华中科技大学

HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

网络空间安全学院

2.4 Linux系统权限管理与SetUID

网络空间安全学院 慕冬亮

Email : dzm91@hust.edu.cn

Linux系统权限管理

- Linux 操作系统是一个多用户操作系统，存在资源贡献与隔离的问题。因此，Linux系统需要一套权限管理的功能。

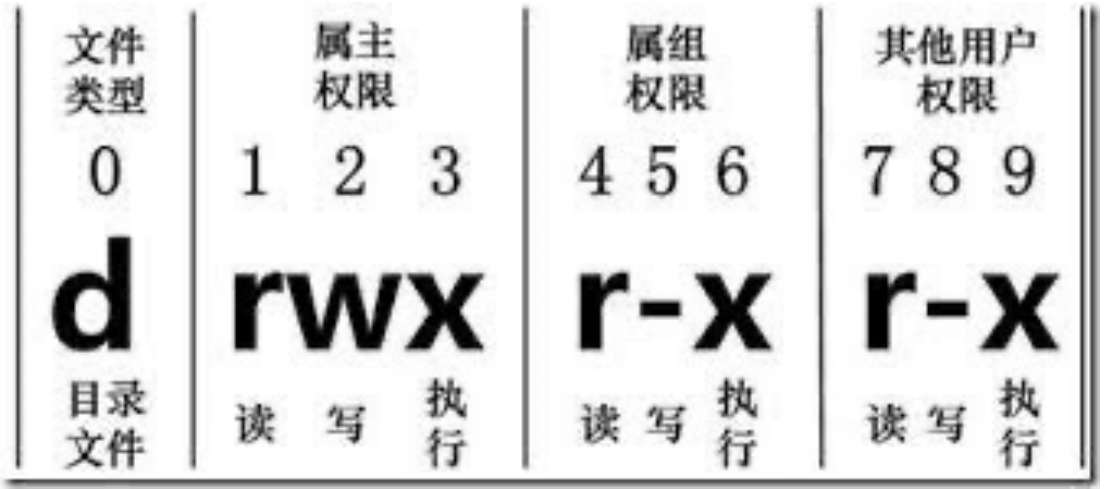
- Linux原生的权限管理机制是基于用户角色的管理机制，即UGO+RWX/ACL权限控制
  - U：User，G：Group，O：Other
  - R：Read，W：Write，X：eXecute
  - ACL是Access Control List的简称

- Linux原生的访问控制称为自主访问控制

Linux系统文件权限

在Linux 系统中，不同的用户处于不同的地位，拥有不同的权限，获取不同级别的资源。

- 读取 (R)：允许查看文件内容，显示目录列表
- 写入 (W)：允许修改文件内容，允许在目录中新建、删除、移动文件或者子目录
- 可执行 (X)：允许运行程序，切换目录
- 无权限 (-)：没有任何权限




```
seclab@VM-0-11-debian:~/s2_demo$ ls -l
total 36
-rw-r--r-- 1 seclab seclab 11357 Mar 20 20:21 LICENSE
-rw-r--r-- 1 seclab seclab    59 Mar 20 20:21 README.md
-rw-r--r-- 1 seclab seclab   228 Mar 20 20:21 compose-dev.yaml
drwxr-xr-x 2 seclab seclab  4096 Mar 20 20:21 test_cracked_elf
drwxr-xr-x 2 seclab seclab  4096 Mar 22 16:07 test_java_deserialization
drwxr-xr-x 4 seclab seclab  4096 Mar 20 20:21 test_pwn
drwxr-xr-x 2 seclab seclab  4096 Mar 20 20:21 test_sql_injection
```

Linux系统进程权限

当用户运行可执行文件时，所启动的进程必须携带发起当前用户的身份信息才能够进行合法的操作。换句话说，进程从执行用户处继承 UID、GID，从而决定对文件系统的存取和访问。

- Linux系统通过进程的实际用户 ID (Real User ID）和实际用户组 ID (Real Group ID) 来决定识别正在运行此进程的用户和组

- Linux 系统通过进程的有效用户 ID (Effective User ID) 和有效用户组 ID (Effective Group ID) 来决定进程对系统资源（如文件）的访问权限

Effective User ID 是为了让非权限用户获得两种不同的权限

SetUID 后门

```
hacker@setuid-backdoor-level-1-0:/challenge$ ls -al setuid-backdoor-level1.0
-rwsr-xr-x 1 root root 17032 Aug 21 09:34 setuid-backdoor-level1.0
```

- 权限位除了 rwx，还有 s，即，set-user-ID 或 SetUID
- SetUID 功能：对于带有 SetUID 权限位的二进制程序，任何用户执行时，都会以该二进制程序所属的用户身份执行
- 对于上述 setuid-backdoor-level1.0 程序，当我们以 hacker 运行该程序时，会以 root 用户进行执行，具体来说，设置了Effective User ID 为 root ID。

这是 pwn.hust.college 设计的核心思路

Linux系统常用命令

- chown
- chmod
- useradd
- userdel
- usermod
- id / whoami
- groupadd
- groupdel
- ……