№ 1

, ,

-
-
-
- [1032225751@pfur.ru]

, SetUID- Sticky- .

. ,

Sticky .

1. - guest simpleid.c

```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;
}
```

2. , id. User ID Group ID .

```
[guest@batagiev ~]$ gcc simpleid.c -o simpleid
[guest@batagiev ~]$ ./simpleid
uid=1001, gid=1002
[guest@batagiev ~]$ id
uid=1001(guest) gid=1002(guest) groups=1002(guest)
:unconfined_t:s0-s0:c0.c1023
[guest@batagiev ~]$
```

. 2:

SetUID

3. , e_uid/e_gid uid/gid. getgid
. getegid

. .

setuid .

```c
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, gid=%d\n", e_uid, gid);
        printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
        return 0;
}
```

. 3: simpleid.c

SetUID

4. - setuid.

```
[guest@batagiev ~]$ sudo !!
sudo chown root:guest /home/guest/simpleid
[guest@batagiev ~]$ sudo chmod u+s /home/guest/simpleid
```

. 4:

5. .

```
[guest@batagiev ~]$ ls -l simpleid
-rwsr-xr-x. 1 root guest 26064 Oct  6 19:56 simpleid
```

. 5: ls -l

6. .

```
[guest@batagiev ~]$ ./simpleid
e_uid=0, e_gid=1002
real_uid=1001, real_gid=1002
[guest@batagiev ~]$ id
uid=1001(guest) gid=1002(guest)
:unconfined_t:s0-s0:c0.c1023
```

. 6:

7. , .

```
[guest@batagiev ~]$ sudo chmod g+s /home/guest/simpleid
[guest@batagiev ~]$ ls -l simpleid
-rwxr-sr-x. 1 root root 26064 Oct  6 19:56 simpleid
[guest@batagiev ~]$ ./simpleid
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1002
[guest@batagiev ~]$
```

. 7:

8. readfile.c

```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);
}
```

9. `readfile.c`. .

```
[guest@batagiev ~]$ sudo chown root:root readfile.c
[guest@batagiev ~]$ sudo chmod 700 readfile.c
[guest@batagiev ~]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@batagiev ~]$
```

. 9: readfile.c

10. readfile, setuid .

```
[guest@batagiev ~]$ sudo chown root:guest ./readfile
[guest@batagiev ~]$ sudo chmod u+s ./readfile
[guest@batagiev ~]$
```

. 10: setuid

11. . `readfile.c` `/etc/shadow`.

```
[guest@batagiev ~]$ ./readfile ./readfile.c
#include <fcntl.h>
#include <stdio.h>
```

. **11:** readfile.c

```
[guest@batagiev ~]$ ./readfile /etc/shadow
root:$6$l0UHCDykMrMqVr5v$7LfXbb7V8ZOiTqEaEuYSO
y/ZZJAAZoWAeGzIFKYqcqjlYRk/::0:99999:7:::
bin:*:19469:0:99999:7:::
```

. **12:** /etc/shadow

1. Sticky /tmp.

```
[guest@batagiev ~]$ ls -l / | grep tmp
drwxrwxrwt.  15 root root 4096 Oct  6 20:07 tmp
```

. 13: /tmp

2. /tmp/file01.txt. .

```
[guest@batagiev ~]$ echo "test" > /tmp/file01.txt
[guest@batagiev ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  6 20:14 /tmp/file01.txt
[guest@batagiev ~]$ chmod o+rw /tmp/file01.txt
[guest@batagiev ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  6 20:14 /tmp/file01.txt
```

. **14:** /tmp/file01.txt

3. guest2.

```
[guest2@batagiev ~]$ cat /tmp/file01.txt
test
```

. **15:** guest2

4. .

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

. **16:** guest2

5. .

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

. **17:** guest2

6. sticky /tmp.

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

. **18:** /tmp

7. .

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

. 19: /tmp