Linux 系统账户安全加固

Linux 系统对账号与组的管理是通过 ID 号来实现的，我们在登录系统时，输入用户对应的密码，后台系统会将用户名转化为 ID 号后再判断该账号是否存在，并对比密码是否匹配。在 Linux 中，用户 ID 号被称为 UID，组 ID 被称为 GID。其中 UID 为 0，代表超级管理员，也就是通常说的 root 账号，1~499 之间 ID 号系统会预留下来。这样我们创建的账号会从 500 算起。

Linux 的组有基本组与附加组之分，一个用户只可以加入一个基本组中，但可以同时加入多个附加组。创建用户时，系统默认会自动创建同名的组，并设置用户加入该基本组中。

对于服务器安全来说，服务器的账号密码是很重要的事情

我们可以选择取消账号密码登陆，只使用公钥登录，但有时可能并不方便

这里告诉大家账号密码如何管理更加安全

一、账号密码最大使用天数

在/etc/login.defs 里面修改 PASS_MAX_DAYS 1095

同一个密码最多只能使用 1095 天

二、密码修改最小间隔天数

在/etc/login.defs 里面修改 PASS_MIN_DAYS 7

密码最少也要 7 天换一个

三、账号不活动最长天数

useradd -D -f 1095

如果在 1095 天内无活动，则注销