

Дискреционное разграничение прав в Linux. Основные атрибуты

Даниил Бузин¹

8 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

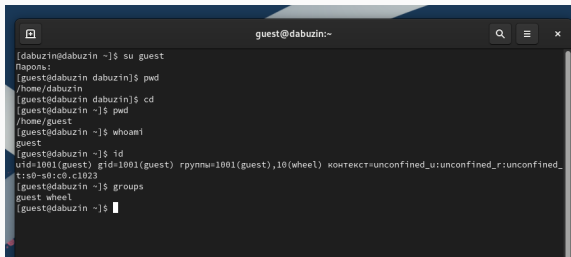
Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

Определяем UID и группу

A terminal window titled 'guest@dabuzin:~' with search, menu, and close icons in the title bar. The terminal shows a sequence of commands and their outputs: 'su guest' switches to the 'guest' user; 'pwd' shows the home directory '/home/dabuzin'; 'cd' changes to the user's home directory; another 'pwd' confirms the path '/home/guest'; 'whoami' returns 'guest'; and 'id' displays the user's identity: 'uid=1001(guest) gid=1001(guest) rpyнны=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_'. Finally, 'groups' lists the groups 'guest' and 'wheel'.

```
guest@dabuzin:~  
[dabuzin@dabuzin ~]$ su guest  
Наpons:  
[guest@dabuzin dabuzin]$ pwd  
/home/dabuzin  
[guest@dabuzin dabuzin]$ cd  
[guest@dabuzin ~]$ pwd  
/home/guest  
[guest@dabuzin ~]$ whoami  
guest  
[guest@dabuzin ~]$ id  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_  
t:s0-s0:c0.c1023  
[guest@dabuzin ~]$ groups  
guest wheel  
[guest@dabuzin ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
sssd:x:991:991:User for sssd:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire/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:/dev/null/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/sbin/nologin
gdm:x:42:42:/var/lib/gdm/sbin/nologin
gnome-initial-setup:x:981:980:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
guest:x:1001:1001:guest:/home/guest/bin/bash
guest2:x:1002:1002:/home/guest2/bin/bash
dabuzin:x:1003:1003:/home/dabuzin/bin/bash
[guest@dabuzin ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@dabuzin ~]$  
[guest@dabuzin ~]$ ls -l /home  
итого 8  
drwx-----, 14 dabuzin dabuzin 4096 сен  8 13:12 dabuzin  
drwx-----, 14 guest  guest  4096 сен  8 14:07 guest  
drwx-----,  3 guest2  guest2   78 сен 17 2023 guest2  
[guest@dabuzin ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@dabuzin ~]$ cd
[guest@dabuzin ~]$ mkdir dir1
[guest@dabuzin ~]$ ls -l | grep dir1
drwxr-xr-x. 2 guest guest 6 сен  8 14:08 dir1
[guest@dabuzin ~]$ chmod 000 dir1
[guest@dabuzin ~]$ ls -l | grep dir1
d----- . 2 guest guest 6 сен  8 14:08 dir1
[guest@dabuzin ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@dabuzin ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@dabuzin ~]$
```

Figure 4: Снятие атрибутов с директории

Права и разрешённые действия

| Операция | Права на директорию | Права на файл |
|------------------------|---------------------|----------------|
| Создание файла | d-wx----- (300) | ----- (000) |
| Удаление файла | d-wx----- (300) | ----- (000) |
| Чтение файла | d--x----- (100) | -r----- (400) |
| Запись в файл | d--x----- (100) | --w----- (200) |
| Переименование файла | d-wx----- (300) | ----- (000) |
| Создание поддиректории | d-wx----- (300) | ----- (000) |
| Удаление поддиректории | d-wx----- (300) | ----- (000) |

Figure 5: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.