

Основы информационной безопасности

Лабораторная работа № 2. Дискреционное разграничение прав в Linux. Основные атрибуты

Подлесный Иван Сергеевич.

14.09.2024

Российский Университет дружбы народов

Информация

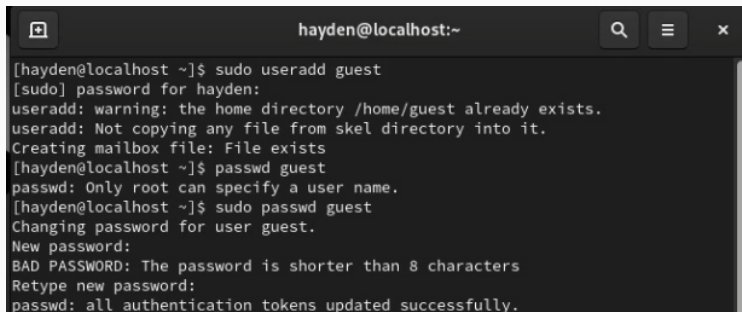
- Подлесный Иван Сергеевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов

Вводная часть

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 # Ход работы

Шаги 1-2

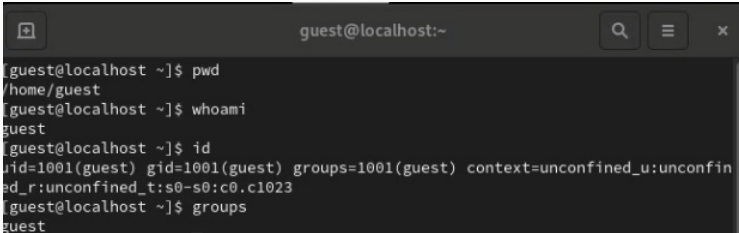
Выполняем шаги 1-2: - Создаем нового гостевого пользователя (guest) “sudo useradd guest” -
Задаём ему пароль “sudo passwd guest”

A terminal window titled 'hayden@localhost:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
[hayden@localhost ~]$ sudo useradd guest
[sudo] password for hayden:
useradd: warning: the home directory /home/guest already exists.
useradd: Not copying any file from skel directory into it.
Creating mailbox file: File exists
[hayden@localhost ~]$ passwd guest
passwd: Only root can specify a user name.
[hayden@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Figure 1: Шаги 1-2

- Входим в систему через пользователя guest
- Определяем директорию, в которой находится пользователь командой “pwd” и определяем является ли она домашней
- Директория является домашней
- Уточняем имя пользователя командой “whoami”
- Уточняем имя пользователя, его группу, а также группы, куда входит пользователь, командой id, потом сравниваем вывод id с выводом команды groups.



```
guest@localhost:~  
[guest@localhost ~]$ pwd  
/home/guest  
[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 ~]$ groups  
guest
```

Figure 2: Шаги 3-7

- Просматриваем файл `/etc/passwd` командой `cat /etc/passwd` и находим в нём свою учётную запись. Определяем `uid` пользователя и `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Данные `uid` и `gid` пользователя `guest` никак не различаются.

Выполняем шаг 8:

```
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:987:987: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
hayden:x:1000:1000:Hayden:/home/hayden:/bin/bash
vboxadd:x:979:1:/:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@localhost ~]$
```

Figure 3: Шаг 8

- Определите существующие в системе директории командой `ls -l /home/` Удалось получить список поддиректорий директории `/home`. На каждой директории установлены права на чтение, запись и исполнение, но только для владельцев(не включая группы и остальных пользователей).

```
[guest@localhost ~]$ ls -l /home/  
total 8  
drwx-----. 14 guest  guest  4096 Sep 14 00:02 guest  
drwx-----. 14 hayden hayden 4096 Sep 13 23:56 hayden
```

Figure 4: Шаг 9

- Проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой “lsattr /home”. Удалось увидеть расширенные атрибуты только своей директорий
- Создаем в домашней директории поддиректорию dir1 командой “mkdir dir1” Определяем командами ls -l и lsattr, и просматриваем права доступа и атрибуты (Владелец – чтение,исполнение,запись. Группа – чтение и исполнение. Остальные – чтение)

Выполняем шаги 10-11

```
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/hayden
----- /home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 14 00:10 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Videos
```

Figure 5: Шаги 10-11

Выполняем шаг 12

- Снимаем с директории dir1 все атрибуты командой “chmod 000 dir1” и проверяем правильность выполнения с помощью команды “ls -l”

```
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Desktop
d------. 2 guest guest 6 Sep 14 00:10 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 23:46 Videos
```

Figure 6: Шаг 12

Попытался создать в директории dir1 файл file1 командой “echo”test” > /home/guest/dir1 file1”
Отказ был получен так как, мы поменяли атрибуты на те, которые не позволяют проводить с папкой операцию чтения и записи.

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

Figure 7: Шаг 13

Шаг 14:

Таблица минимальных прав доступа на совершения действий с файлами и папками

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переимено- вание файла	d(300)	(000)

Заключение

Мы 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