

Дискреционное разграничение прав в Linux. Основные атрибуты

Филиппова Екатерина¹

7 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

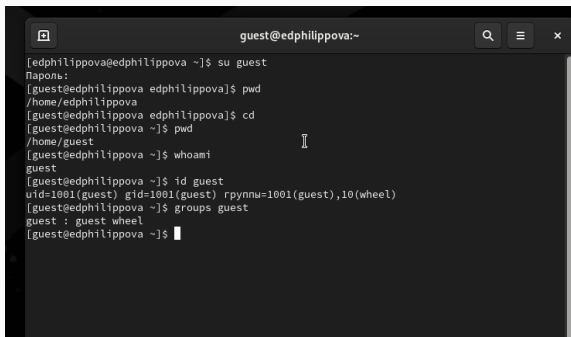
Цели и задачи работы

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

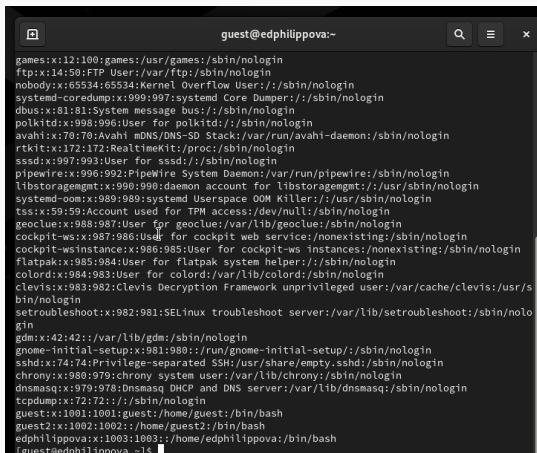
Определяем UID и группу

A terminal window titled 'guest@edphilippova:~' with search, menu, and close icons. It shows a sequence of commands to switch to the 'guest' user and view their details. The output shows the user's home directory, current directory, and identity (UID 1001, GID 1001, primary group rpynnw, secondary group wheel).

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

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar shows 'guest@edphilippova:~'. The terminal displays the output of a command that lists the contents of the /etc/passwd file. Each line represents a system or user account, showing the username, UID, GID, and shell path. The accounts listed include games, ftp, nobody, systemd-coredump, dbus, polkitd, avahi, rtkit, sssd, pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, guest, guest2, and edphilippova. The prompt at the bottom is 'guest@edphilippova ~\$'.

```
guest@edphilippova:~  
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/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/s  
bin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nolo  
gin  
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  
edphilippova:x:1003:1003:/home/edphilippova:/bin/bash  
guest@edphilippova ~$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@edphilippova ~]$  
[guest@edphilippova ~]$ ls -l /home  
итого 8  
drwx-----, 14 edphilippova edphilippova 4096 сен  7 17:18 edphilippova  
drwx-----, 14 guest      guest      4096 сен  7 17:21 guest  
drwx-----,  3 guest2     guest2     78 сен 17  2023 guest2  
[guest@edphilippova ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
drwxr-xr-x. 2 guest guest 6 сен 7 17:31 dir1
[guest@edphilippova ~]$
[guest@edphilippova ~]$
[guest@edphilippova ~]$ cd
[guest@edphilippova ~]$ mkdir dir1
[guest@edphilippova ~]$ ls -l | grep dir1
drwxr-xr-x. 2 guest guest 6 сен 7 17:31 dir1
[guest@edphilippova ~]$ chmod 000 dir1/
[guest@edphilippova ~]$ ls -l | grep dir1
d------. 2 guest guest 6 сен 7 17:31 dir1
[guest@edphilippova ~]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@edphilippova ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@edphilippova ~]$
```

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.