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@neobiju ~]$
```


Снятие атрибутов с директории dir1

```
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Music
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Public
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 15:29 Videos
[guest@neobiju ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@neobiju ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@neobiju ~]$
```

Вывод

- Получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

