

Дискреционное разграничение прав в Linux. Основные атрибуты

Кальсин Захар¹

5 ноября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

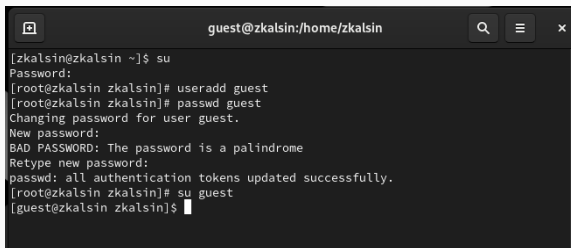
Цели и задачи работы

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 with a dark background and light text. The title bar shows 'guest@zkalsin:/home/zkalsin'. The terminal content shows a sequence of commands and their outputs: a user switches to root via 'su', then uses 'useradd guest' to create a user, 'passwd guest' to set a password, and 'su guest' to switch back to the 'guest' user. The password '12345678' is entered twice, with a warning that it is a palindrome. The terminal ends with the 'guest@zkalsin zkalsin\$' prompt.

```
guest@zkalsin:/home/zkalsin
[zkalsin@zkalsin ~]$ su
Password:
[root@zkalsin zkalsin]# useradd guest
[root@zkalsin zkalsin]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@zkalsin zkalsin]# su guest
[guest@zkalsin zkalsin]$
```

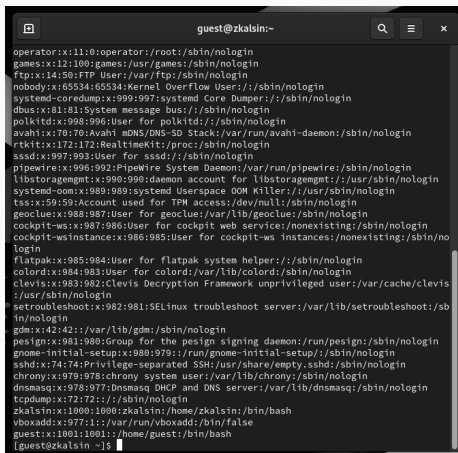
Figure 1: Информация о пользователе guest

Файл с данными о пользователях

```
[guest@zkalsin ~]$ pwd
/home/zkalsin
[guest@zkalsin zkalsin]$ cd
[guest@zkalsin ~]$ pwd
/home/guest
[guest@zkalsin ~]$ whoami
guest
[guest@zkalsin ~]$ id guest
uid=1001(guest) gid=1001(guest) groups=1001(guest)
[guest@zkalsin ~]$ groups guest
guest : guest
[guest@zkalsin ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

A terminal window titled 'guest@zkalsin:~' displays the contents of the /etc/passwd file. The output lists system users like operator, 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, design, gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, and regular users zkalsin, vboxadd, and guest, each with their UID, GID, name, and home directory or shell path.

```
guest@zkalsin:~  
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  
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  
design:x:981:980:Group for the design signing daemon:/run/design:/sbin/nologin  
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin  
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin  
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
tcpdump:x:72:72:/sbin/nologin  
zkalsin:x:1000:1000:zkalsin:/home/zkalsin:/bin/bash  
vboxadd:x:977:1:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@zkalsin ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@zkalsin ~]$  
[guest@zkalsin ~]$ ls -l /home  
total 4  
drwx-----, 3 guest  guest    78 Nov  5 21:27 guest  
drwx-----, 19 zkalsin zkalsin 4096 Nov  5 21:21 zkalsin  
[guest@zkalsin ~]$
```

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.