## 保护root账号：

1. 检查/etc/passwd文件，是否有非root账户的UID为0

使用命令：awk -F: '($1!="root" && $3==0) {print $1}' /etc/passwd

也可以顺便用命令：awk -F: '($2=="") {print $1}' /etc/passwd 检查登录不需要输入密码的账号

1. 检查/etc/sudoers文件，是否为普通用户设置了sudo权限，如果有，删除。

使用命令 grep -v ^# /etc/sudoers 检查文件内容，除了root ALL=（ALL） ALL，不应有其他有效权限设置行。

1. 如果/etc/passwd、/etc/shadow、/etc/sudoers的内容经检查无误，可为这些文件设置完全不可更改属性，文件将不可被删除、修改内容、追加内容。

使用命令： chattr +i /etc/passwd /etc/shadow /etc/sudoers

可用命令查看i属性是否添加成功： lsattr /etc/passwd /etc/shadow /etc/sudoers

1. 限制su命令的使用

最简单的方法是把/bin/su文件重命名。

复杂一点的方法是编辑/etc/pam.d/su文件，去除auth required pam\_wheel.so use\_uid 行前面的“#”注释符，但同时要检查/etc/group文件中，确保wheel组内除了root不能有其他用户存在。

1. 检查系统中所有的SUID文件

使用命令：find / -type f -perm -4000 | xargs /bin/ls

注意：因为系统中存在大量的默认SUID，所以需要事先在干净的系统里运行命令，了解系统中默认存在的以后，和靶机里面的对比，凡是多出的都不正常，建议删除