CVE-2019-14287实验报告

1. 漏洞介绍

2019年10月14日，CVE官方发布了CVE-2019-14287的漏洞预警。通过特定payload，用户可提升至root权限（即使用sudo运行命令）。

sudo，也就是以超级管理员身份运行（superuser do）的意思。sudo是 Linux中最常使用的重要实用程序之一，它功能十分强大，几乎安装在每一款基于UNIX或 Linux的操作系统上，也是这些操作系统的核心命令。作为一个系统命令，普通用户可通过它以特殊权限来运行程序或命令（通常以root用户身份运行命令），而无需切换使用环境。

管理员可以配置 sudoers 文件，来定义哪些用户可以运行哪些命令。即便限制了用户以 root 身份运行特定或任何命令，该漏洞也可允许用户绕过此安全策略，并完全控制系统。

此漏洞复现起来较为简单，但环境较为落后，限制条件较为严苛，因此并不会对其他计算机造成太大伤害。

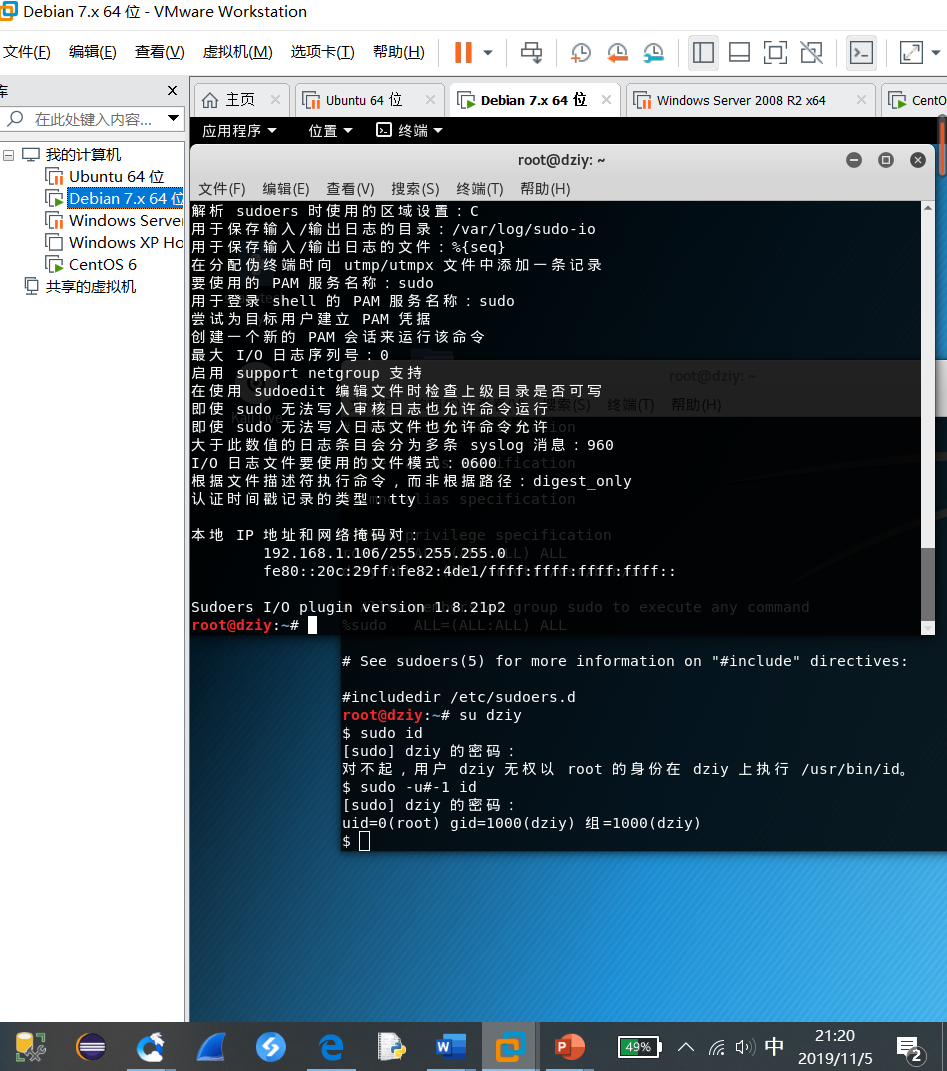
1. 漏洞原理

之所以会产生这个漏洞，是因为将用户 ID 转换为用户名的函数会将 -1（或无效等效的 4294967295）误认为是 0，而这正好是 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。

此漏洞更像是一个bug。没有去验证此函数的返回值是否溢出，这样给了某些动机不良的苍蝇开了鸡蛋的一条缝，某些黑客可以通过接触计算机修改sudoers文件，给非root用户提权，做一些管理员权限的事，来完成自己的需求。

1. 环境准备

使用kali的虚拟机，并且sudo版本低于1.8.28



命令：sudo -V

可以看出我所使用的环境，其sudo的版本为1.8.21

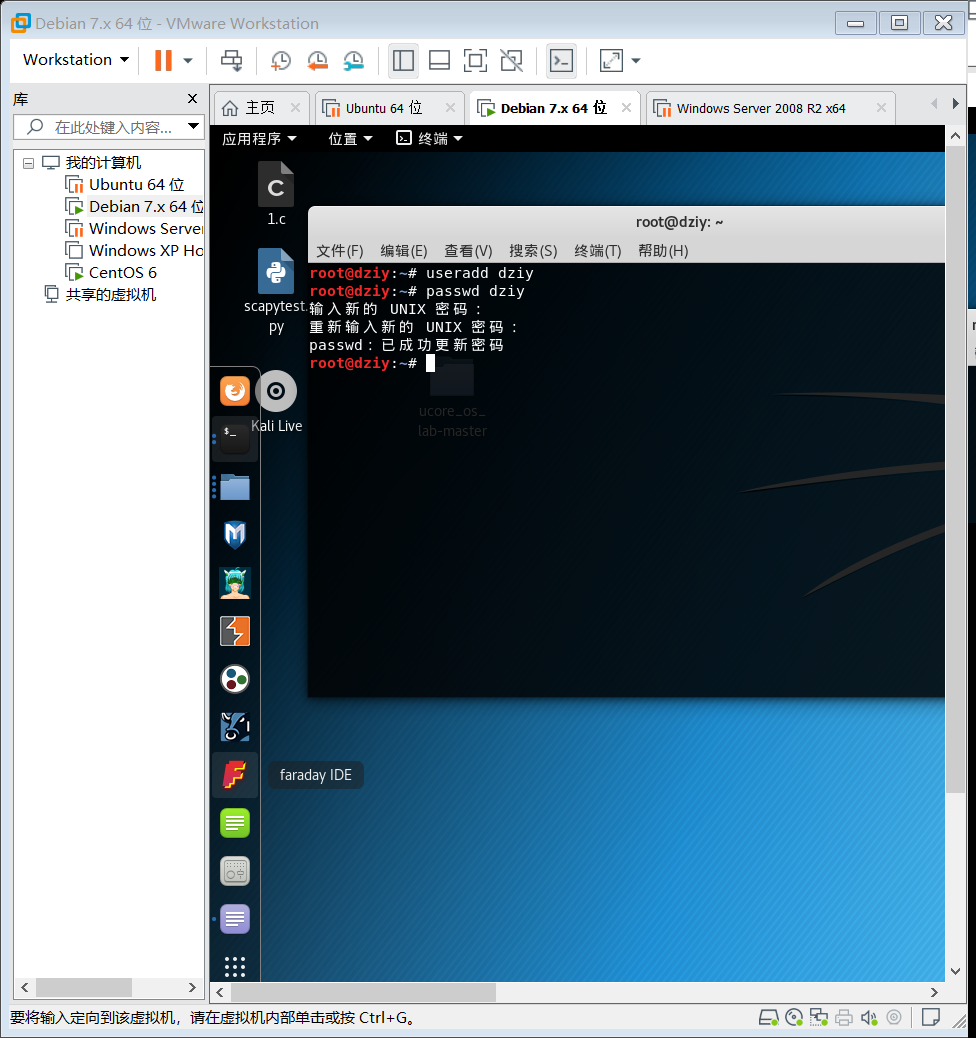
因此，可以进行漏洞复现

1. 漏洞复现
2. 首先建立一个非root用户

使用命令useradd +”name”

之后使用passed+“name”给其设置密码

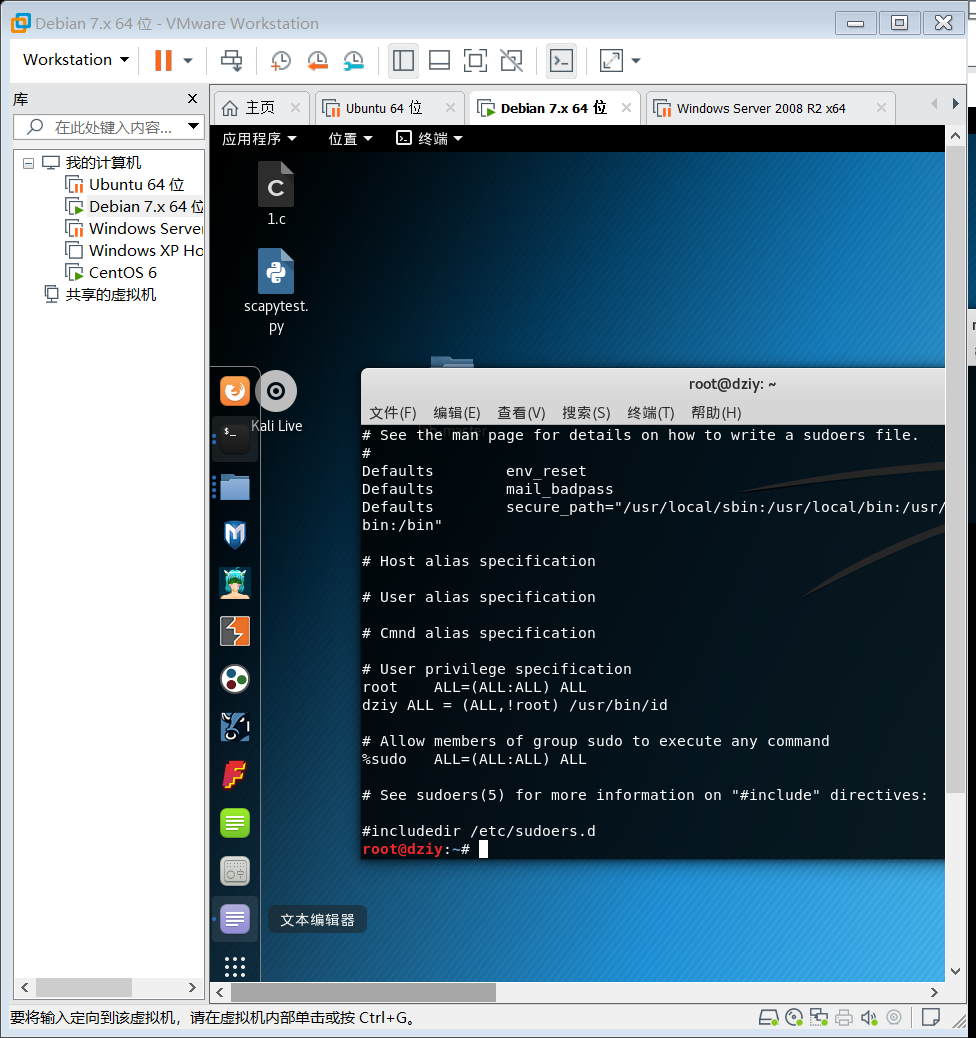
实现如下：



2.配置sudoers文件

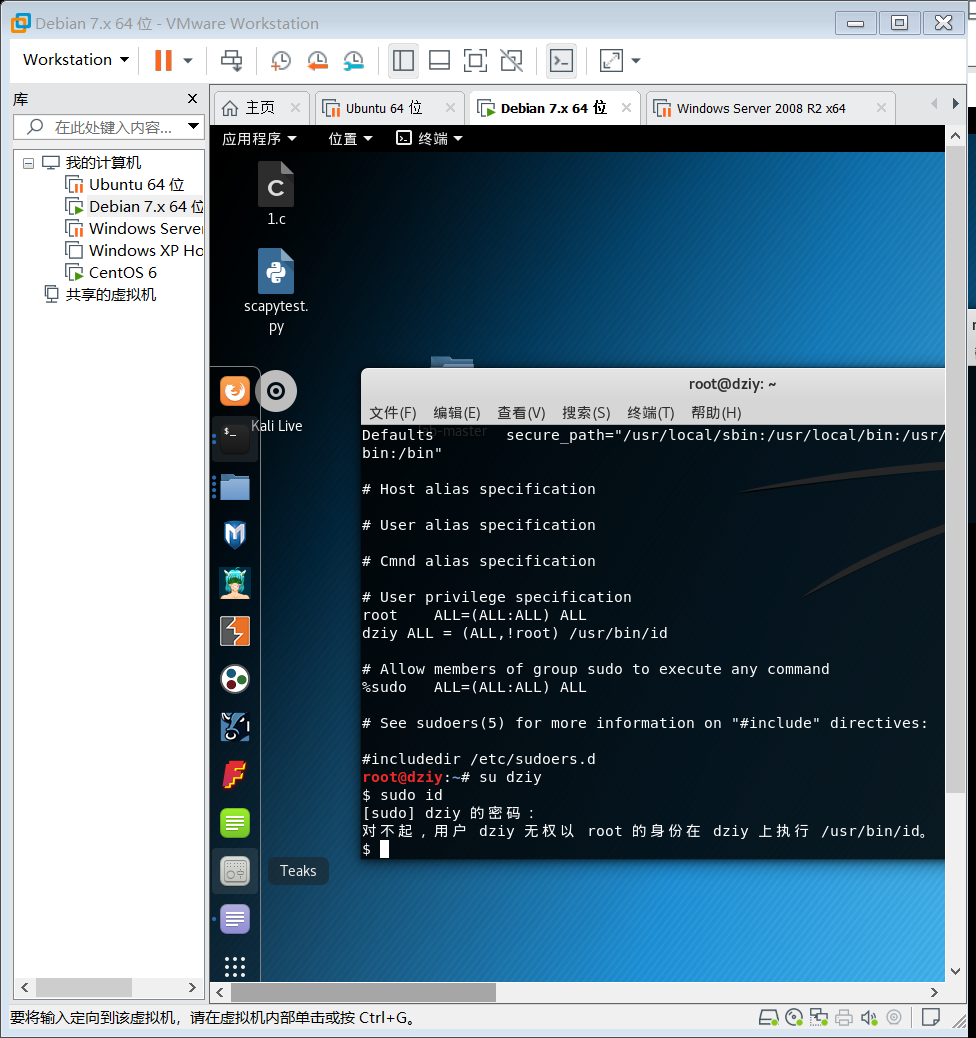
Sudoers文件存放于/etc中

修改之后的文件内容为：



3.使用用户并利用漏洞提权

使用用户dziy执行sudo命令：sudo id

之

后使用命令：sudo -u#-1 id:



则可以看到使用非root用户可以在没有root用户密码的条件下，使用root的命令（即sudo命令）。至此，以实现漏洞。

1. 漏洞总结

CVE-2019-14287漏洞影响1.8.28之前的Sudo版本。而且漏洞一旦被利用，会导致极大的风险。但是，此漏洞有着很严格的限制条件。只有通过sudoers配置文件为用户提供了对命令的访问权限，它才能起作用。如果不是这样，并且大多数Linux发行版默认情况下都没有，那么此错误将无效。因此大多数人无需担心，只需要平常注意自己的计算机就不会被黑客利用此漏洞攻击。

同时，感兴趣的人也可以根据此漏洞进行学习了解，通过该类型的漏洞，分析其原理，去进行更多的漏洞学习。