

Лабораторная 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Шалыгин Г. Э.

Российский университет дружбы народов, Москва, Россия

Информация

- Шалыгин Георгий Эдуардович
- студент НФИ-02-20
- Российский университет дружбы народов

Вводная часть

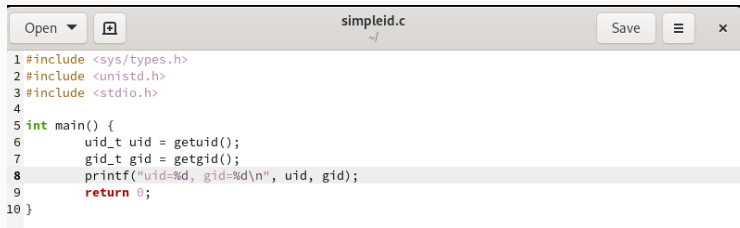
- Информационная безопасность - важная часть компетенции в образовательном треке НФИ

- Изучение механизмов изменения идентификаторов, применения SetUID- 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.

- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
 - `pdf`
 - `html`
- Автоматизация процесса создания: `Makefile`
- Компилятор Julia
- `OpenModelica`

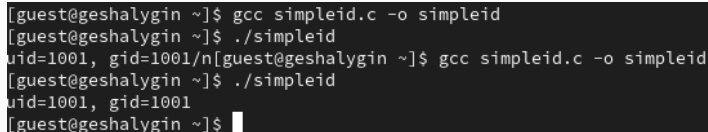
Результаты

От имени пользователя guest2 создадим программу simpleid.c



```
1 #include <sys/types.h>
2 #include <unistd.h>
3 #include <stdio.h>
4
5 int main() {
6     uid_t uid = getuid();
7     gid_t gid = getgid();
8     printf("uid=%d, gid=%d\n", uid, gid);
9     return 0;
10 }
```

Figure 1: Расширенные атрибуты



```
[guest@geshalygin ~]$ gcc simpleid.c -o simpleid
[guest@geshalygin ~]$ ./simpleid
uid=1001, gid=1001
[guest@geshalygin ~]$ gcc simpleid.c -o simpleid
[guest@geshalygin ~]$ ./simpleid
uid=1001, gid=1001
[guest@geshalygin ~]$
```

Figure 2: run simpleid

Усложним программу, добавив вывод действительных идентификаторов. Скомпилируем и запустим simpleid2.c

```
[guest@geshalygin ~]$ gcc simpleid.c -o simpleid2  
[guest@geshalygin ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@geshalygin ~]$
```

Figure 3: simpleid2

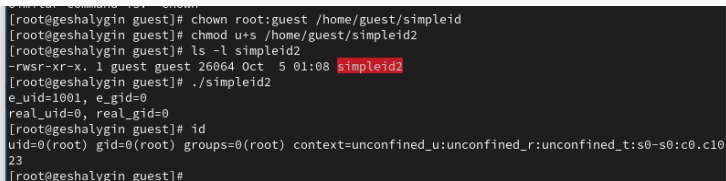
Добавление uid бита

От имени суперпользователя выполним команды. Изменим владельца и добавим uid бит.

Выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid2: `ls -l simpleid2 11`.

Запустите simpleid2 и id: `./simpleid2 id`

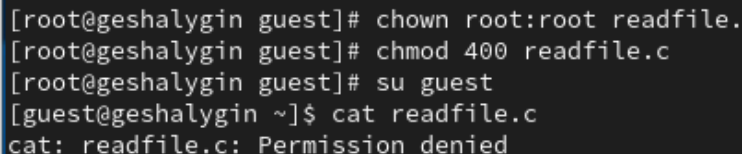
Результаты совпадают.

A terminal window showing a series of commands and their outputs. The commands are: 'chown root:guest /home/guest/simpleid', 'chmod u+s /home/guest/simpleid2', 'ls -l simpleid2', and './simpleid2 id'. The output of 'ls -l simpleid2' shows the file permissions as '-rwsr-xr-x. 1 guest guest 26064 Oct 5 01:08 simpleid2', where 'simpleid2' is highlighted in red. The output of './simpleid2 id' shows the effective user and group IDs as 'e_uid=1001, e_gid=0' and the real user and group IDs as 'real_uid=0, real_gid=0'. The output of 'id' shows the user as 'uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023'.

```
[root@geshalygin guest]# chown root:guest /home/guest/simpleid
[root@geshalygin guest]# chmod u+s /home/guest/simpleid2
[root@geshalygin guest]# ls -l simpleid2
-rwsr-xr-x. 1 guest guest 26064 Oct 5 01:08 simpleid2
[root@geshalygin guest]# ./simpleid2
e_uid=1001, e_gid=0
real_uid=0, real_gid=0
[root@geshalygin guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@geshalygin guest]#
```

Figure 4: simpleid2 with u+s

Сменим владельца у файла `readfile.c` и права так, чтобы только суперпользователь (`root`) мог прочитать его, а `guest` не мог. (fig. 5). Проверим что `guest` не имеет доступ к файлу.



```
[root@geshalygin guest]# chown root:root readfile.  
[root@geshalygin guest]# chmod 400 readfile.c  
[root@geshalygin guest]# su guest  
[guest@geshalygin ~]$ cat readfile.c  
cat: readfile.c: Permission denied
```

Figure 5: Проверка прав доступа для новых атрибутов

Результаты run readfile

Сменим у программы readfile владельца и установите SetU'D-бит. Проверим, может ли программа readfile прочитать файл readfile.c? Как видим, может.

[illegible]

Figure 6: run readfile

Доступ для пользователя gues2

От имени пользователя guest создадим файл file01.txt в директории /tmp со словом test. Просмотрим атрибуты у только что созданного файла и разрешим чтение и запись для категории пользователей «все остальные».

От пользователя guest2 (не являющегося владельцем) попробуем прочитать файл /tmp/file01.txt. Доступ открыт. Дозаписать в файл уже нельзя (fig. 7).

```
[guest@geshalygin ~]$ su guest2
Password:
[guest2@geshalygin guest]$ cat /tmp/file01.txt
test
[guest2@geshalygin guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@geshalygin guest]$
```

Figure 7: проверка доступа

Проверьте содержимое файла. Дозапись и удаление невозможны.

Выполним команду, снимающую sticky-бит.

Теперь дозапись недоступна, удаление доступно.

```
[guest2@geshalygin guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@geshalygin guest]$ cat /tmp/file01.txt
test
[guest2@geshalygin guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@geshalygin guest]$ ls /tmp
dbus-xmABtX2BT4
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-chronyd.service-iMqU2F
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-colord.service-8XxdJc
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-dbus-broker.service-ZPz3xS
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-geoclue.service-TEaNiC
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-ModemManager.service-3C0xr2
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-power-profiles-daemon.service-oiuDDj
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-rtkit-daemon.service-YbtXPg
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-switcheroo-control.service-30Xgvt
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-systemd-logind.service-Xc168Z
systemd-private-6e0e6cdf6abd4005b5b03329d23d2a3c-upower.service-ySHIer
[guest2@geshalygin guest]$
```

Figure 8: проверка доступа

Вывод

В результате выполнения работы мы изучили механизмы изменения идентификаторов, применения SetUID- 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.