Основы информационной безопасности

Лабораторная работа № 2

Оразгелдиев Язгелди

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

::::::::::::::: {.columns align=center} ::: {.column width="70%"}

- Оразгелдиев Язгелди
- студент 2-го курса
- Российский университет дружбы народов
- orazgeldiyev.yazgeldi@gmail.com
- https://YazgeldiOrazgeldiyev.github.io/ru/

Актуальность

- Работа в консоли Линукс очень важна для дальнейшей практики

Цели и задачи

- 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

Материалы и методы

- Операционная система Linux
- RedHat

1. Создали гостевую дополнительную учетную запись и входим в виртуальную машину от его имени.

```
[yazgeldi_o@localhost ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[yazgeldi_o@localhost ~]$ sudo useradd guest
[sudo] password for yazgeldi_o:
[yazgeldi_o@localhost ~]$ passwd guest
passwd: Only root can specify a user name.
[yazgeldi_o@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[yazgeldi_o@localhost ~]$
```

Рис. 1: Создание учетной записи guest

2. Мы в новой учетной записи прописали некоторые команды для того, чтобы вывести информацию о пользователе guest

```
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whami
bash: whami: command not found...
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:
s0-s0:c0.c1023
[guest@localhost ~]$ 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
```

3. Определили uid, gid пользователя и сравниваем с предыдущими пунктами

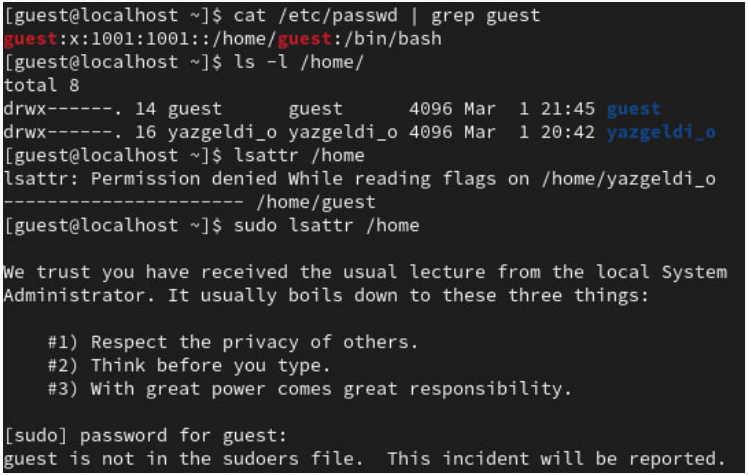

Рис. 3: id, gid пользователя

4. Создали поддиректорию dirl

```
[guest@localhost ~]$ mkdir dirl
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Desktop
drwxr-xr-x. 2 guest guest 6 Mar  1 21:50 dirl
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Documents
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Downloads
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Music
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Pictures
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Public
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Templates
drwxr-xr-x. 2 guest guest 6 Mar  1 21:45 Videos
[guest@localhost ~]$ lsattr
---------------------- ./Desktop
---------------------- ./Downloads
---------------------- ./Templates
---------------------- ./Public
---------------------- ./Documents
---------------------- ./Music
---------------------- ./Pictures
---------------------- ./Videos
---------------------- ./dirl
```

5. Тестировали на поддиректории различные команды и изменяем права доступа. Проверяли работу команд

```
[guest@localhost ~]$ echo "test" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Permission denied
[guest@localhost ~]$ ;s dirl
bash: syntax error near unexpected token `;'
[guest@localhost ~]$ ls dirl
ls: cannot open directory 'dirl': Permission denied
[guest@localhost ~]$ rm dirl/test
rm: cannot remove 'dirl/test': Permission denied
[guest@localhost ~]$ echo "test" > test
[guest@localhost ~]$ echo "test" > dirl/test
bash: dirl/test: Permission denied
[guest@localhost ~]$ cat dirl/test
cat: dirl/test: Permission denied
[guest@localhost ~]$ mv dirl/test ~
mv: cannot stat 'dirl/test': Permission denied
[guest@localhost ~]$ ls -l dirl
ls: cannot open directory 'dirl': Permission denied
[guest@localhost ~]$ mv dirl/test dirl/test10
mv: failed to access 'dirl/test10': Permission denied
[guest@localhost ~]$ chmod 100 dir/test
chmod: cannot access 'dir/test': No such file or directory
```

6. Заполняли таблицу, выполняя действия от имени владельца директорий

```
[guest@localhost ~]$ mv dirl/test dirl/test10
mv: failed to access 'dirl/test10': Permission denied
[guest@localhost ~]$ chmod 100 dir/test
chmod: cannot access 'dir/test': No such file or directory
[guest@localhost ~]$ chmod 700 dirl
[guest@localhost ~]$ chmod 100 dirl/test
chmod: cannot access 'dirl/test': No such file or directory
[guest@localhost ~]$ chmod 000 dirl
[guest@localhost ~]$ chmod 000 dirl
[guest@localhost ~]$ rmdir dirl/b
rmdir: failed to remove 'dirl/b': Permission denied
[guest@localhost ~]$ chmod 100 dirl
[guest@localhost ~]$ rmdir dirl/b
```

Рис. 6: Команды для нашего dirl

Результаты

- 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

Итоговый слайд

- Лучше сделать сегодня хоть что-то, чем завтра ничего!