

Лабораторная работа №2

Дисциплина - основы информационной безопасности

Пронякова О.М.

24 февраля 2024

Российский университет дружбы народов, Москва, Россия

Информация

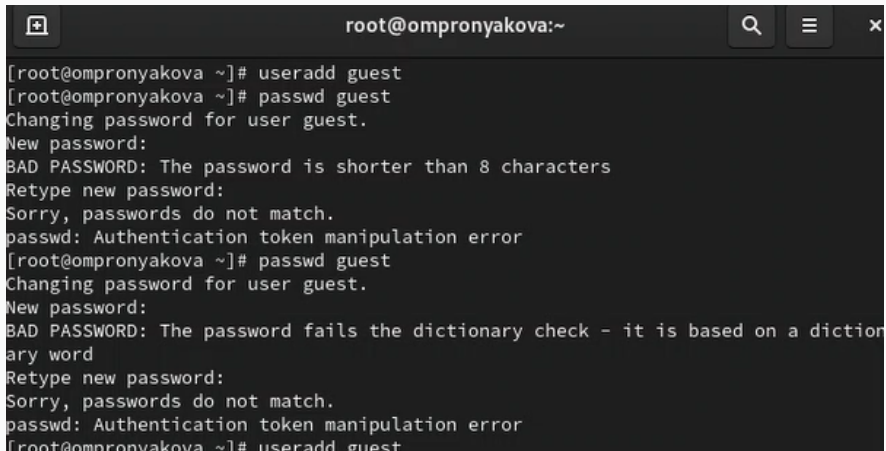
- Пронякова Ольга Максимовна
- студент НКАбд-02-22
- факультет физико-математических и естественных наук
- Российский университет дружбы народов

Создание презентации

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

Этапы выполнения работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создаю учётную запись пользователя guest: `useradd guest`. Далее задаю пароль для пользователя guest: `passwd guest`(рис.1).



```
root@ompronyakova:~  
[root@ompronyakova ~]# useradd guest  
[root@ompronyakova ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
[root@ompronyakova ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
[root@ompronyakova ~]# useradd guest
```

Этапы выполнения работы

Вхожу в систему от имени пользователя guest. Определяю директорию, в которой нахожусь, командой `pwd`. Определяю, является ли она домашней директорией? Уточняю имя моего пользователя командой `whoami` и его группу, а также группы, куда входит пользователь, командой `id` (рис.2), (рис.3).

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

```
ompronyakova.localdomain
[guest@ompronyakova ~]$ hostnamectl
Static hostname: ompronyakova.localdomain
Icon name: computer-vm
Chassis: vm 01F 5B4 I
Machine ID: 6f2f1c15257c446abd9eaaa856cdbbc78
Boot ID: b8f9510d08304ecd9f2017329f49825f
Virtualization: oracle
Operating System: Rocky Linux 9.3 (Blue Onyx)
CPE OS Name: cpe:/o:rocky:rocky:9::baseos
Kernel: Linux 5.14.0-362.18.1.el9_3.x86_64
Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
[guest@ompronyakova ~]$
```


Этапы выполнения работы

Просматриваю файл /etc/passwd командой `cat /etc/passwd`. Нахожу в нём свою учётную запись. Определяю uid пользователя. Определяю gid пользователя(рис.4).

```
[guest@ompronyakova ~]$ 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
```

Этапы выполнения работы

Определяю существующие в системе директории командой `ls -l /home/` Проверяю какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` Создаю в домашней директории поддиректорию `dir1` командой `mkdir dir1` Определяю командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`(рис.5).

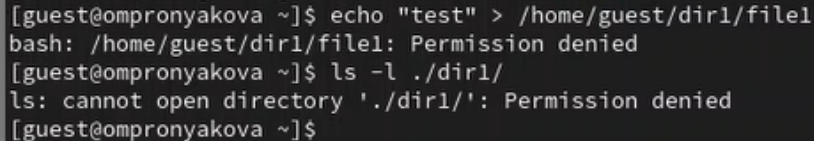
```
gnome-initial-setup:x:980:979:./run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
ompronyakova:x:1000:1000:ompronyakova:/home/ompronyakova:/bin/bash
vboxadd:x:977:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@ompronyakova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:./home/guest:/bin/bash
[guest@ompronyakova ~]$ ls /home/
guest  ompronyakova
[guest@ompronyakova ~]$ ls -l /home/
total 8
```

Этапы выполнения работы

Снимаю с директории dir1 все атрибуты командой `chmod 000 dir1` и проверяю с её помощью правильность выполнения команды `ls -l`(рис.6).

```
[guest@ompronyakova ~]$ chmod 000 dir1
[guest@ompronyakova ~]$ chmod 000 dir1/
[guest@ompronyakova ~]$ ls -l ./ grep dir1
ls: cannot access 'grep': No such file or directory
./:
total 0
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Desktop
d------. 2 guest guest 6 Feb 24 18:21 dir1
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Documents
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Music
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Public
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Templates
```

Создаю в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` Проверяю командой `ls -l /home/guest/dir1`(рис.7).

A terminal window with a dark background and light-colored text. The text shows a user named 'guest' at a machine named 'ompronyakova' in the home directory '~'. The user attempts to create a file 'file1' in the directory '/home/guest/dir1' using the command 'echo "test" > /home/guest/dir1/file1'. The terminal returns the error 'bash: /home/guest/dir1/file1: Permission denied'. The user then attempts to list the contents of the directory using 'ls -l ./dir1/'. The terminal returns the error 'ls: cannot open directory './dir1/': Permission denied'. The prompt returns to the user's home directory.

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

Рис. 7: Снятие с директории атрибутов

Заполняю таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заношу в таблицу знак «+», если не разрешена, знак «-». На основании заполненной таблицы определяю те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполняю таблицу(рис.8), (рис.9).

Этапы выполнения работы

Liberation Sans 10 pt B I U											
O8											
You are running version 7.1 of LibreOffice for the first time. Do you want to learn what's new?											
	A	B	C	D	E	F	G	H	I	J	
1	Права директории	Права файла	Создание файла	Удаление файла	Запись в файле	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла	
2	0	0	-	-	-	-	-	-	+	-	
3	100	0	-	-	-	-	-	-	-	-	
4	200	0	-	-	-	-	-	-	-	-	
5	300	0	+	+	-	-	+	+	-	-	
6	400	0	-	-	-	-	+	-	-	-	
7	500	0	-	-	-	-	-	+	+	+	
8	600	0	-	-	-	-	-	-	-	+	
9	700	0	-	-	-	-	-	+	-	+	
10	0	100	+	+	-	-	+	-	-	-	
11	100	100	-	-	-	-	-	-	-	-	
12	200	100	-	-	-	-	-	+	-	-	
13	300	100	-	-	-	-	-	-	-	+	
14	400	100	+	+	-	-	-	-	-	-	
15	500	100	-	-	-	-	-	-	-	-	
16	600	100	-	-	-	-	-	-	-	-	
17	700	100	-	-	-	-	-	-	-	-	
18	0	200	+	+	-	-	-	-	-	-	
19	100	200	-	-	+	+	+	+	+	+	
20	200	200	-	-	-	-	-	-	-	-	
21	300	200	-	-	+	+	+	+	-	-	
22	400	200	+	+	-	-	-	-	-	-	
23	500	200	-	-	+	+	+	+	+	+	
24	600	200	-	-	-	-	-	-	-	-	
25	700	200	-	-	+	+	+	+	+	+	
26	0	300	+	+	-	-	-	-	-	-	
27	100	300	-	-	-	-	-	-	-	-	
28	200	300	-	-	-	-	-	-	-	-	
29	300	300	-	-	-	-	-	-	-	-	
30	400	300	+	+	+	+	-	+	+	+	
31	500	300	-	-	-	-	+	-	-	-	
32	600	300	-	-	-	-	+	-	-	-	
33	700	300	-	-	-	-	-	-	-	-	
34	0	400	+	+	-	-	-	-	+	-	
35	100	400	-	-	-	-	-	-	-	+	
36	200	400	-	-	-	-	-	-	-	-	
37	300	400	-	-	-	-	-	-	-	-	
38	400	400	+	+	+	+	+	+	+	+	

L	M	N	O	P
	Оперция	Минимальные права на директорию	Минимальные права на файл	
	Создание файла	300	0	
	Удаление файла	300	0	
	Чтение файла	100	400	
	Запись в файл	100	200	
	Переименование файла	300	0	
	Создание поддиректории	300	0	
	Удаление поддиректории	300	0	

Рис. 9: Определение минимально необходимых прав для выполнения операций внутри директории

Получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.