

Дискреционное разграничение прав в Linux. Основные атрибуты

Ким Реачна¹

12 сентября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

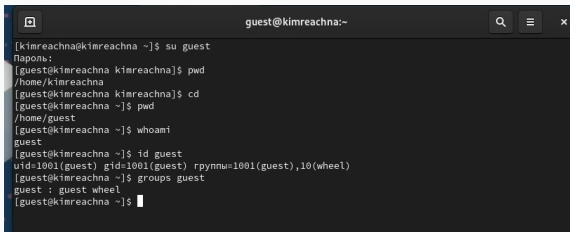
Цели и задачи работы

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

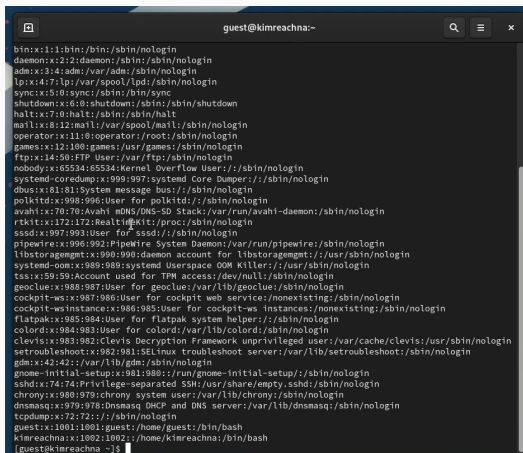
Определяем UID и группу

A terminal window titled 'guest@kimreachna:~' with search, menu, and close icons. It shows a sequence of commands and their outputs to determine the user 'guest's details. The commands and outputs are: 'su guest' (password prompt), 'pwd' (returns /home/kimreachna), 'cd' (returns /home/guest), 'whoami' (returns guest), 'id guest' (returns uid=1001(guest) gid=1001(guest) rгруппы=1001(guest),10(wheel)), and 'groups guest' (returns guest : guest wheel).

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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@kimreachna:~' displays the contents of the /etc/passwd file. The output is a list of system and user accounts, each on a new line, showing their username, UID, GID, and home directory/shell path. The window has a search icon, a menu icon, and a close icon in the top right corner. The prompt at the bottom is '[guest@kimreachna ~]\$' with a cursor.

```
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
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
tsix: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 Encryption 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
kimreachna:x:1002:1002:/home/kimreachna:/bin/bash
[guest@kimreachna ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@kimreachna ~]$  
[guest@kimreachna ~]$ ls -l /home  
итого 8  
drwx-----. 14 guest      guest      4096 сен 12 12:26 guest  
drwx-----. 14 kimreachna kimreachna 4096 сен 12 12:25 kimreachna  
[guest@kimreachna ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@kimreachna ~]$ cd
[guest@kimreachna ~]$ mkdir dir1
[guest@kimreachna ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 12 12:35 dir1
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Видео
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Документы
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Изображения
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Музыка
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Шаблоны
[guest@kimreachna ~]$ chmod 000 dir1
[guest@kimreachna ~]$ ls -l dir1/
ls: невозможно открыть каталог 'dir1/': Отказано в доступе
[guest@kimreachna ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@kimreachna ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@kimreachna ~]$
```

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.