

Дискреционное разграничение прав в Linux. Основные атрибуты

Хайдари Ахмад Насир¹

9 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

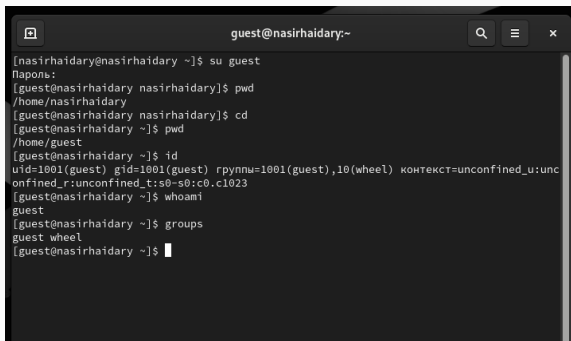
Цели и задачи работы

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

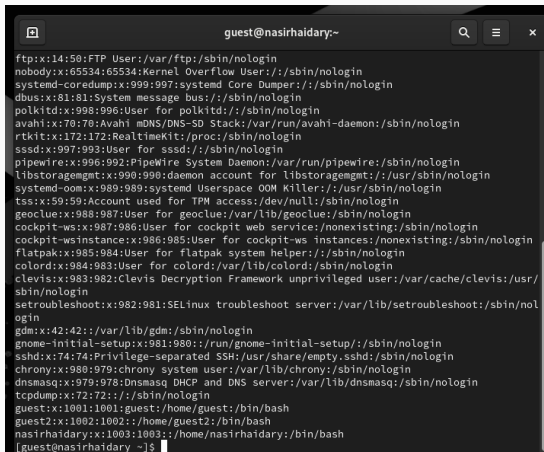
Определяем UID и группу

A terminal window titled 'guest@nasirhaidary:~' with search, menu, and close icons. It shows a sequence of commands and their outputs to determine the user's identity. The commands are: 'su guest', 'pwd', 'cd', 'pwd', 'id', 'whoami', and 'groups'. The output of 'id' provides detailed information about the user's UID, GID, group memberships, and SELinux context.

```
[nasirhaidary@nasirhaidary ~]$ su guest
Пароль:
[guest@nasirhaidary nasirhaidary]$ pwd
/home/nasirhaidary
[guest@nasirhaidary nasirhaidary]$ cd
[guest@nasirhaidary ~]$ pwd
/home/guest
[guest@nasirhaidary ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@nasirhaidary ~]$ whoami
guest
[guest@nasirhaidary ~]$ groups
guest wheel
[guest@nasirhaidary ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@nasirhaidary:~' with a search icon, a hamburger menu icon, and a close icon in the top right corner. The terminal displays the output of the 'cat /etc/passwd' command, listing system users and regular users. The output is as follows:

```
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
nasirhaidary:x:1003:1003:/home/nasirhaidary:/bin/bash
[guest@nasirhaidary ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@nasirhaidary ~]$  
[guest@nasirhaidary ~]$ ls -l /home  
итого 8  
drwx-----. 15 guest      guest      4096 сен  9 18:19 guest  
drwx-----.  3 guest2     guest2     78 сен 17 2023 guest2  
drwx-----. 14 nasirhaidary nasirhaidary 4096 сен  9 18:07 nasirhaidary  
[guest@nasirhaidary ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@nasirhaidary ~]$  
[guest@nasirhaidary ~]$ cd  
[guest@nasirhaidary ~]$ mkdir dir1  
[guest@nasirhaidary ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 сен  9 18:19 dir1  
[guest@nasirhaidary ~]$ chmod 000 dir1/  
[guest@nasirhaidary ~]$ ls -l | grep dir1  
d------. 2 guest guest 6 сен  9 18:19 dir1  
[guest@nasirhaidary ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@nasirhaidary ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@nasirhaidary ~]$
```

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.