口令破解

姓名：任宇 学号：33920212204567

1. 实践任务

针对Windows/Linux系统平台，在获得系统控制权限的基础上，提取出用户账户的口令明文。

包含两个主要步骤：

1）如何获取用户账户的口令密文；

2）如何通过破解工具获取口令明文。

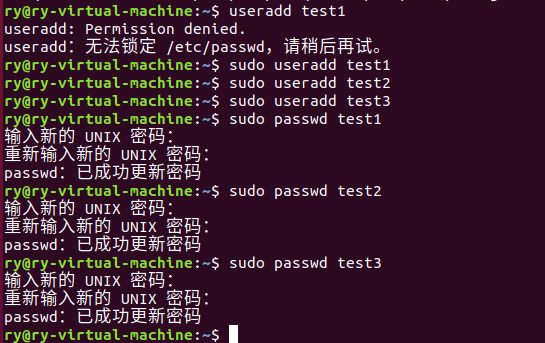
1. 实践要求、

* 用户口令设置成学号后6位；
* 观察并记录下各操作写入实验报告中。

1. 实践环境

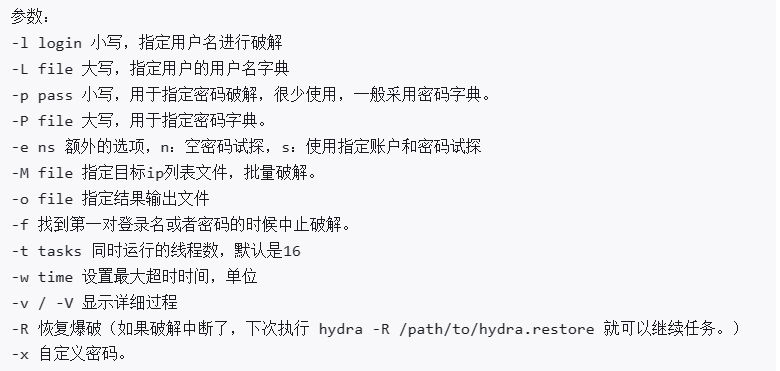
虚拟机版本为Kali 2024.1，靶机为Ubuntu18.04。

1. 实践步骤
2. 在Ubuntu靶机中新建用户：

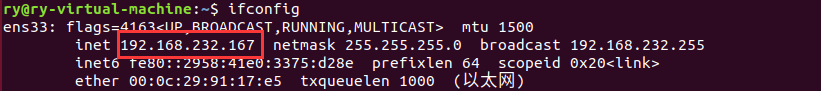


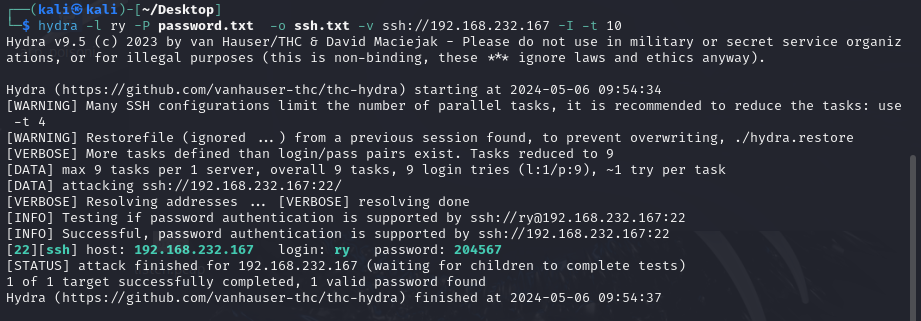
1. 在Kali攻击机中，通过Hydra破解靶机用户ry的SSH连接：

Hydra参数详解如下图：



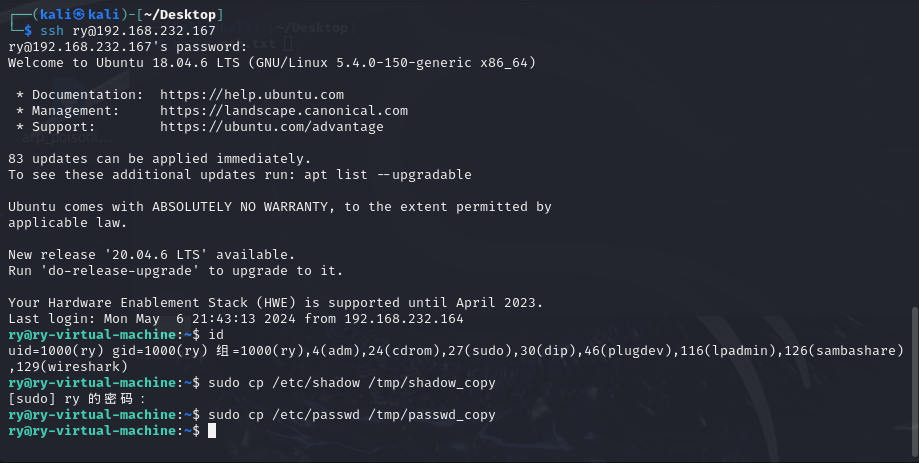
**hydra -l ry -P password.txt -o ssh.txt -v ssh://192.168.232.167 -I -t 10**





可见成功破解密码，密码为204567。

1. 获取SSH连接后，将存储用户加密密码的/etc/shadow文件和存储用户基本信息的/etc/passwd文件拷贝到/tmp下并修改文件权限：





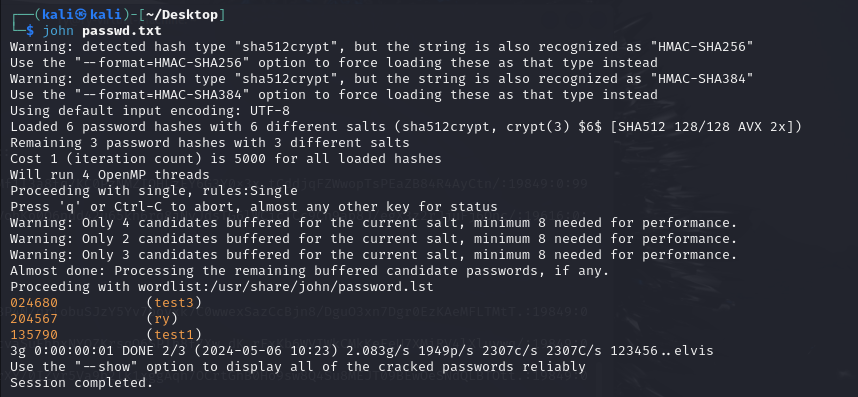
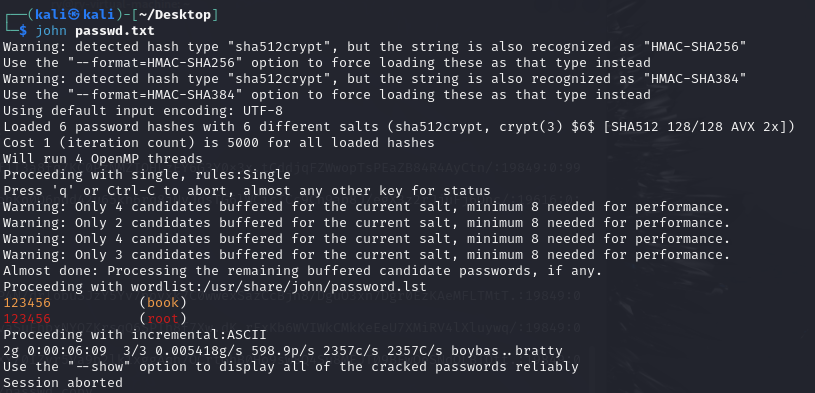
1. 在攻击机上通过scp命令将两个文件下载到本地：



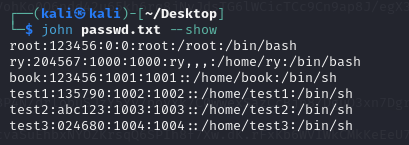
1. 通过unshadow工具合并两个文件，以便进行密码破解：



1. 使用John the Ripper对合并后的文件进行破解：



1. 查看破解结果：



1. 实践总结

在本次实践中，我通过模拟渗透测试的完整流程，成功地对Ubuntu 18.04靶机进行了安全测试。首先，我通过Hydra破解了靶机上用户ry的SSH密码，接着获取了靶机的/etc/shadow和/etc/passwd文件，并使用scp命令成功地将这些文件下载到攻击机上。随后，利用unshadow工具合并了这两个文件，并使用John the Ripper进行了密码破解，最终获取了用户的明文密码。此过程不仅加深了我对密码破解工具和技术的理解，还提高了我在实际环境中应用渗透测试技术的能力。