

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

дисциплина: Информационная безопасность

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Серенко Данил Сергеевич

Группа: НФИбд-01-19

МОСКВА 2022 г.

Прагматика выполнения лабораторной работы

- работа с дополнительными атрибутами
-

Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов.

Выполнение лабораторной работы

1. Создание программы simpleid.c и выполнение

```
[guest@dsserenko lab5]$ cat simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getegid ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

simpleid

```

[guest@dssserenko lab5]$ gcc simpleid.c -o simpleid
[guest@dssserenko lab5]$ ls
readfile.c simpleid simpleid2.c simpleid.c
[guest@dssserenko lab5]$ ./simpleid
uid=1001, gid=1001
[guest@dssserenko lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

```

compile and run

2. Создание программы simpleid2.c и выполнение

```

#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t real_uid = getuid ();
    uid_t e_uid = geteuid ();

    gid_t real_gid = getgid ();
    gid_t e_gid = getegid ();

    printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf ("real_uid=%d, real_gid=%d\n", real_uid,
        ↵ real_gid);

    return 0;
}

```

simpleid2.c

```

[guest@dssserenko lab5]$ gcc simpleid2.c -o simpleid2
[guest@dssserenko lab5]$ ls
readfile.c simpleid simpleid2 simpleid2.c simpleid.c
[guest@dssserenko lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001

```

simpleid2

3. Установка новых атрибутов и запуск simpleid2

```
[root@dssserenko ~]# chown root:guest /home/guest/lab5/simpleid2
[root@dssserenko ~]# chmod u+s /home/guest/lab5/simpleid2
[root@dssserenko ~]#
```

chmod

```
-rw-rw-r--. 1 guest guest 191 Oct 8 15:54 simpleid.c
[guest@dssserenko lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@dssserenko lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@dssserenko lab5]$
```

simpleid2 run

4. Создание программы 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;
}
```

readfile.c

5. Смена владельца readfile

```
[root@dssserenko ~]# chown root:guest /home/guest/lab5/readfile.c
[root@dssserenko ~]# chmod 700 /home/guest/lab5/readfile.c
```

chown

```
[guest@dssserenko lab5]$ cat readfile.c
cat: readfile.c: Permission denied
```

cant read

6. Смена владельца readfile и установил SetU'D-бит

```
chown: cannot access '/home/guest/lab5/readfile': No such file or directory
[root@dssserenko ~]# chown root:guest /home/guest/lab5/readfile
[root@dssserenko ~]# chmod u+s /home/guest/lab5/readfile
[root@dssserenko ~]#
```

readfile

```
[guest@dssserenko lab5]$ ./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;
}
```

readfile read

```
geoclue:!!:19241:~~~~~:
cockpit-ws:!!:19241:~~~~~:
cockpit-wsinstance:!!:19241:~~~~~:
setroubleshoot:!!:19241:~~~~~:
flatpak:!!:19241:~~~~~:
colord:!!:19241:~~~~~:
clevis:!!:19241:~~~~~:
gdm:!!:19241:~~~~~:
systemd-oom:!*:19241:~~~~~:
pesign:!!:19241:~~~~~:
gnome-initial-setup:!!:19241:~~~~~:
sshd:!!:19241:~~~~~:
chrony:!!:19241:~~~~~:
dnsmasq:!!:19241:~~~~~:
tcpdump:!!:19241:~~~~~:
dsserenko:$6$48ZAwQVFz78X4hF$83LJeSIGjVRGMf649f4srA8PAJmVoI98I4/5sCdIqvv9jnQVg
WlmmS0dYwfbGBEiJNy0DIFXQ6mXEU3DTety.:0:99999:7:::
vboxadd:!!:19241:~~~~~:
guest:$6$MnVk0R3at0cP0DiH$cCp5zLSc7jymREKFVtNSr.dTPMwped8CccmlWMY6COMlE9moshSFZ
rUaXuWay3s0huiyy3KLoU0ImX0hj9M2f.:19249:0:99999:7:::
guest2:$6$BpBLQ0yVfzpm8qCq$5ht7wAlnK2iAZCM0ts6RCHGItp6FoS5110moFhQjFTFKN1xhWN7R
F/OqL.WfhR8zX.tCTLtZlcnYdge8jIvJV.:19256:0:99999:7:::
[guest@dsserenko lab5]$
```

/etc/shadow read

7. Проверка sticky бит на категории tmp.

```
[guest@dsserenko lab5]$ ls -l / | grep tmp
drwxrwxrwt. 14 root root 4096 Oct  8 16:04 tmp
[guest@dsserenko lab5]$ echo "test" > /tmp/file01.txt
[guest@dsserenko lab5]$ cd /tmp/
[guest@dsserenko tmp]$ ls
file01.txt
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-chronyd.service-GC0dbx
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-colord.service-JvRaxz
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-dbus-broker.service-RoA0xd
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-fwupd.service-FLNAmB
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-ModemManager.service-luVnqJ
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-power-profiles-daemon.service-
APVYZF
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-rtkit-daemon.service-vmW5ug
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-switcheroo-control.service-mvm
KvR
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-systemd-logind.service-v26pM0
systemd-private-e620e33a05c54fe6a6b0f92354cfe25e-upower.service-6t8Cz4
[guest@dsserenko tmp]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 16:20 /tmp/file01.txt
[guest@dsserenko tmp]$ cd /tmp/
```

sticky

8. Выполнение различных операций от guest2

```
[guest@dssserenko tmp]$ su - guest2
Password:
[guest2@dssserenko ~]$ cat /tmp/file01.txt
test
[guest2@dssserenko ~]$ echo "test2" > /tmp/file01.txt
[guest2@dssserenko ~]$ cat /tmp/file01.txt
test2
[guest2@dssserenko ~]$ echo "test3" > /tmp/file01.txt
[guest2@dssserenko ~]$ cat /tmp/file01.txt
test3
[guest2@dssserenko ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

guest2 file01

9. Снятие атрибут t (Sticky-бит) сдиректории /tmp и выполнение предыдущих шагов

```
Password:
[root@dssserenko ~]# chmod -t /tmp
[root@dssserenko ~]# exit
logout
[guest2@dssserenko ~]$ ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 Oct  8 16:24 tmp
[guest2@dssserenko ~]$
```

-t

```
logout
[guest2@dssserenko ~]$ ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 Oct  8 16:24 tmp
[guest2@dssserenko ~]$ echo "test2" > /tmp/file01.txt
[guest2@dssserenko ~]$ cat /tmp/file01.txt
test2
[guest2@dssserenko ~]$ echo "test3" >> /tmp/file01.txt
[guest2@dssserenko ~]$ cat /tmp/file01.txt
test2
test3
[guest2@dssserenko ~]$ rm /tmp/file01.txt
```

guest2 file01 try 2

Вывод

Выполнив данную лабораторную работу, я получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.