

Дискреционное разграничение прав в Linux. Основные атрибуты

Хамзат Межидов ¹

11 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

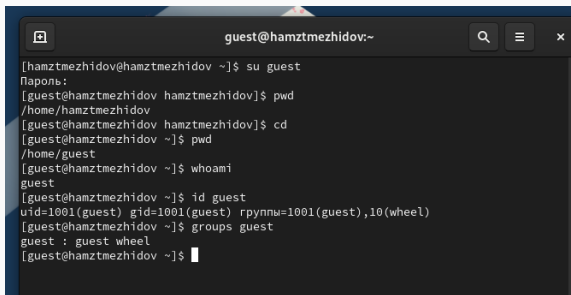
Цели и задачи работы

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

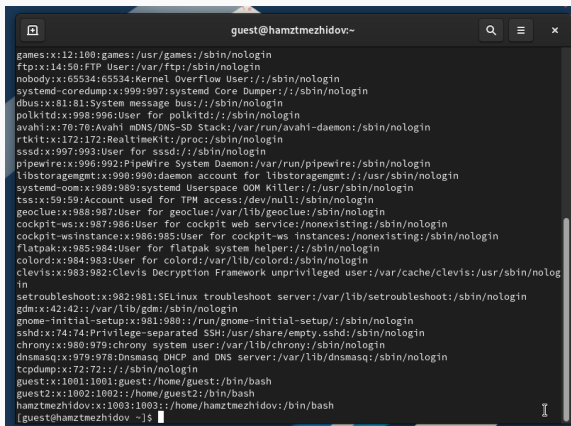
Определяем UID и группу

A terminal window titled 'guest@hamztmezhidov:~' with search, menu, and close buttons. The terminal shows a sequence of commands and their outputs to identify the 'guest' user. The commands include 'su guest', 'pwd', 'cd', 'whoami', and 'id guest'. The output of 'id guest' shows 'uid=1001(guest) gid=1001(guest) rpyнны=1001(guest),10(wheel)'. The 'groups guest' command shows 'guest : guest wheel'.

```
guest@hamztmezhidov:~  
[hamztmezhidov@hamztmezhidov ~]$ su guest  
Пароль:  
[guest@hamztmezhidov hamztmezhidov]$ pwd  
/home/hamztmezhidov  
[guest@hamztmezhidov hamztmezhidov]$ cd  
[guest@hamztmezhidov ~]$ pwd  
/home/guest  
[guest@hamztmezhidov ~]$ whoami  
guest  
[guest@hamztmezhidov ~]$ id guest  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest),10(wheel)  
[guest@hamztmezhidov ~]$ groups guest  
guest : guest wheel  
[guest@hamztmezhidov ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@hamtmezhidov:~' displays the output of the 'cat /etc/passwd' command. The window has a dark background with a search icon, a menu icon, and a close icon in the top right corner. The text is white and lists system and regular users with their IDs, names, and home directories. The prompt '[guest@hamtmezhidov ~]\$' is visible at the bottom.

```
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
sssd:x:997:993: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
hamtmezhidov:x:1003:1003:/:/home/hamtmezhidov:/bin/bash
[guest@hamtmezhidov ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@hamztmezhidov ~]$  
[guest@hamztmezhidov ~]$ ls -l /home  
иторо 8  
drwx-----, 14 guest      guest      4096 сен 11 11:19 guest  
drwx-----,  3 guest2     guest2      78 сен 17  2023 guest2  
drwx-----, 14 hamztmezhidov hamztmezhidov 4096 сен 11 11:09 hamztmezhidov  
[guest@hamztmezhidov ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@hamztmezhidov ~]$  
[guest@hamztmezhidov ~]$ cd  
[guest@hamztmezhidov ~]$ mkdir dir1  
[guest@hamztmezhidov ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 сен 11 11:22 dir1  
[guest@hamztmezhidov ~]$ chmod 000 dir1  
[guest@hamztmezhidov ~]$ ls -l | grep dir1  
d------. 2 guest guest 6 сен 11 11:22 dir1  
[guest@hamztmezhidov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@hamztmezhidov ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@hamztmezhidov ~]$
```

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.