Презентация о выполнении лабораторной работы №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Евсеева Дарья Олеговна

8 октября, 2022

Российский Университет Дружбы Народов, Москва, Россия

Цель работы

Целью данной работы является изучение механизмов изменения идентификаторов и применения SetUID-, SetGID- и Sticky-битов, получение практических навыков работы в консоли с дополнительными атрибутами, рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Задачи выполнения

Необходимо выполнить следующие задачи:

1. Провести работу с SetUID- и SetGID-битами.
2. Провести работу со Sticky-битом.

Результаты выполнения

В ходе работы были выполнены поставленные задачи:

- Проведена работа с SetUID- и SetGID-битами

Figure 1: Вход в систему от имени пользователя guest

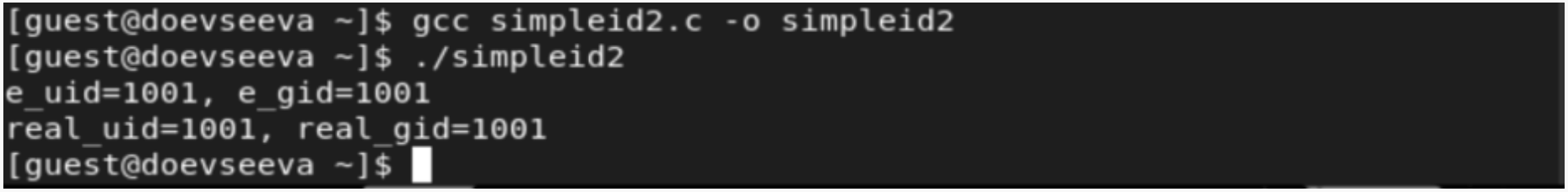

Figure 2: Результаты запуска программы вывода значений идентификаторов

Результаты выполнения

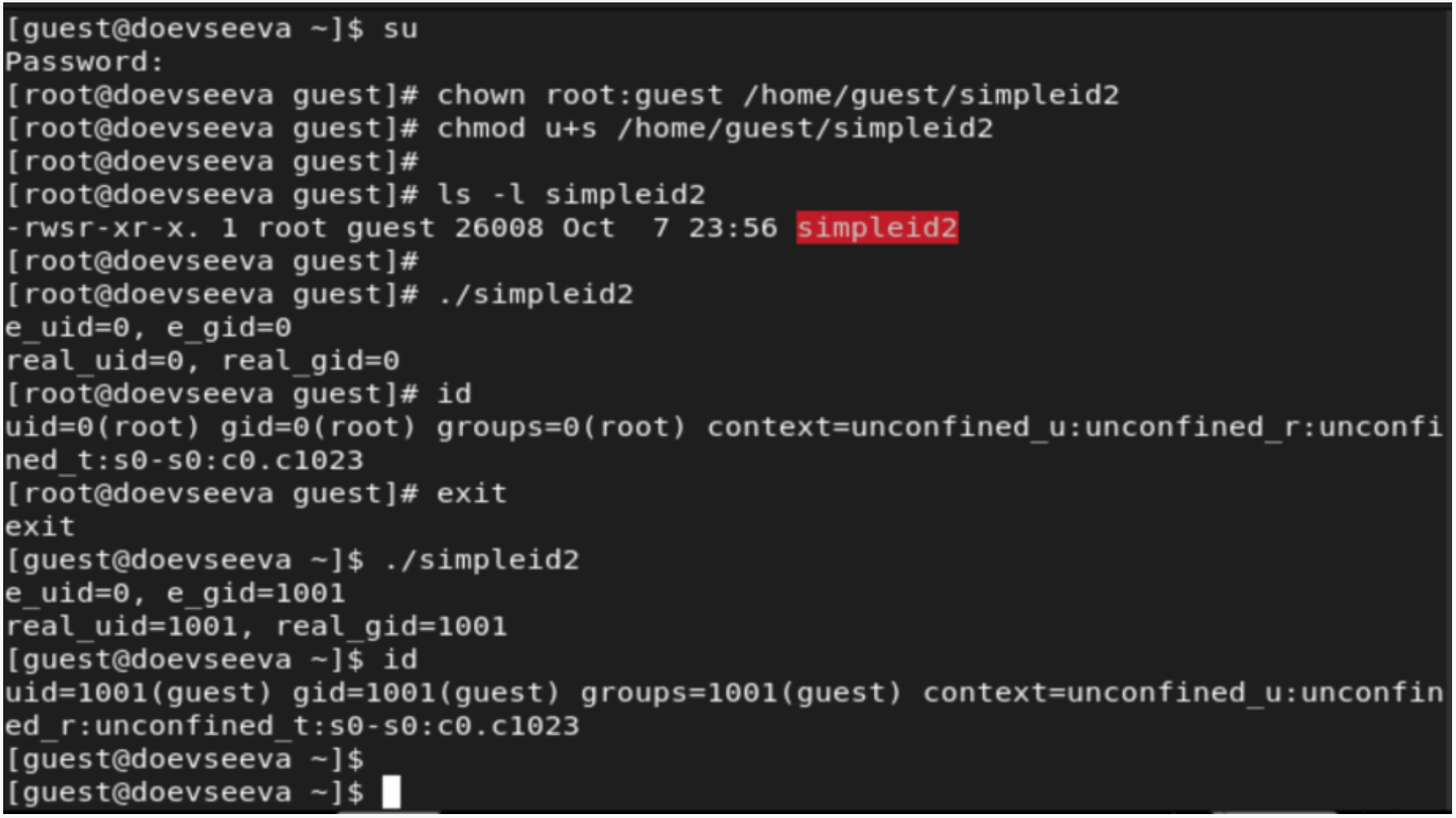

Figure 3: Установка атрибута s для пользователя

Результаты выполнения

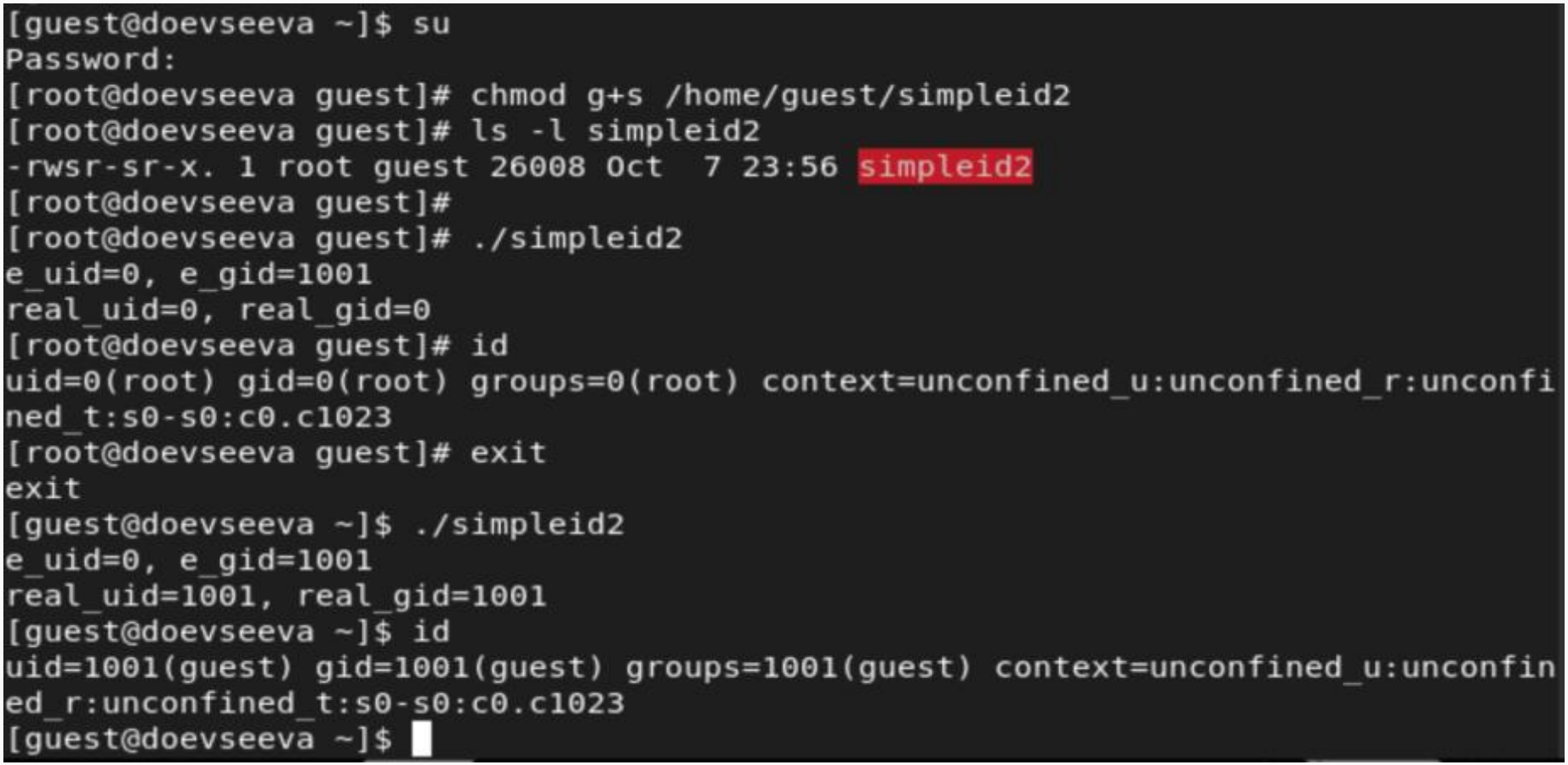

Figure 4: Установка атрибута s для группы

Результаты выполнения

```
[guest@doevseeva ~]$ su
Password:
[root@doevseeva guest]# chown root:root /home/guest/readfile.c
[root@doevseeva guest]# chmod o-r /home/guest/readfile.c
[root@doevseeva guest]# chmod g-r /home/guest/readfile.c
[root@doevseeva guest]# ls -l /home/guest/
total 96
drwxrwx---. 2 guest guest    19 Oct  7 23:20 dir1
-rwxr-xr-x. 1 guest guest 25952 Oct  8 00:12 readfile
-rw-------. 1 root  root    422 Oct  8 00:12 readfile.c
-rwxr-xr-x. 1 guest guest 25904 Oct  7 23:50 simpleid
-rwsr-sr-x. 1 root  guest 26008 Oct  7 23:56 simpleid2
-rw-r--r--. 1 guest guest   313 Oct  7 23:56 simpleid2.c
-rw-r--r--. 1 guest guest   181 Oct  7 23:50 simpleid.c
[root@doevseeva guest]#
[root@doevseeva guest]# exit
exit
[guest@doevseeva ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@doevseeva ~]$
```

Figure 5: Смена владельца файла и изменение прав

```
[guest@doevseeva ~]$ su
Password:
[root@doevseeva guest]# chown root /home/guest/readfile
[root@doevseeva guest]# chmod u+s /home/guest/readfile
[root@doevseeva guest]#
```

Figure 6: Смена владельца и установка SetUID-бита

Результаты выполнения

```
[root@doevseeva guest]# exit
exit
[guest@doevseeva ~]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

int main (int argc, char* argv[]) {
        unsigned char buffer[16];
        size_t bytes_read;
        int i;

        int fd = open (argv[1], O_RDONLY);
        do {
                bytes_read = read (fd, buffer, sizeof (buffer));
                for (i = 0; i < bytes_read; ++i)
                        printf("%c", buffer[i]);
        }
        while (bytes_read == sizeof (buffer));
        close (fd);
        return 0;
}
```

Figure 7: Чтение readfile.c от имени пользователя guest

Результаты выполнения

```
[guest@doevseeva ~]$ ./readfile /etc/shadow
root:$6$WBTn0LvqyZ30L6dS$vQtWyhTUOY9ABTAVak9ZDgcwlHWG03eq4/wi5KVUZVj5m9Lx9PDFGeb
D.n8UuzEOS8z9lS3lMvm4dh6C9QihF/::0:99999:7:::
bin:*:19123:0:99999:7:::
daemon:*:19123:0:99999:7:::
adm:*:19123:0:99999:7:::
lp:*:19123:0:99999:7:::
sync:*:19123:0:99999:7:::
shutdown:*:19123:0:99999:7:::
halt:*:19123:0:99999:7:::
mail:*:19123:0:99999:7:::
operator:*:19123:0:99999:7:::
games:*:19123:0:99999:7:::
ftp:*:19123:0:99999:7:::
nobody:*:19123:0:99999:7:::
systemd-coredump:!!:19245::::::
dbus:!!:19245::::::
polkitd:!!:19245::::::
rtkit:!!:19245::::::
sssd:!!:19245::::::
avahi:!!:19245::::::
pipewire:!!:19245::::::
libstoragemgmt:!!:19245::::::
```

Figure 8: Чтение /etc/shadow от имени пользователя guest

Результаты выполнения

- Проведена работа со Sticky-битом

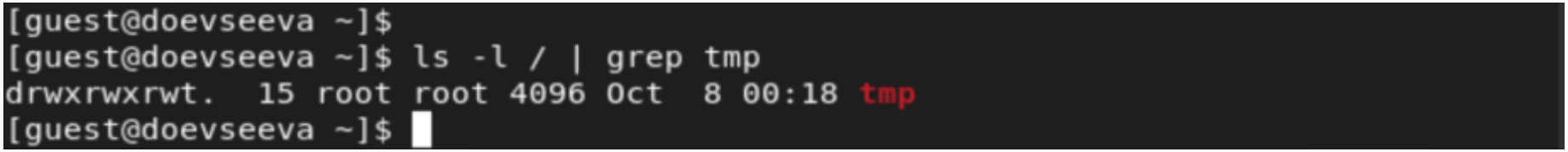

Figure 9: Проверка наличия атрибута Sticky

Результаты выполнения

```
[guest@doevseeva ~]$
[guest@doevseeva ~]$ echo "test" > /tmp/file01.txt
[guest@doevseeva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  8 00:26 /tmp/file01.txt
[guest@doevseeva ~]$ chmod o+rw /tmp/file01.txt
[guest@doevseeva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  8 00:26 /tmp/file01.txt
[guest@doevseeva ~]$
```

Figure 10: Создание файла и изменение прав

```
[guest2@doevseeva ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@doevseeva ~]$ cat /tmp/file01.txt
test
[guest2@doevseeva ~]$
```

Figure 11: Попытка дозаписи в файл

Результаты выполнения

```
[guest2@doevseeva ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@doevseeva ~]$ cat /tmp/file01.txt
test
[guest2@doevseeva ~]$
```

Figure 12: Попытка перезаписи файла

```
[guest2@doevseeva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@doevseeva ~]$
```

Figure 13: Попытка удаления файла

Результаты выполнения

```
[guest2@doevseeva ~]$ su -
Password:
[root@doevseeva ~]# chmod -t /tmp
[root@doevseeva ~]#
```

Figure 14: Снятие атрибута Sticky

```
[root@doevseeva ~]# exit
logout
[guest2@doevseeva ~]$ ls -l / | grep tmp
drwxrwxrwx.  15 root root 4096 Oct  8 00:30 tmp
[guest2@doevseeva ~]$
```

Figure 15: Проверка атрибутов

Результаты выполнения

```
[guest2@doevseeva ~]$ cat /tmp/file01.txt
test
[guest2@doevseeva ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@doevseeva ~]$ cat /tmp/file01.txt
test
[guest2@doevseeva ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@doevseeva ~]$ cat /tmp/file01.txt
test
[guest2@doevseeva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@doevseeva ~]$
```

Figure 16: Попытка повторного выполнения команд

Выводы

В результате проделанной работы мы изучили механизмы изменения идентификаторов и применения SetUID-, SetGID- и Sticky-битов, получили практические навыки работы в консоли с дополнительными атрибутами, рассмотрели работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.