**Shellshock漏洞复现实验报告**

漏洞相关CVE编号 CVE-2019-14287

马志立4042017021

1. 原理分析

Sudo命令是Linux系统下用来赋予用户权限的命令，允许用户在不需要切换环境的前提下用其他用户的权限运行程序或命令，通常是以root身份运行命令，以减少root用户的登陆和管理时间，也可提高安全性。在使用sudo命令时，若sudo的版本低于1.8.28，当sudo配置为允许用户以任意方式运行命令时，用户通过Runas规范中的ALL关键字可以通过指定用户ID -1或者4294967295以root用户身份运行命令，允许普通用户绕过该策略并完全控制系统。

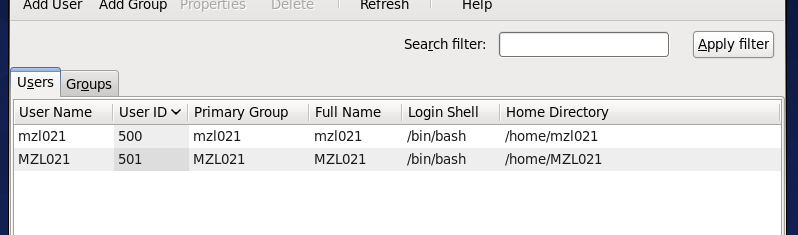
1. 复现准备

虚拟机：CentOS 6

ash版本：4.1.2

1. 复现过程
2. 创建一个新账户：MZL021



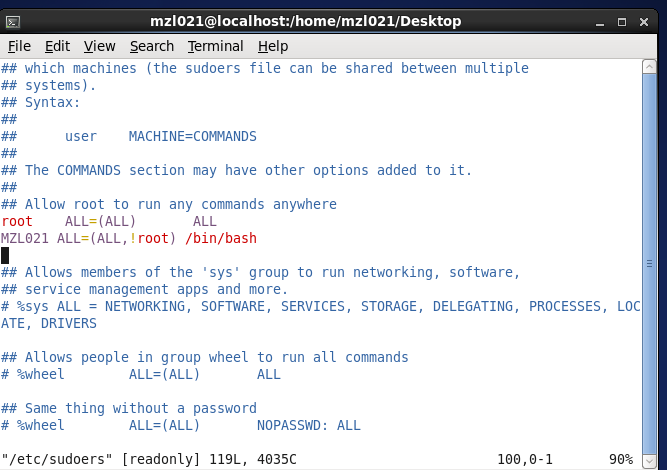


1. 修改/etc/sudoers配置文件

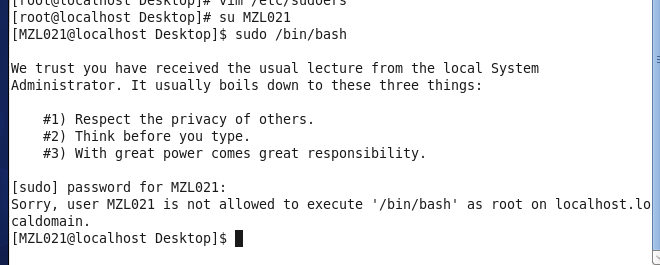
首先输入命令vim /etc/sudoers打开文件



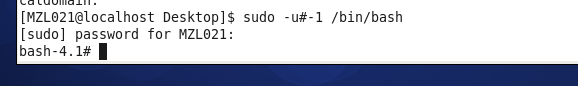
之后添加sudo权限，使得所创建的用户MZL021不能使用root执行的/bin/bash命令。



1. 待修改好权限后，尝试正常使用用户输入/bin/bash命令

由图可见显示不成功。

1. 此次使用漏洞，重新尝试输入sudo -u#-1 /bin/bash、



由图可见这样可以执行成功从而实现越权控制。

1. 原因分析

之所以会产生这个漏洞，是因为虚拟机用户将用户 ID 转换为用户名的函数无法识别-1（或无效等效的 4294967295），从而会将 -1默认为是0，0代表是root用户User ID。此外，由于通过 -u 选项指定的 User ID 在密码数据库中不存在，因此不会运行任何 PAM 会话模块。

1. 修复办法

老版本sudo才会出现此问题，只需将sudo升级到最新版本即可避免此问题。