# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

```
[root@localhost ~]# yum install gcc
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: mirror.docker.ru
 * extras: mirror.reconn.ru
 * updates: mirror.reconn.ru
base                                                          | 3.6 kB  00:00:00
extras                                                        | 2.9 kB  00:00:00
updates                                                      | 2.9 kB  00:00:00
(1/4): base/7/x86_64/group_gz                                | 153 kB  00:00:00
(2/4): extras/7/x86_64/primary_db                            | 243 kB  00:00:01
(3/4): base/7/x86_64/primary_db                              | 6.1 MB  00:00:03
(4/4): updates/7/x86_64/primary_db                           |  13 MB  00:00:06
```

```
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
```

Base [Работает] - Oracle VM VirtualBox

Файл  Машина  Вид  Ввод  Устройства  Справка

```
GNU nano 2.3.1                        File: 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;
}
```

```
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ls
simpleid  simpleid.c
[guest@localhost ~]$ ./simpleid
uid=1000, gid=1000
[guest@localhost ~]$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest@localhost ~]$
```

```
[guest@localhost ~]$ cat simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int main() {
    uid_t e_uid = geteuid();
    gid_t e_gid = getegid();
    uid_t real_uid = getuid();
    gid_t real_gid = getgid();
    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;
}
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ./simpleid
e_uid=1000, e_gid=1000
real_uid1000, real_gid=1000
[guest@localhost ~]$
```

```
[guest@localhost ~]$ su -
Password:
Last login: Sat Feb 19 14:06:37 EST 2022 on tty1
[root@localhost ~]# chown root:guest /home/guest/simpleid
[root@localhost ~]# chmod u+s /home/guest/simpleid
[root@localhost ~]# ^C
[root@localhost ~]# logout
[guest@localhost ~]$ ls -s
total 16
12 simpleid    4 simpleid.c
[guest@localhost ~]$ ls -l
total 16
-rwsrwxr-x. 1 root  guest 8576 Feb 19 14:12 simpleid
-rw-rw-r--. 1 guest guest  323 Feb 19 14:11 simpleid.c
[guest@localhost ~]$ ./simpleid
e_uid=0, e_gid=1000
real_uid1000, real_gid=1000
[guest@localhost ~]$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest@localhost ~]$
```

```
  GNU nano 2.3.1                    File: readfile.c

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

int main() {
    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(f);
    return 0;
}
```

```
[guest@localhost ~]$ gcc readfile.c -o readfile
[guest@localhost ~]$
```

```
[guest@localhost ~]$ chmod u-wrx readfile.c
[guest@localhost ~]$ ls -l
total 32
-rwxrwxr-x. 1 guest guest 8512 Feb 19 14:19 readfile
-----rw-r--. 1 guest guest  464 Feb 19 14:19 readfile.c
-rwsrwxr-x. 1 root  guest 8576 Feb 19 14:12 simpleid
-rw-rw-r--. 1 guest guest  323 Feb 19 14:11 simpleid.c
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

```
[root@localhost ~]# chown root:root /home/guest/readfile
[root@localhost ~]# ls -l /home/guest/readfile
-rwxrwxr-x. 1 root root 8512 Feb 19 14:19 /home/guest/readfile
[root@localhost ~]#
```

```
[root@localhost ~]# /home/guest/readfile /etc/shadow
root:$6$SkJdIW15Dk5K2mCi$QMab1WwDsNLXNGHQUY/Qb1Dp1ETDg52iaLBmrxmHUvU1UQunwFPVvmdRv0QfBMyorbzCKDr8ja9
Y8MP7gQM360::0:99999:7:::
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
systemd-network:!!:19042::::::
dbus:!!:19042::::::
polkitd:!!:19042::::::
sshd:!!:19042::::::
postfix:!!:19042::::::
chrony:!!:19042::::::
guest:$6$.FsFlyzD$ND1Jci6BscgU8bRHf5MOMF0w.NuAsehYCaAVPkAkrdZsaw3LctXBL3Oh1MgDGtvj287TD8y/pyV/T6QcB1
vlA.:19042:0:99999:7:::
```

```
[guest@localhost ~]$ ls
readfile  readfile.c  simpleid  simpleid.c
[guest@localhost ~]$ echo "text" > /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Feb 19 14:24 /tmp/file01.txt
[guest@localhost ~]$ su -
Password:
Last login: Sat Feb 19 14:22:17 EST 2022 on tty1
[root@localhost ~]# useradd guest2
[root@localhost ~]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
[guest2@localhost ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@localhost ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@localhost ~]$ su -
Password:
Last login: Sat Feb 19 14:24:48 EST 2022 on tty1
[root@localhost ~]# chmod -t /tmp
[root@localhost ~]# exit
logout
[guest2@localhost ~]$ ls -l / grep tmp
ls: cannot access grep: No such file or directory
ls: cannot access tmp: No such file or directory
/:
total 16
lrwxrwxrwx.   1 root root    7 Feb 19 13:53 bin -> usr/bin
dr-xr-xr-x.   5 root root 4096 Feb 19 13:58 boot
drwxr-xr-x.  20 root root 3120 Feb 19 14:02 dev
drwxr-xr-x.  75 root root 8192 Feb 19 14:25 etc
drwxr-xr-x.   4 root root   33 Feb 19 14:24 home
lrwxrwxrwx.   1 root root    7 Feb 19 13:53 lib -> usr/lib
lrwxrwxrwx.   1 root root    9 Feb 19 13:53 lib64 -> usr/lib64
drwxr-xr-x.   2 root root    6 Apr 11  2018 media
drwxr-xr-x.   2 root root    6 Apr 11  2018 mnt
drwxr-xr-x.   2 root root    6 Apr 11  2018 opt
dr-xr-xr-x. 108 root root    0 Feb 19 14:02 proc
dr-xr-x---.   2 root root  135 Feb 19 14:06 root
drwxr-xr-x.  24 root root  720 Feb 19 14:06 run
lrwxrwxrwx.   1 root root    8 Feb 19 13:53 sbin -> usr/sbin
drwxr-xr-x.   2 root root    6 Apr 11  2018 srv
dr-xr-xr-x.  13 root root    0 Feb 19 14:02 sys
drwxrwxrwx.   8 root root  229 Feb 19 14:24 tmp
```

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

```
[guest2@localhost ~]$ su -
Password:
Last login: Sat Feb 19 14:27:01 EST 2022 on tty5
Last failed login: Sat Feb 19 14:28:52 EST 2022 on tty5
There was 1 failed login attempt since the last successful login.
[root@localhost ~]# chmod +t /tmp
[root@localhost ~]# exit
logout
```