密码破解系列

2017-10-28 | 48

前言

本文总结了有关Windows密码、Linux密码、网络设备密码、数据库密码、无线网络密码、web应用登陆密码的破解以及在线扫描服务的密码破解。

正文

####1.windows密码破解

获取密码（抓取HASH）：pwdump、wce、mimikatz

破解密码：hashcat、LC5、SAMInside.exe、Ophcrack、mimikatz、hashsuite

密码抓取：

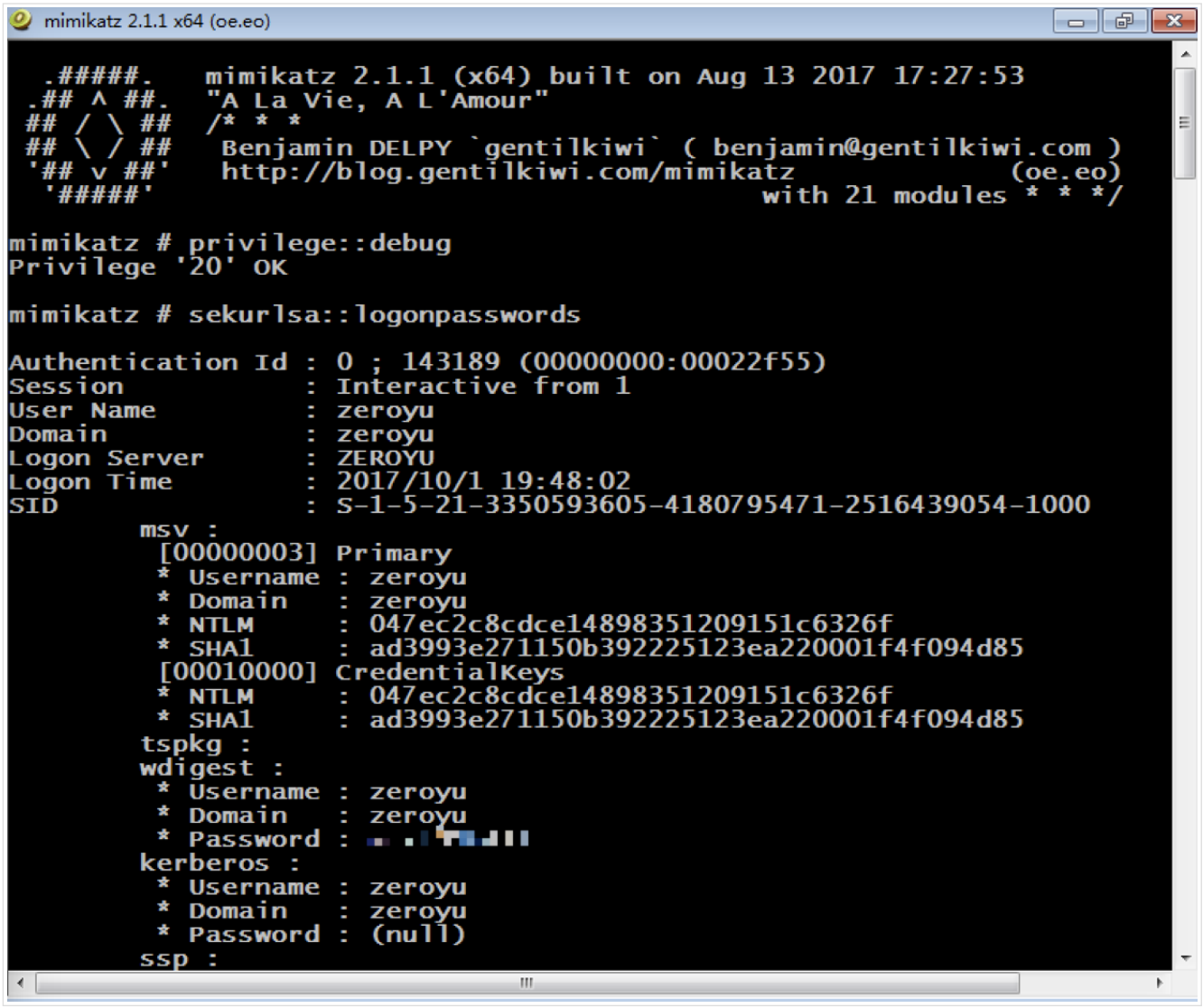
环境：windows7

前提：已经获取root权限

工具：mimikatz

操作：

原理是从lsass.exe进程中直接获取密码信息进行破解，而且该破解应该并非穷举方式，而是直接根据算法进行反向计算。



密码提取：

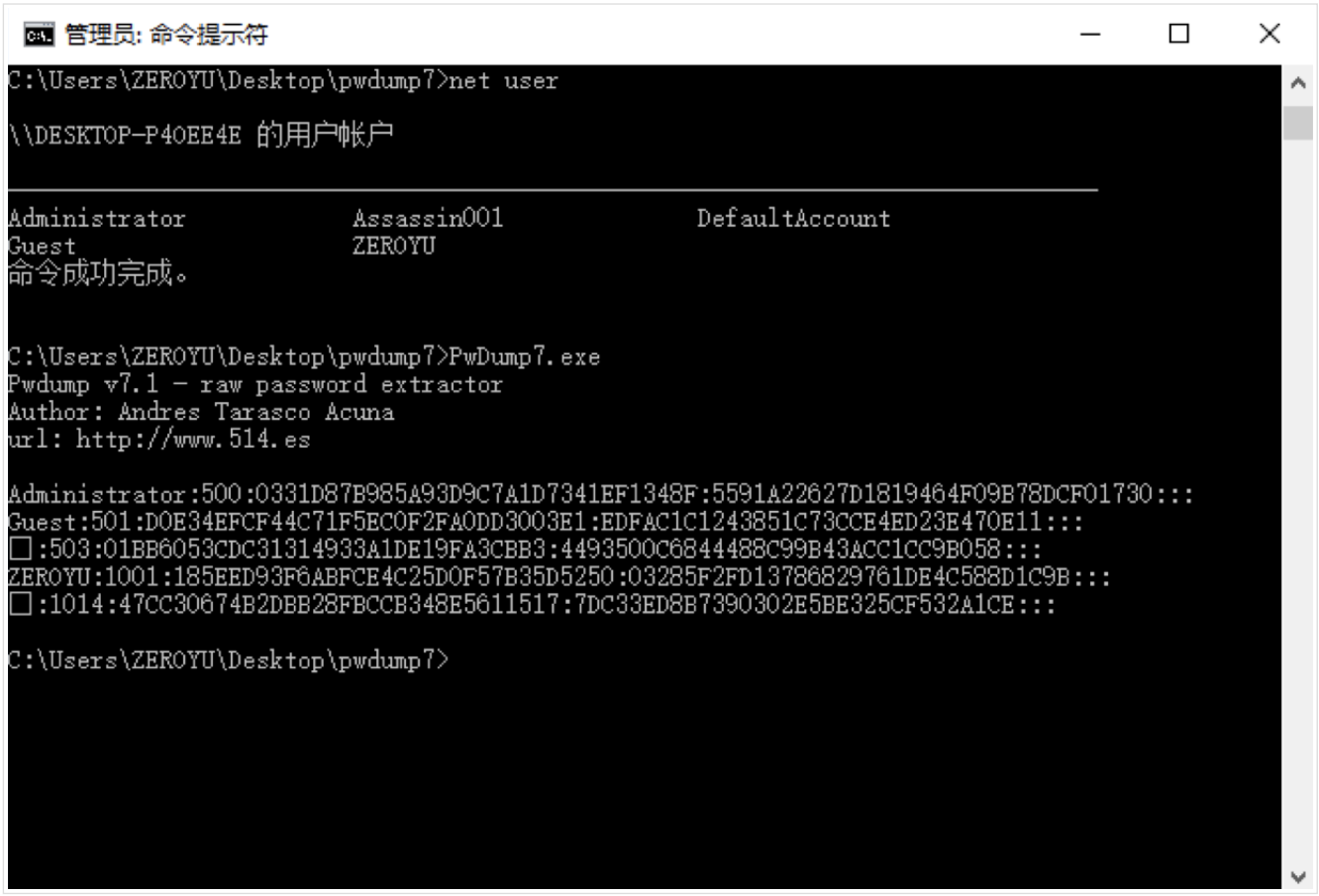
原因：为了进行口令破解，必须首先运行一个工具，将Windows口令从SAM文件中提取出来，做这一步工作的原因在于Windows运行过程中SAM被锁定，不能直接复制或编辑这个文件(即使有管理员权限也不行)。

环境：windows10（提取hash）、Windows7（破解hash）

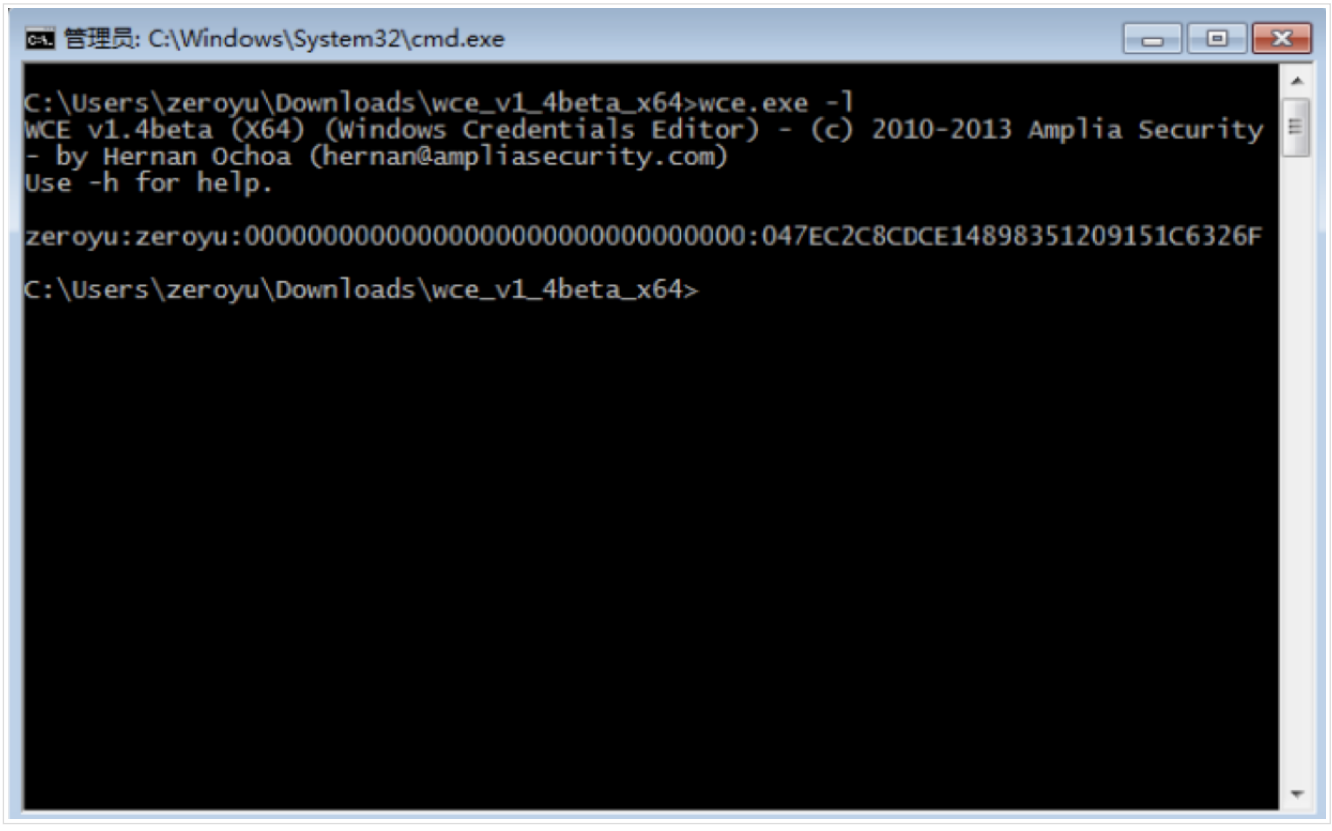
工具：Pwdump7，wce（Windows Credentials Editor）

操作：

用管理员权限打开Pwdump7，从而获得Windows口令



用管理员权限打开wce，从而获得Windows的NTML HASH



还可以利用wce直接获取Windows的密码（ -w参数是通过摘要式认证缓存一个明文的密码 ）：

```
C:\Users\zeroyu\Downloads\wce_v1_4beta_x64>wce.exe -w
WCE v1.4beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

zeroyu\zeroyu:[illegible]
```

密码破解：

环境：Windows10（CPU：i5；GPU：gtx860）

工具：hashcat、hashsuite

操作：

1.使用hashcat进行密码的破解

hashcat参数简介：

-m 这个是指定破解的hash的类型，具体的类型可以在–help参数中看到。 默认是0也就是MD5，而NTLM则是1000。

-a 指定破解的模式，默认是字典模式

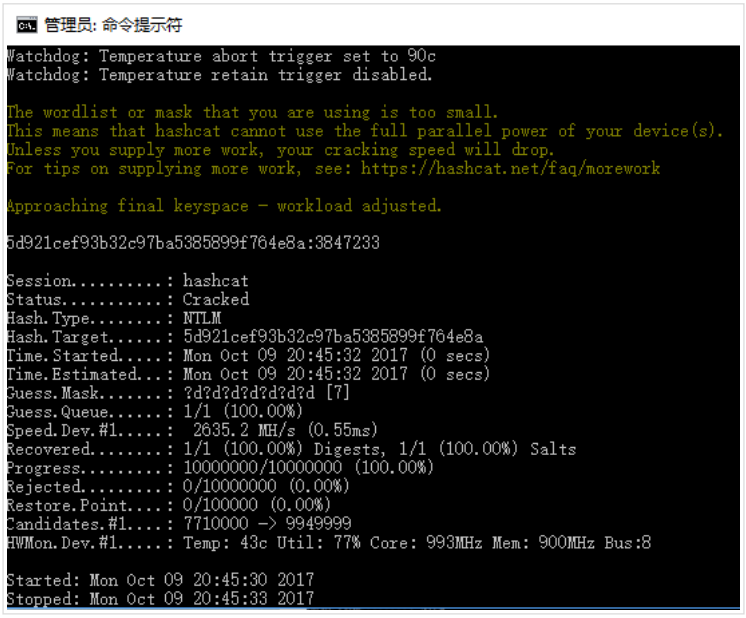
-o 输出文件，破解成功的密码存放的文件

–remove移除破解成功的hash，当hash是从文本中读取时有用，避免自 己手工移除已经破解的hash

–username 忽略用户名，如果你的hash文件中是username:hash这种格式只 需要指定这个参数，就不需要再手工编辑了

-r 指定规则文件，字典根据规则文件做变形，用于破解相似密码当-a指定为3 时，就是暴力破解模式，这个模式下需要自己指定mask和长度。

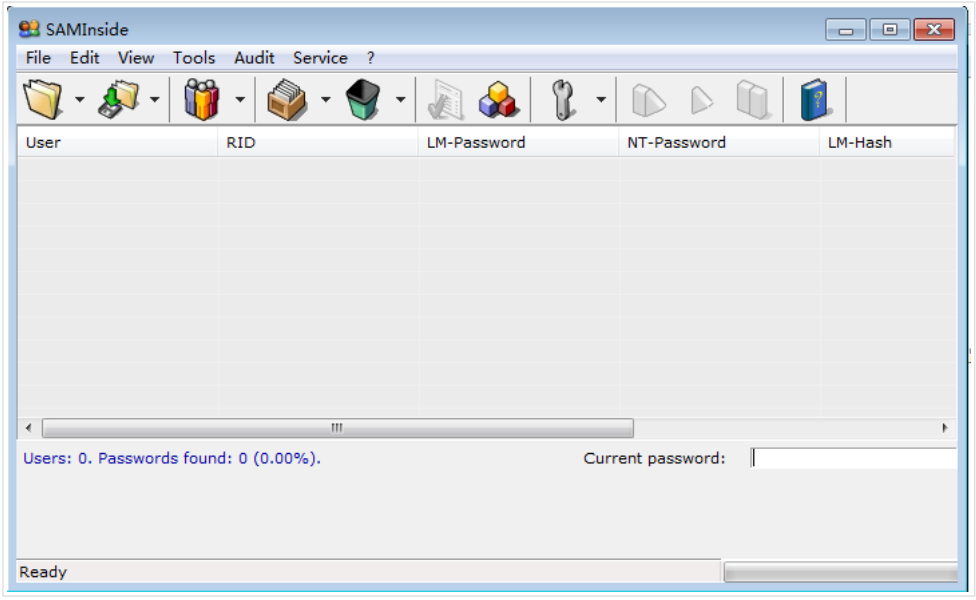
Hashcat-plus中以?l表示小写字母，?d表示数字，?u表示大写字母，?s表示所有可打印符号，?a代表所有可打印字符，它等于?l?u?d?s加在一起。



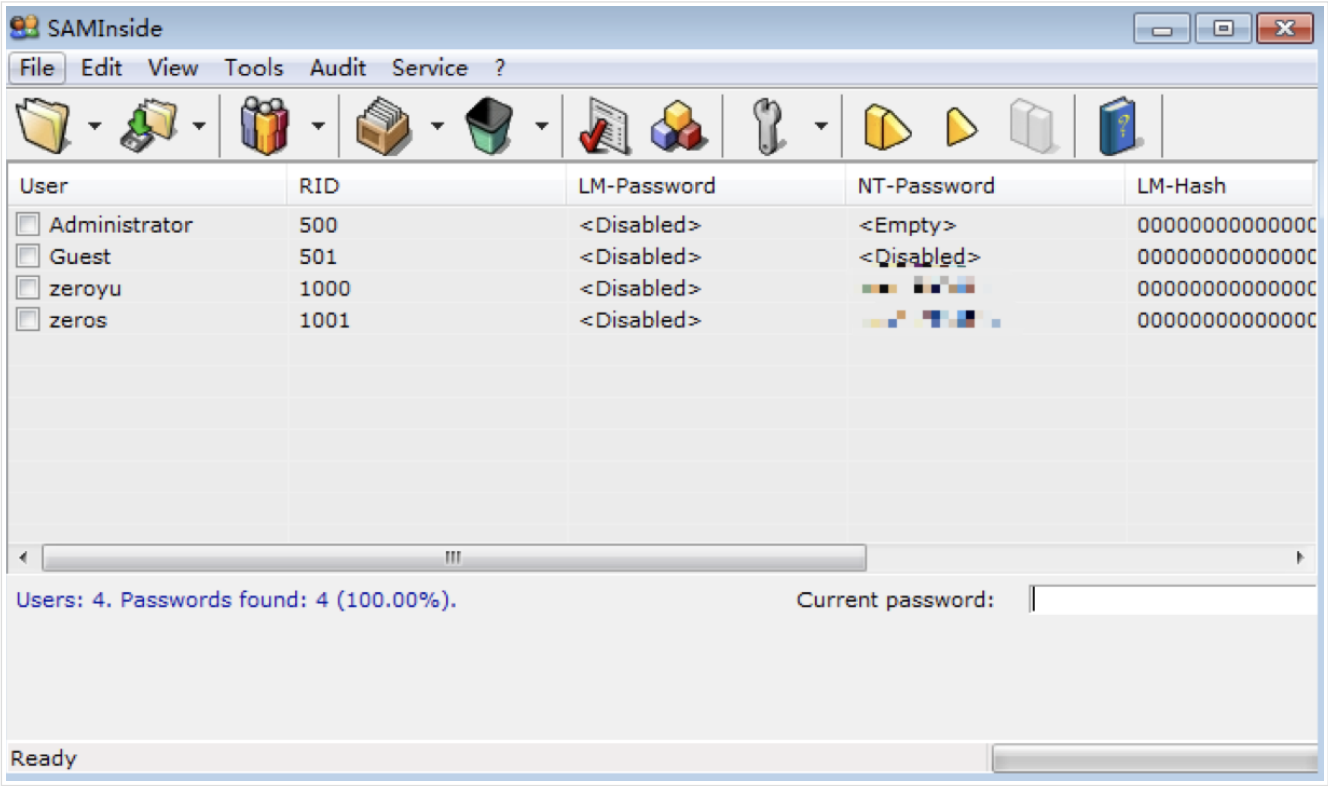
2.使用SAMInside.exe进行密码破解

环境：Windows10

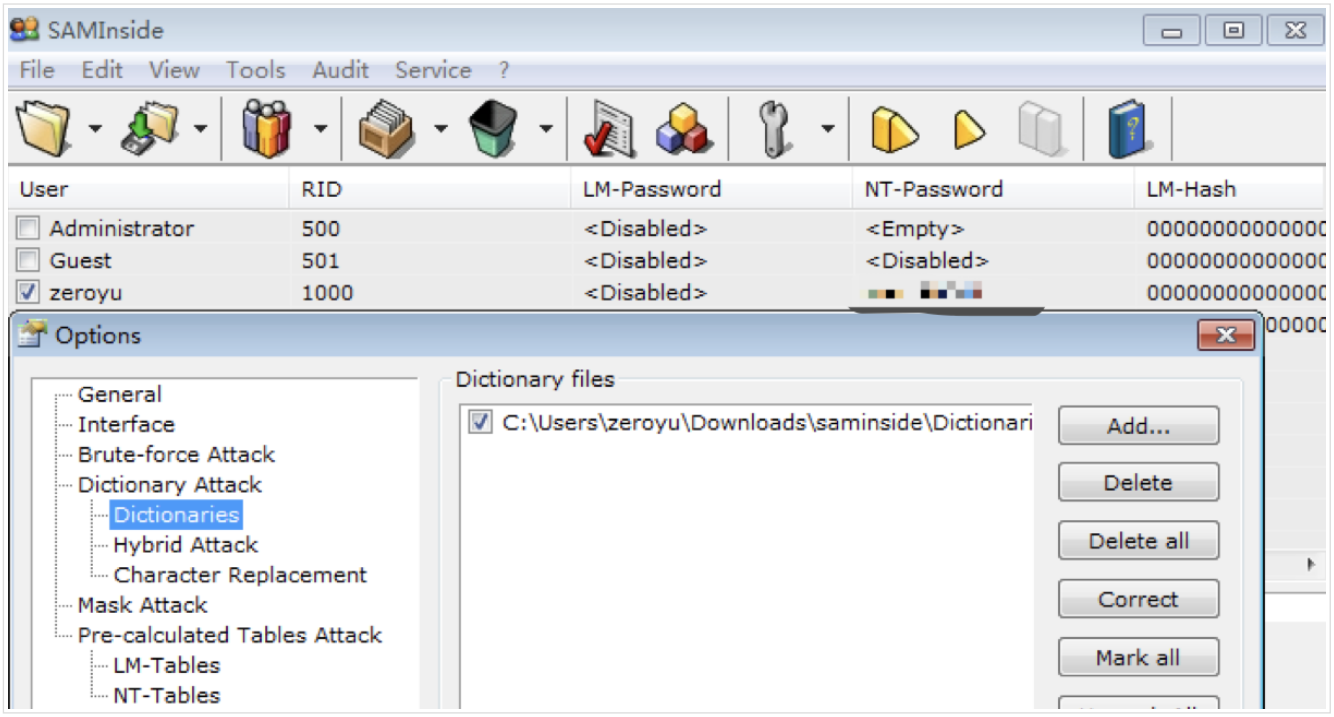
1）使用管理员身份运行SAMInside.exe



2）你可以选择使用Pwdump7获取口令之后将其导入SAMInside.exe进行破解；或者使用SAMInside.exe来直接获取本地口令进行破解（本例使用第二种方式，点击三个小人的图标然后选择import local users via scheduler将本地用户的hash导出来）。



3）选择用户加载字典来进行爆破，最终可以看到已经破解了口令

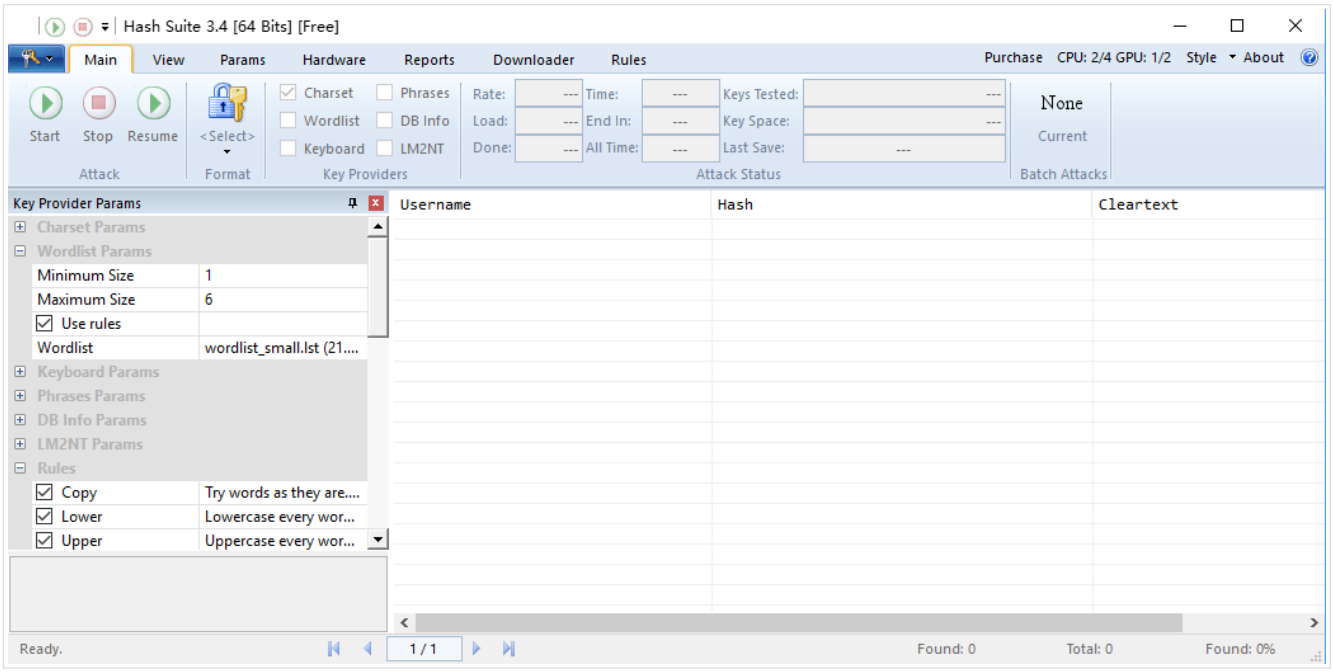


注：由于我之前载入字典破解了本地密码所以在每次导入时均会显示已经破解了密码

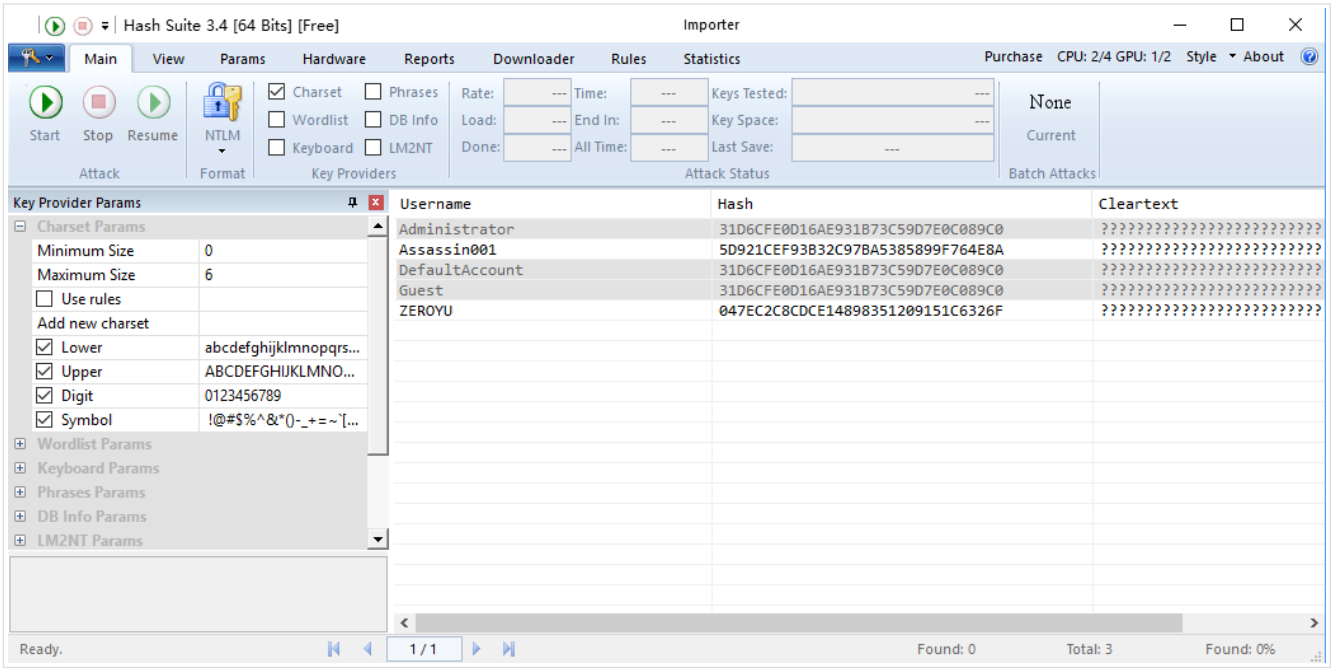
3.使用hashsuite可以直接进行windows的NTML HASH的抓取与破解。但是前提依旧是在管理员权限下进行

环境：windows10

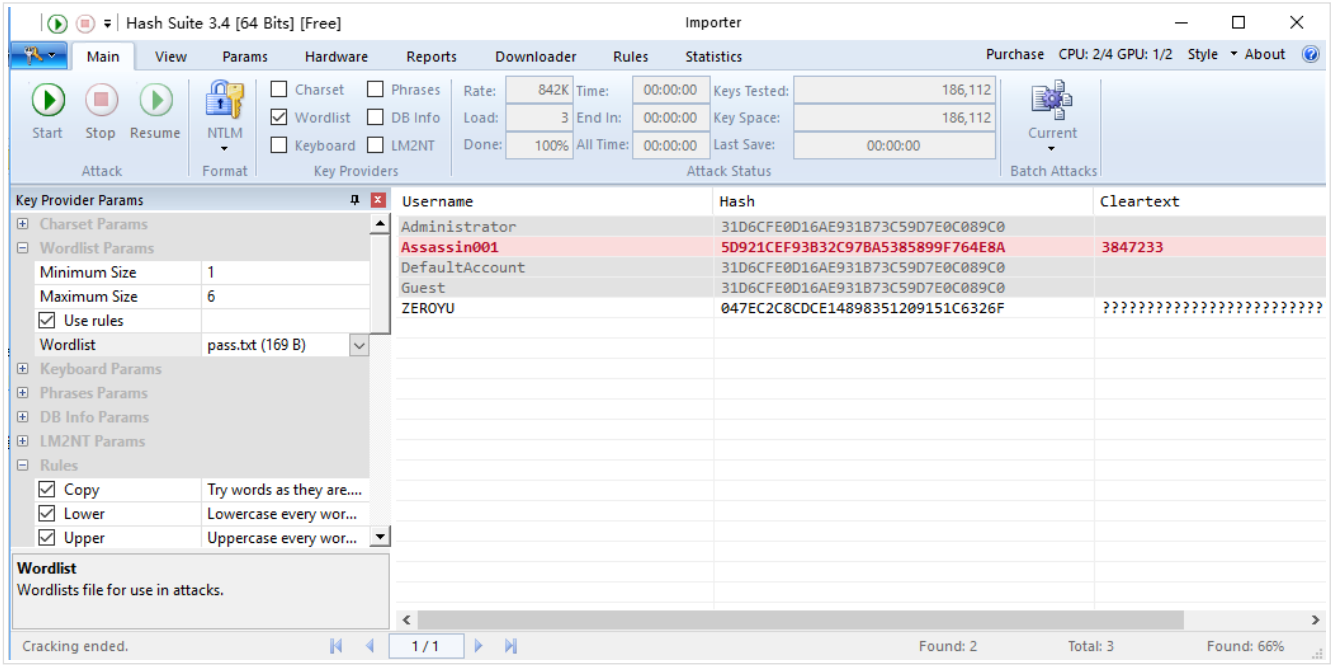
1）首先以管理员身份运行hashsuite



2）导入要破解的口令，在这里我们选择导入本地的口令（选择后软件会自动将口令进行提取）



3）之后我们选择使用字典破解的方式对账户Assassin001的口令进行破解



####2.Linux密码破解

知识概要：

‣head -n 2 /etc/passwd

root;x:0:0:root:/root:/usr/bin/zsh

daemon:x;1:1:daemon:/usr/sbin:/usr/sbin/nologin

以":"分隔，共有七个字段：

1.账号名称；2.密码（Linux早期密码存放地，现在均存在/etc/shadow中）；3.UID（用户标识符）；4.GID；5.用户信息说明列；6.主文件夹；7.shell

‣head -n 2 /etc/shadow

root:6XrLBeXo2$iYJYakUC6eBvRl40PnFKlemX7IjI7QkFu7f3qTZjIr.RBy3dp3YT3QWkDYxmKBmmzQO8FUXXbK72lnaz.GeSB0:17304:0:99999:7:::

daemon:*:17043:0:99999:7:::

以":"分隔，共有九个字段：

1.账号名称；2.密码；3.最近更新密码的日期；4.密码不可被更动的天数；5.密码需要重新更改的天数；6.密码需要更改期限前的警告天数；7.密码过期后的账号宽限时间；8.账号失效日期；9.保留

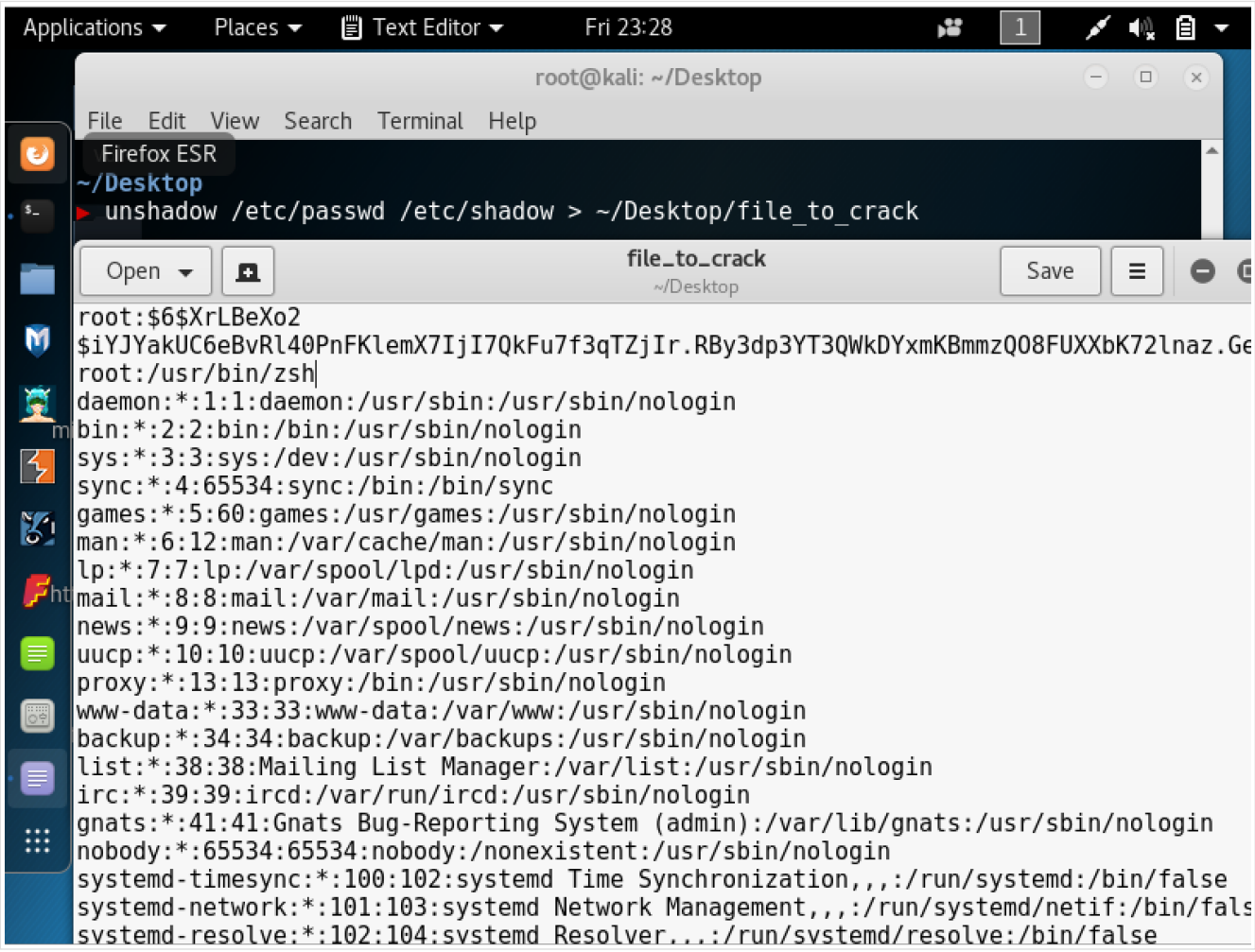
密码抓取：

环境：kali linux

前提：已经获取root权限(可以使用dirtycow.c等0day进行Linux的提权操作)

工具：mimipenguin(Linux下的mimikatz)

操作：



密码破解：

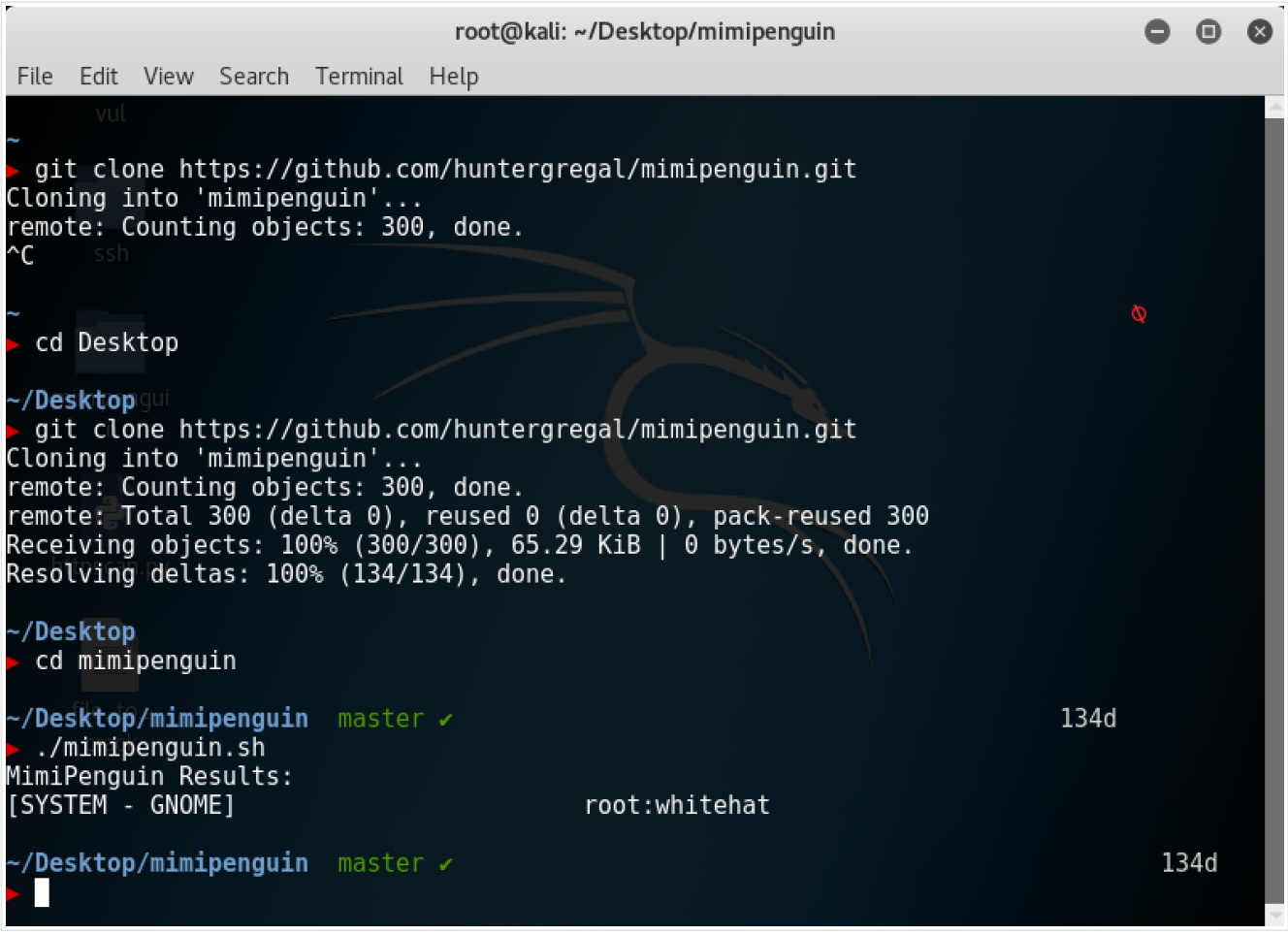
环境：kali linux

前提：已经获取root权限(可以使用dirtycow.c等0day进行Linux的提权操作)

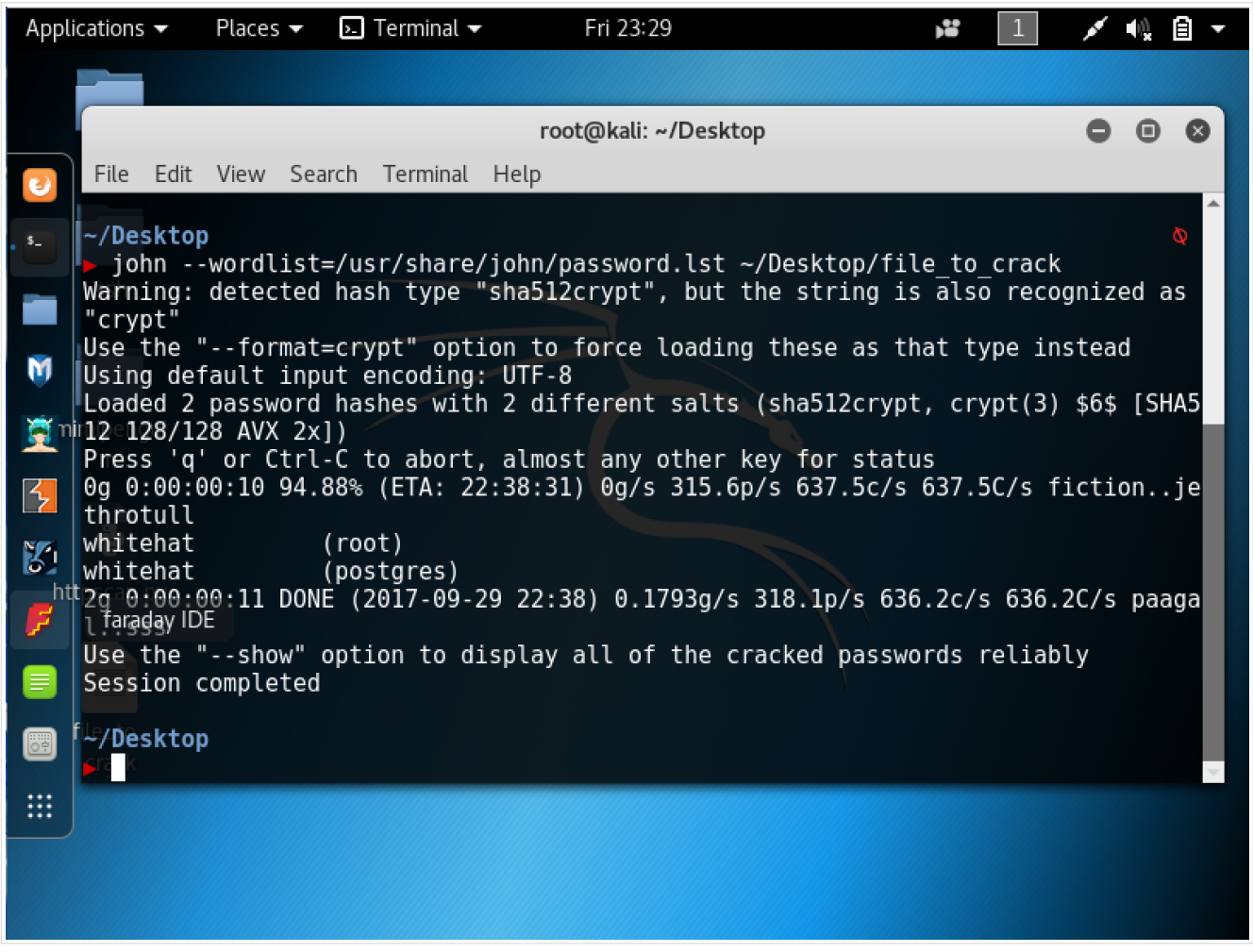
工具：John the ripper

操作：

1.使用unshadow命令创建1个含有用户名和密码详细信息的文件


root@kali: ~/Desktop/mimipenguin
File Edit View Search Terminal Help
git clone https://github.com/huntergregal/mimipenguin.git
Cloning into 'mimipenguin'...
remote: Counting objects: 300, done.
^C
cd Desktop
~/Desktop
git clone https://github.com/huntergregal/mimipenguin.git
Cloning into 'mimipenguin'...
remote: Counting objects: 300, done.
remote: Total 300 (delta 0), reused 0 (delta 0), pack-reused 300
Receiving objects: 100% (300/300), 65.29 KiB | 0 bytes/s, done.
Resolving deltas: 100% (134/134), done.
~/Desktop
cd mimipenguin
~/Desktop/mimipenguin master ✔ 134d
./mimipenguin.sh
MimiPenguin Results:
[SYSTEM - GNOME] root:whitehat
~/Desktop/mimipenguin master ✔ 134d

2.使用John来破解


Applications Places Terminal Fri 23:29
root@kali: ~/Desktop
File Edit View Search Terminal Help
~/Desktop
john --wordlist=/usr/share/john/password.lst ~/Desktop/file_to_crack
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) 6 [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 94.88% (ETA: 22:38:31) 0g/s 315.6p/s 637.5c/s 637.5C/s fiction..jethrotull
whitehat (root)
whitehat (postgres)
2g 0:00:00:11 DONE (2017-09-29 22:38) 0.1793g/s 318.1p/s 636.2c/s 636.2C/s paaga
Use the "--show" option to display all of the cracked passwords reliably
Session completed
~/Desktop
faraday IDE

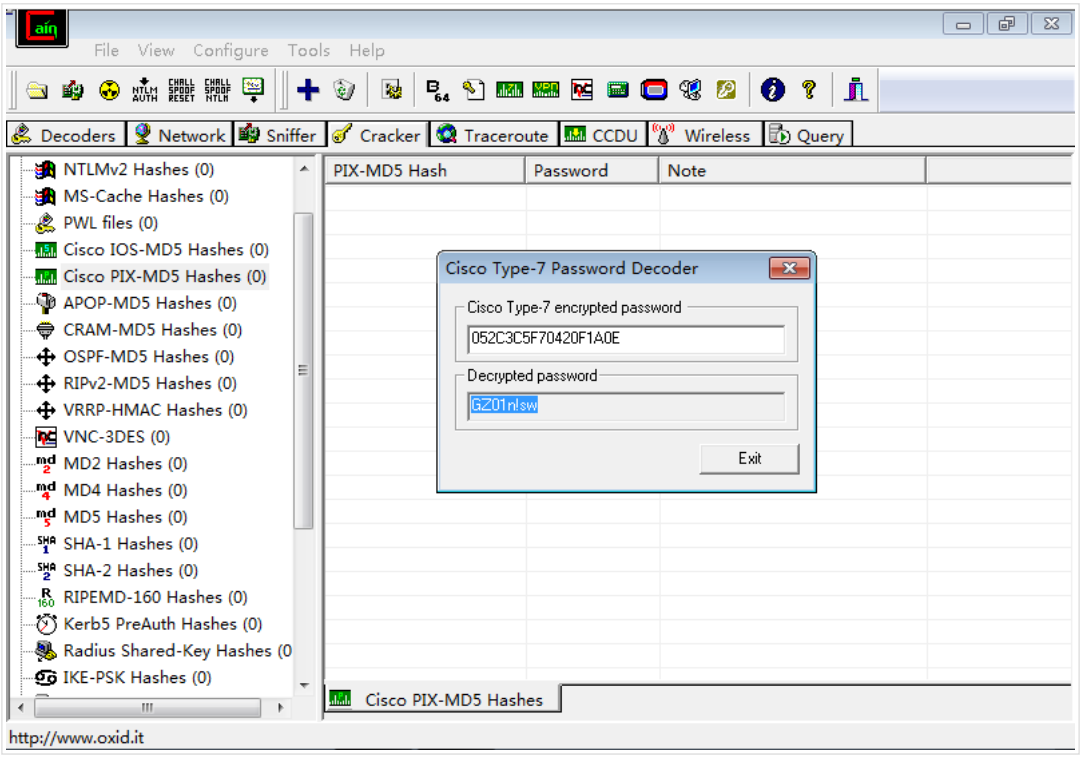
####3.网络设备密码破解

环境：windows7

工具：Cain

操作：

破解Cisco中Password 7加密，密文为052C3C5F70420F1A0E

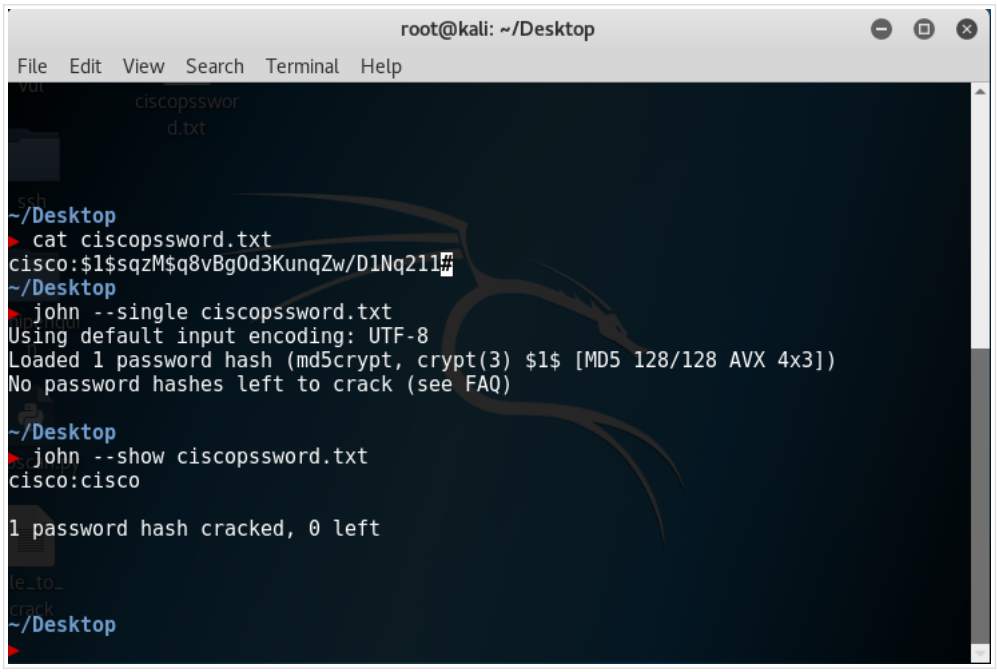


环境：kali linux

工具：John the ripper

操作：

1.将密文整理成cisco: 1sqzM$q8vBgOd3KunqZw/D1Nq211，保存在文件中然后使用john进行破解



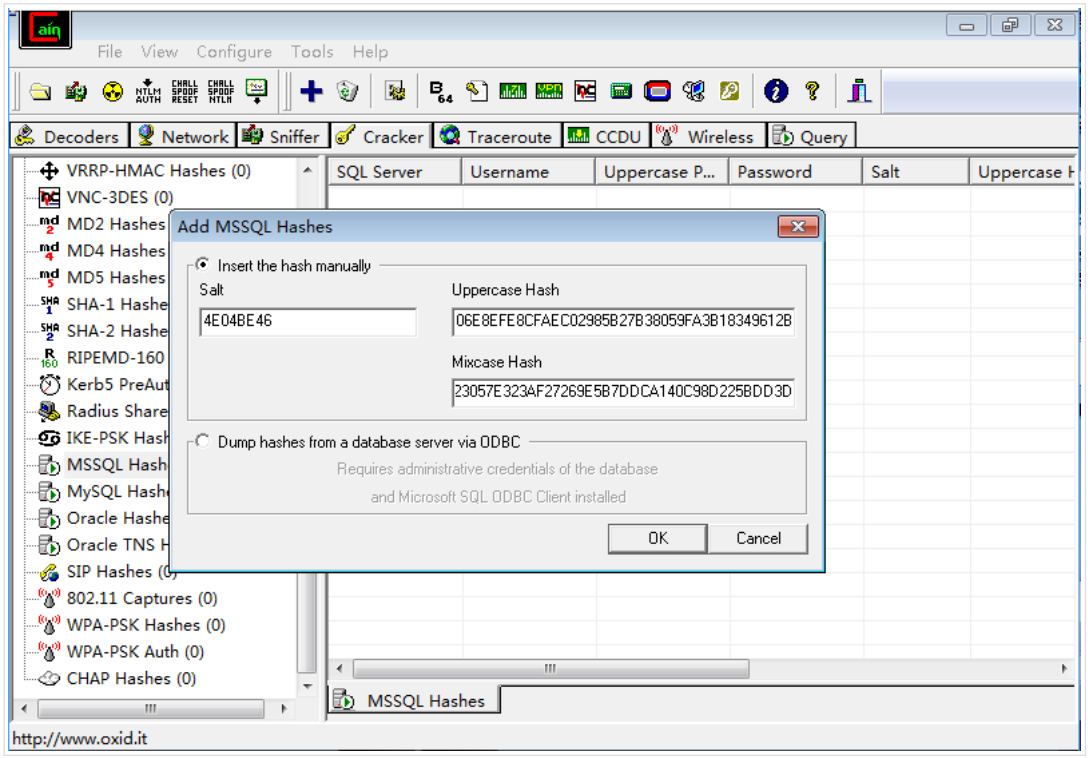
####4.数据库密码破解

环境：windows10 MSSQL数据库

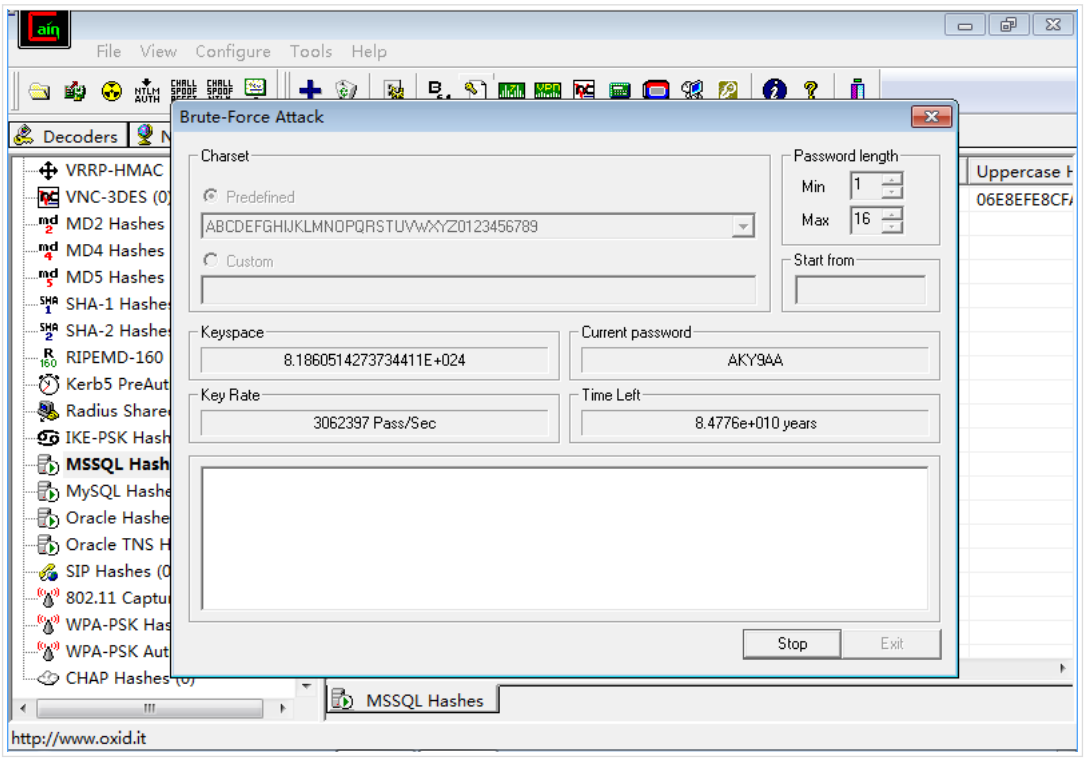
工具：Cain

操作：

1.添加Hash到队列



2.开始暴力破解



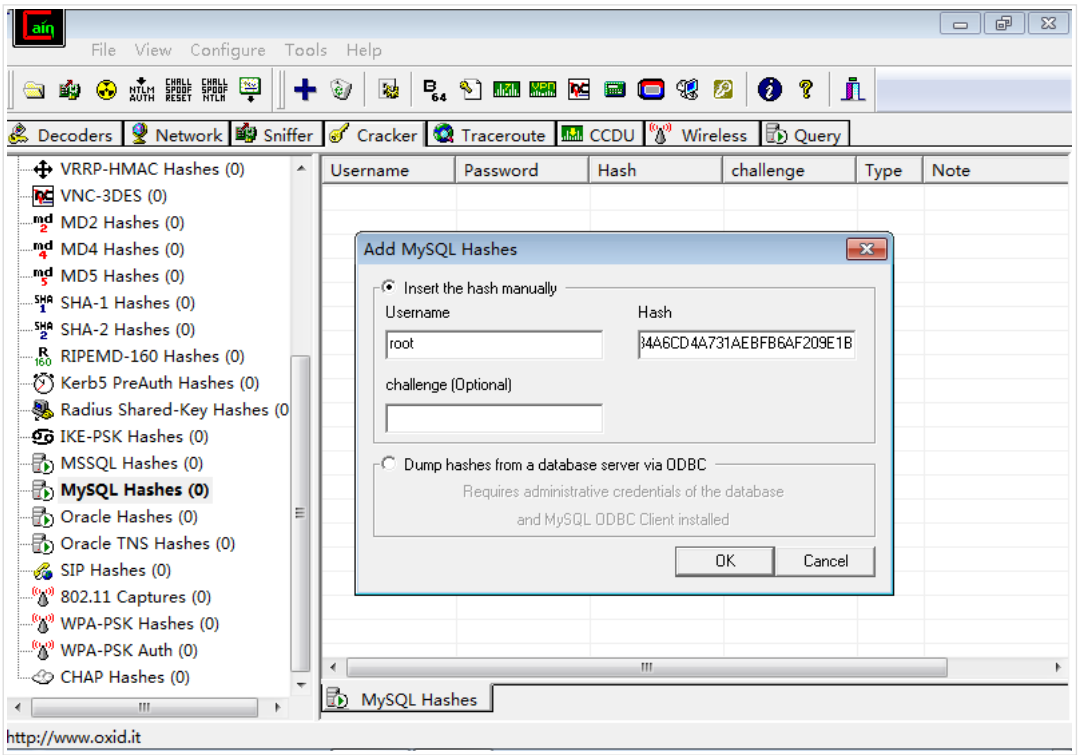
环境：windows10 MYSQL数据库

工具：Cain

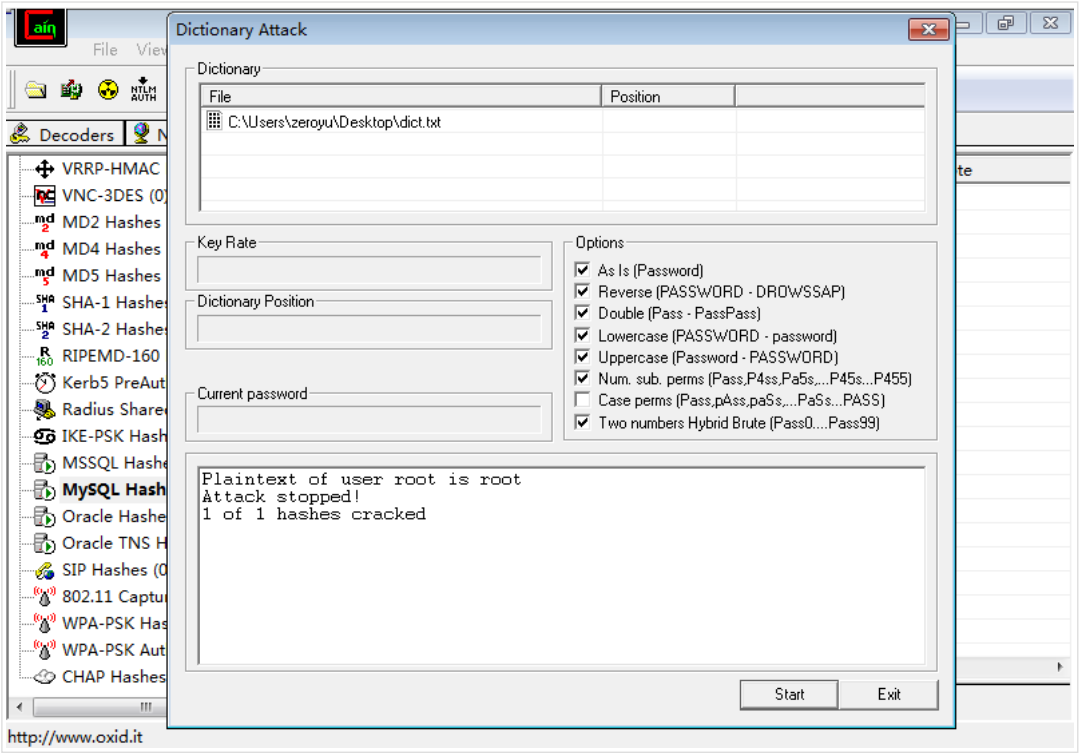
操作：

1.执行SELECT password,USER() FROM mysql.user;来获取密文

2.将MYSQL的密文导入Cain



3.使用字典攻击模式进行攻击

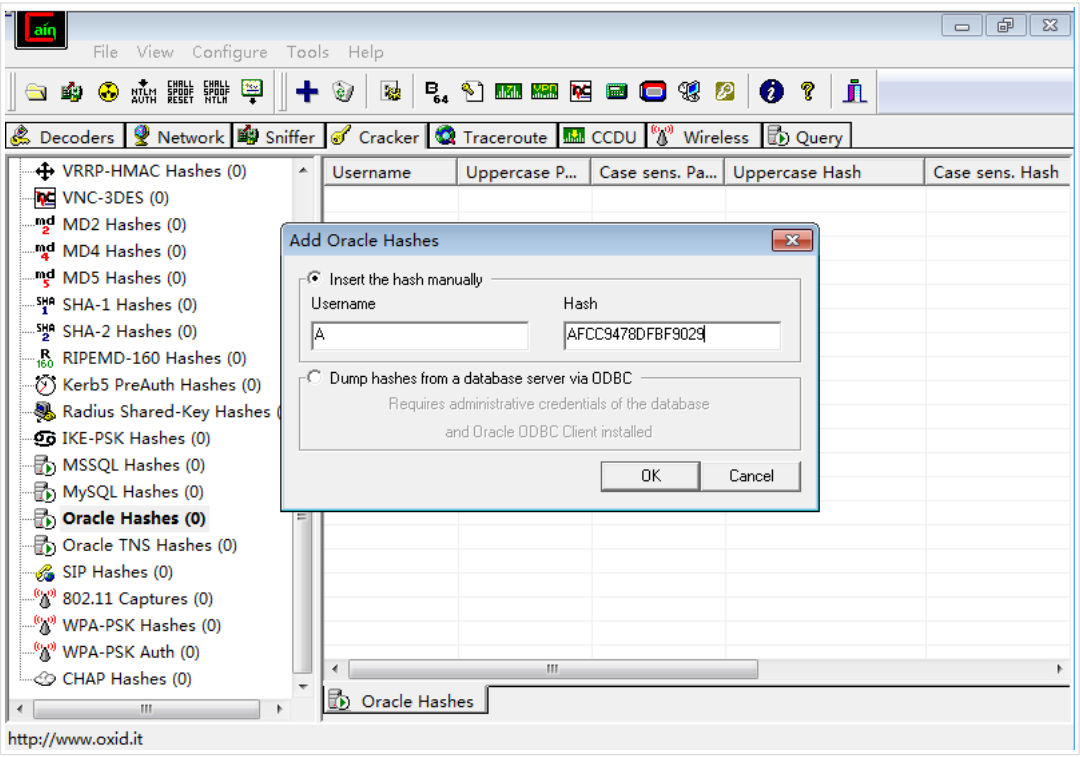


环境：windows10 Oracle数据库

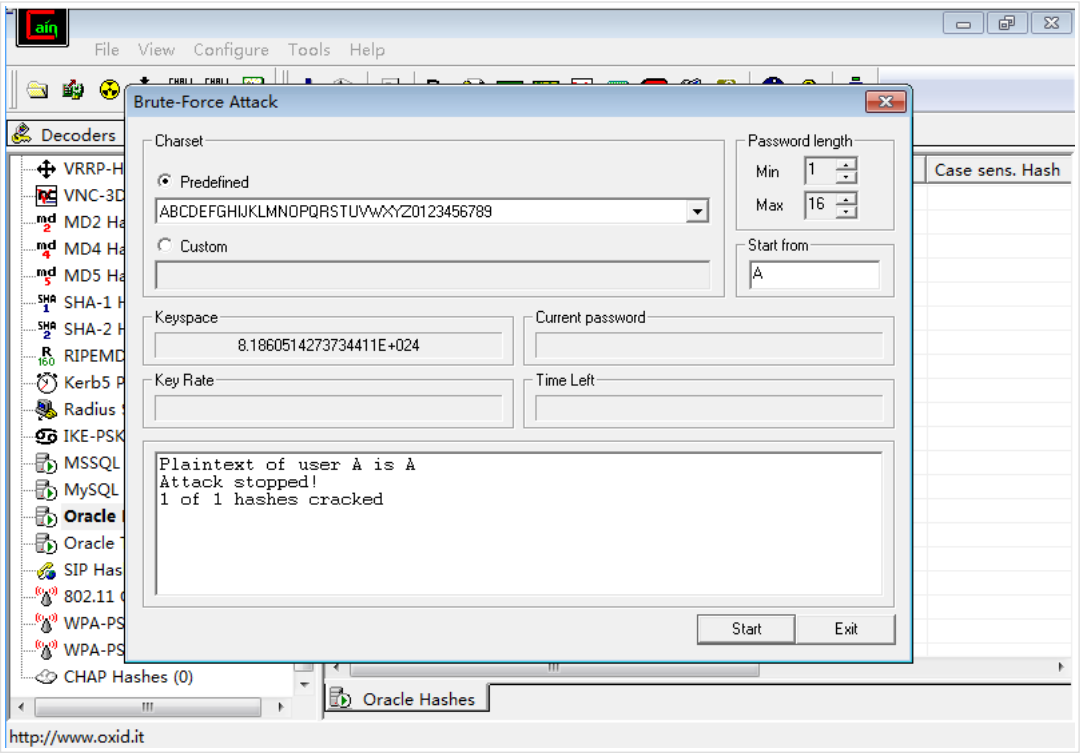
工具：Cain

操作：

1.导入Oracle数据库账号密码



2.进行暴力破解



####5.无线密码破解

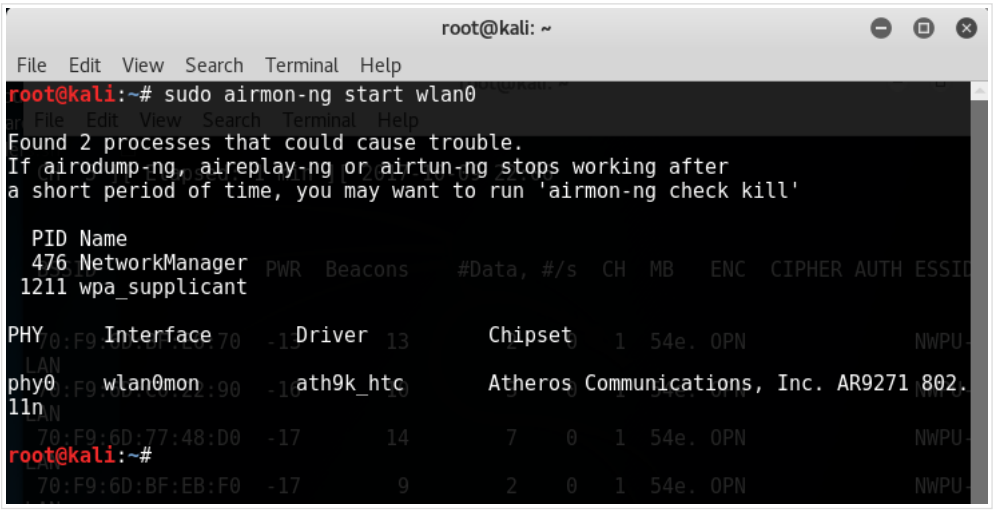
环境：kali linux、WPA/WPA2 PSK加密 无线路由器 TP-LINK_4D16、Windows10（hashcat进行GPU运算）

工具：外置USB无线网卡

操作：

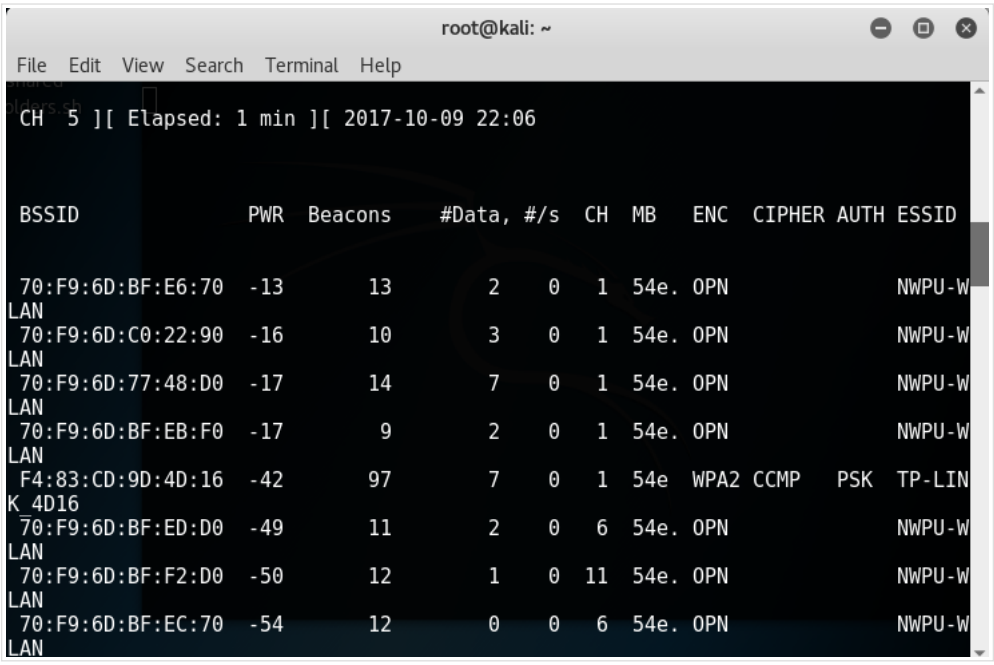
1. 把网卡切换为监听模式

```
sudo airmon-ng start wlan0
```



2.监听网络流量信息

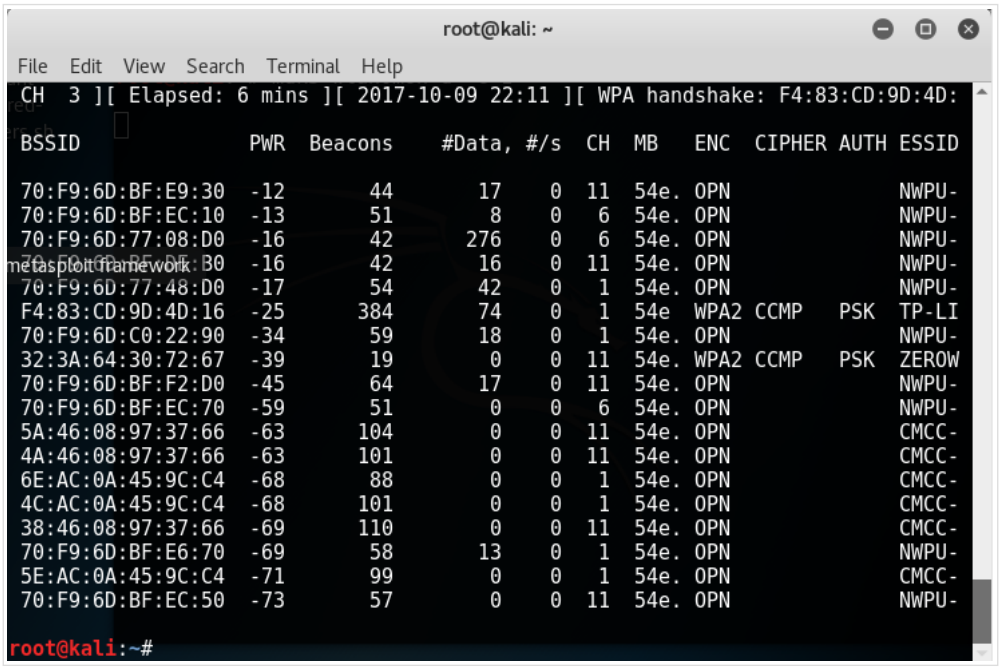
```
sudo airodump-ng -w file wlan0mon
```



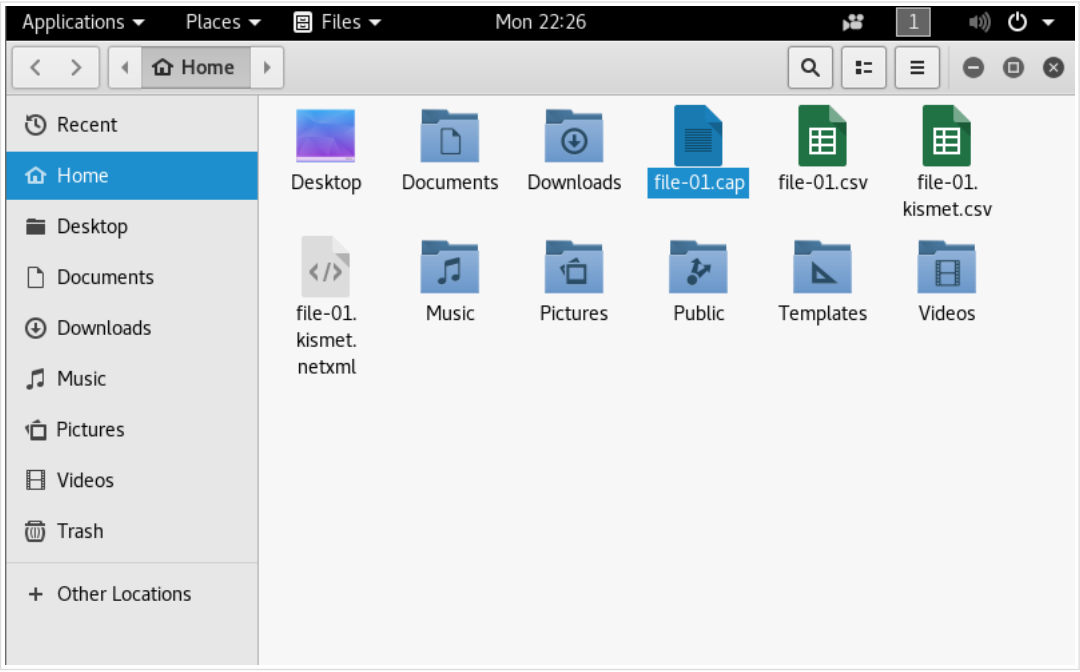
1. 使用mdk3， 强制断线路由的所有链接， 此次操作是为了能让aircrack抓到wifi的握手信息 ， -c为需要强制断线的信道：

```
1  mdk3 wlan0mon d -c 11
```

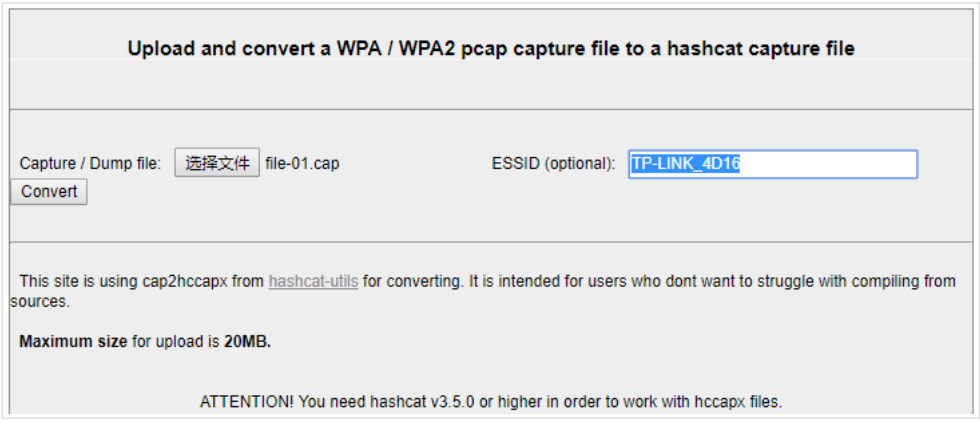
过了几分钟， 可以看到， 用户重新连接上了901路由， 我们也捕获到了handshake信息， 上面airodump-ng的命令窗口顶部出现了以下信息 WPA handshake ，此时直接ctrl + c ，停止捕获信息



在kali的Home目录下生成了了几个文件 ，此时的file-01.cap为最重要的文件：

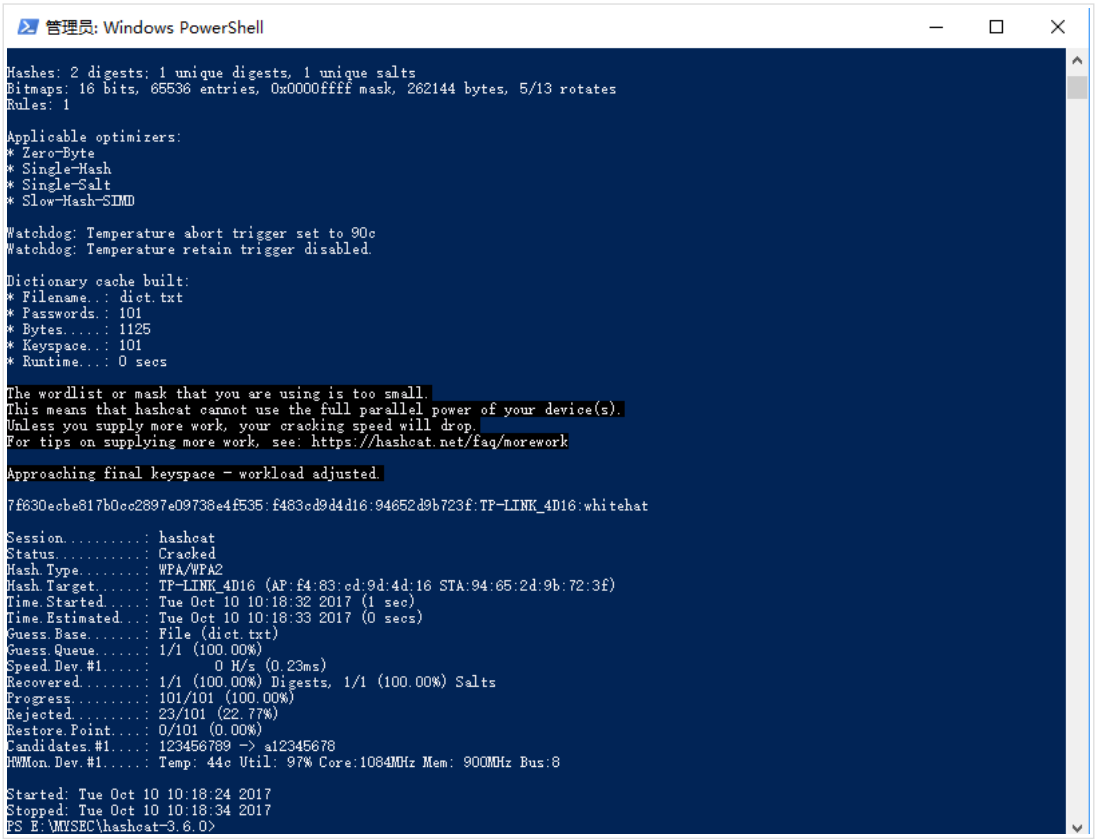


4.把文件转换为hccapx格式， 我们打开这个网站：https://hashcat.net/cap2hccapx/ ， 然后选择cap文件并点击covert按钮， 并下载一个hccapx格式的文件



5.网页会返回一个hccapx的文件， 使用hashcat命令破解， 参数dict.txt为生成的字典文件 ， -m参数2500代表破解的方式为WPA/WPA2， 999.hccapx为生成的文件， 最后破解出来的密码为whitehat：

PS E:\MYSEC\hashcat-3.6.0> .\hashcat64.exe -m 2500 999.hccapx dict.txt



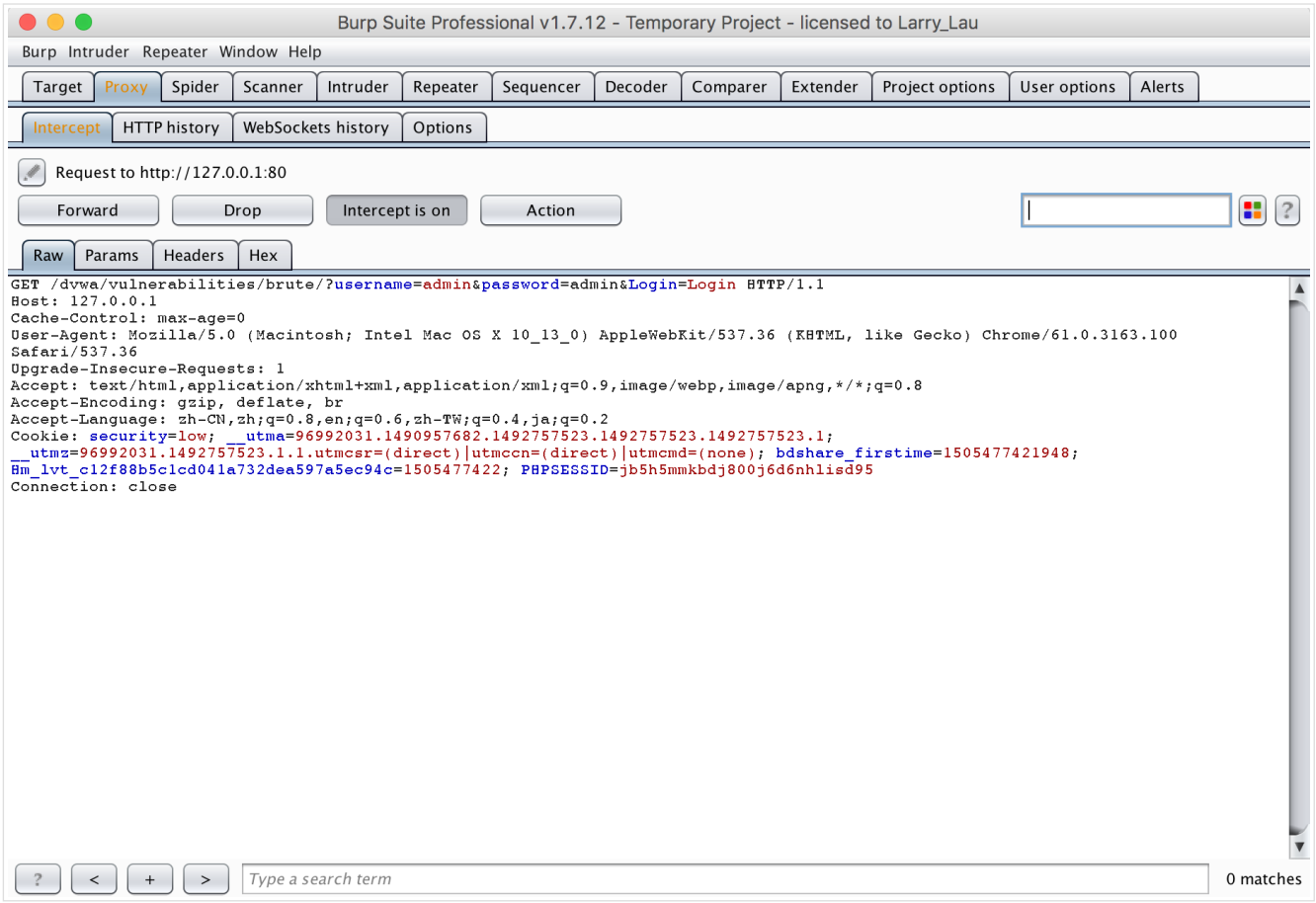
####6.web应用破解

环境：Windows10（phpstudy搭建漏洞靶场DVWA的爆破模块）

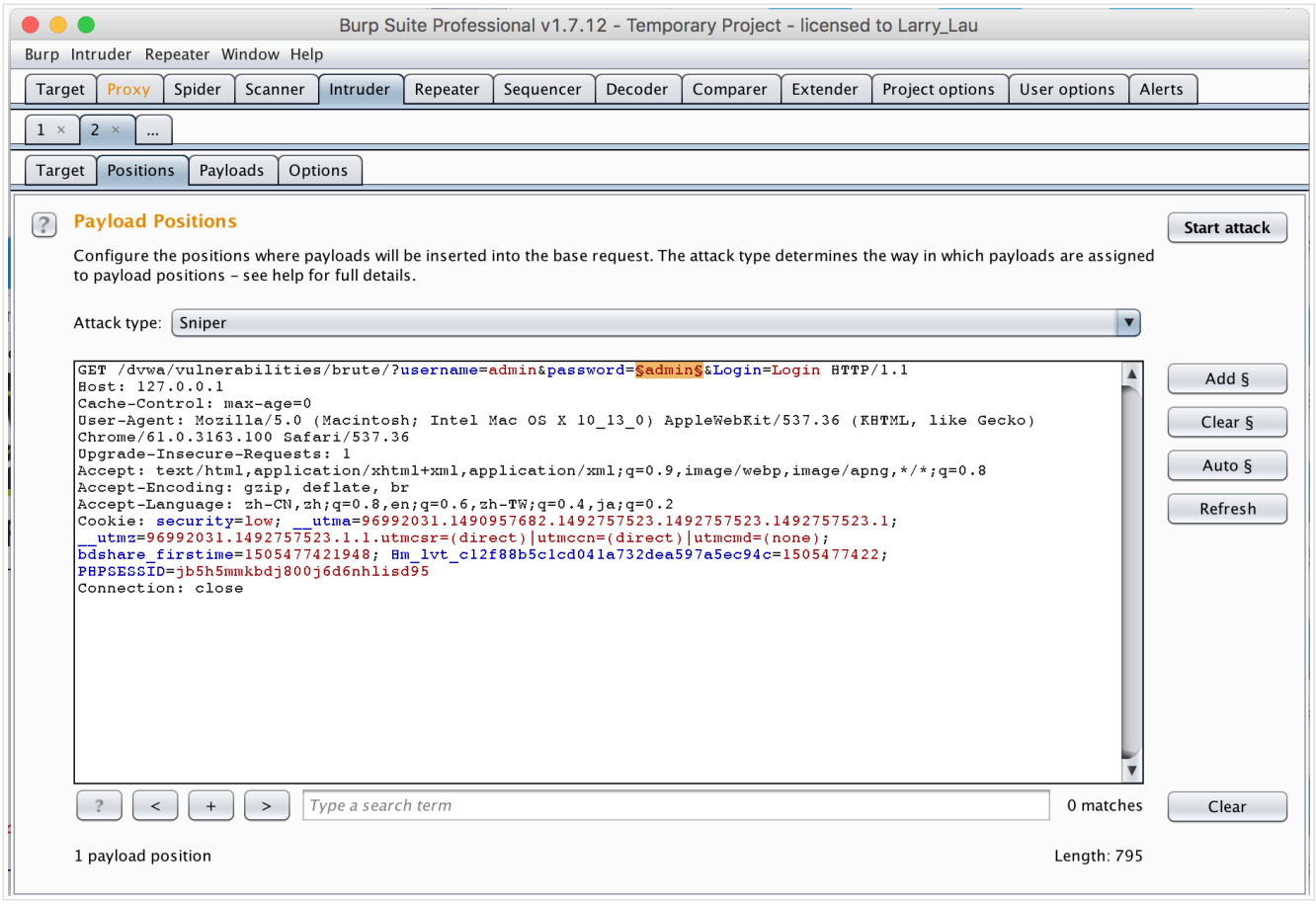
工具：burpsuite

操作：

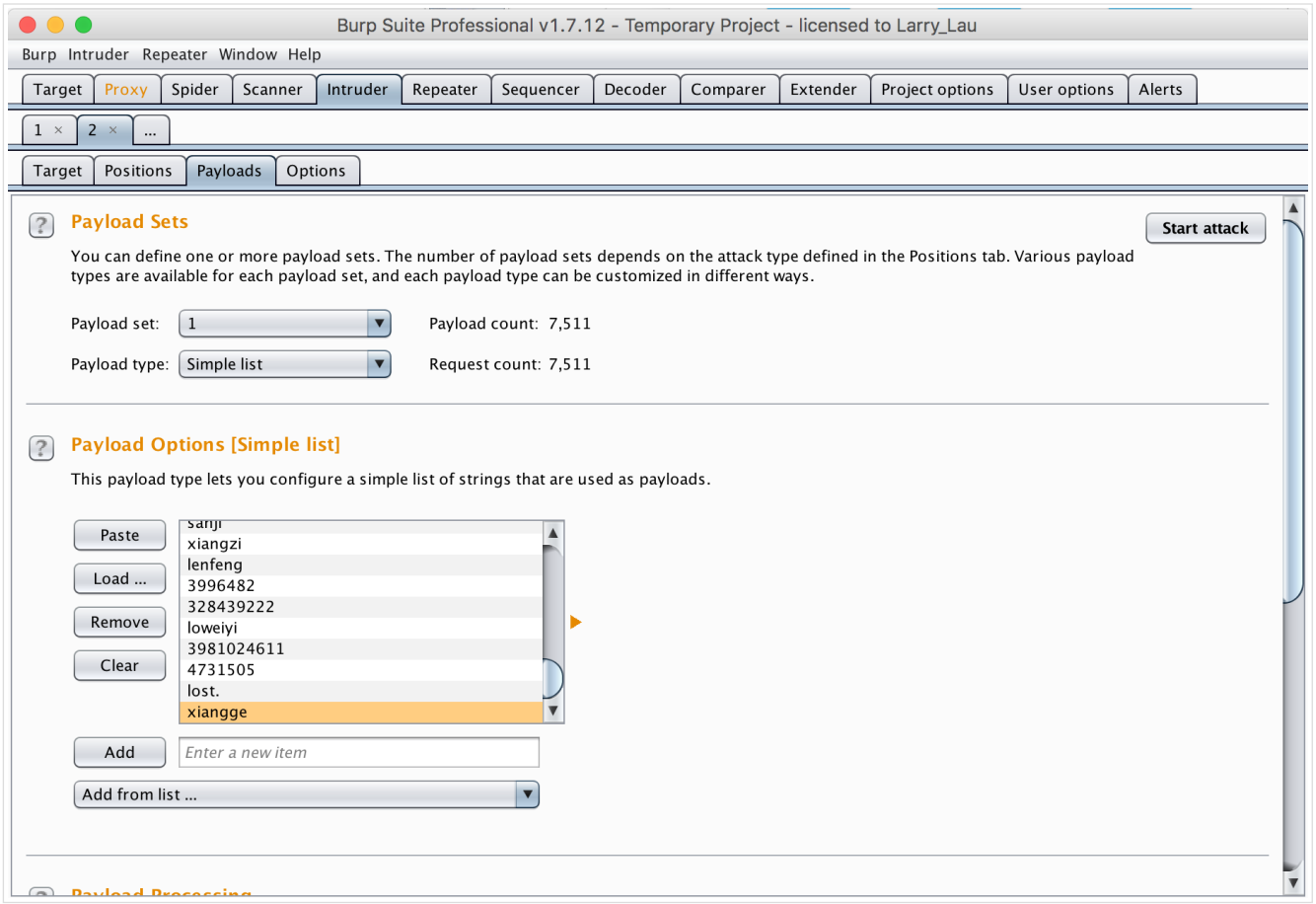
1.使用burpsuite抓取登录时候的数据包



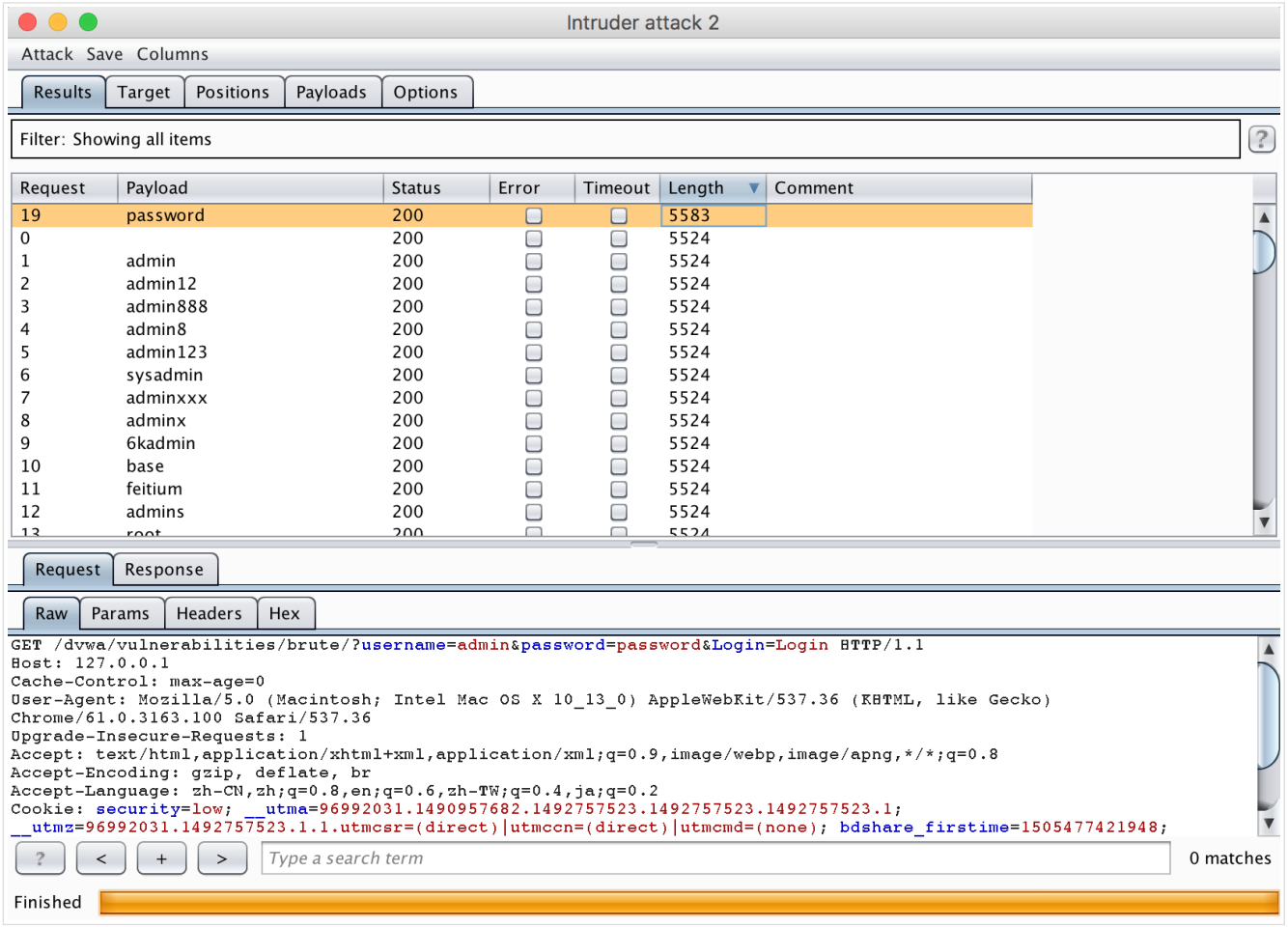
2.将数据包发送至Intruder模块并对攻击点进行标注



3.载入攻击字典并进行暴力破解



4.暴力破解后效果



5.验证破解密码是否正确（一般观察Length和Status来判断正确的密码）