Cupp

CUPP是通用的用户密码分析器，最常见的身份验证形式是用
户名和密码或密码的组合。如果这两个值都匹配存储在本地存储表中的值，则将对用户进行连接身份验证。密码强度是通过密码技术或基于库的交替值自动测试来衡量猜测或破解密码的困难程度。

弱密码可能很短，或者只使用幻影字符，使解密变得简单。弱密码也可以是一个很容易被描述用户的人猜到的密码，比如生日、昵称、地址、宠物或亲戚的名字，或者像上帝、爱情、金钱或密码这样的普通单词。
这就是为什么Cupp诞生的原因，它可以用于法律渗透测试或法医犯罪调查。

The most common form of authentication is the combination of a username and a password or passphrase. If both match values stored within a locally stored table, the user is authenticated for a connection. Password strength is a measure of the difficulty involved in guessing or breaking the password through cryptographic techniques or library-based automated testing of alternate values.
A weak password might be very short or only use alphanumberic characters, making decryption simple. A weak password can also be one that is easily guessed by someone profiling the user, such as a birthday, nickname, address, name of a pet or relative, or a common word such as God, love, money or password.
That is why CUPP was born, and it can be used in situations like legal penetration tests or forensic crime investigations.

二，所需环境
如果想让CUPP在Windows上运行，则需要使用到Python 3 环境。

本文主要在KALI LINUX环境下进行使用，由于KALI未将CUPP所预装，所以需要在更新仓库中调取。

安装命令如下：
apt-get install cupp
安装cupp程序

如果未查到有cupp相关信息可以换一个官方源，或者从github上进行下载。

三，使用文档

```
  cupp.py!                 # Common
     \                     # User
      \   ,,               # Passwords
       \  (oo)__           # Profiler
          (__)    )\
             ||--|| *      [ Muris Kurgas | j0rgan@remote-exploit.org ]
```

For more help take a look in docs/README
想要获得更多的帮助，请查看docs/README

Global configuration file is cupp.cfg
全局配置文件是cup .cfg

-i Interactive questions for user password profiling
-用于用户密码分析的交互式问题

-w Use this option to improve existing dictionary,
使用这个选项来改进现有的字典，

or WyD.pl output to make some pwnsauce
或WyD.pl输出来制作pwnsauce

-l Download huge wordlists from repository
-我从资料库下载大量的单词表

-a Parse default usernames and passwords directly from Alecto DB.

-直接从Alecto数据库解析默认用户名和密码。
Project Alecto uses purified databases of Phenoelit and

CIRT
Alecto项目使用了表型和CIRT纯化数据库

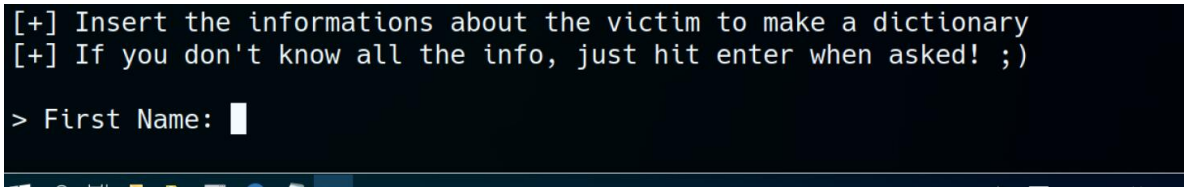
which where merged and enhanced.
其中合并和增强。

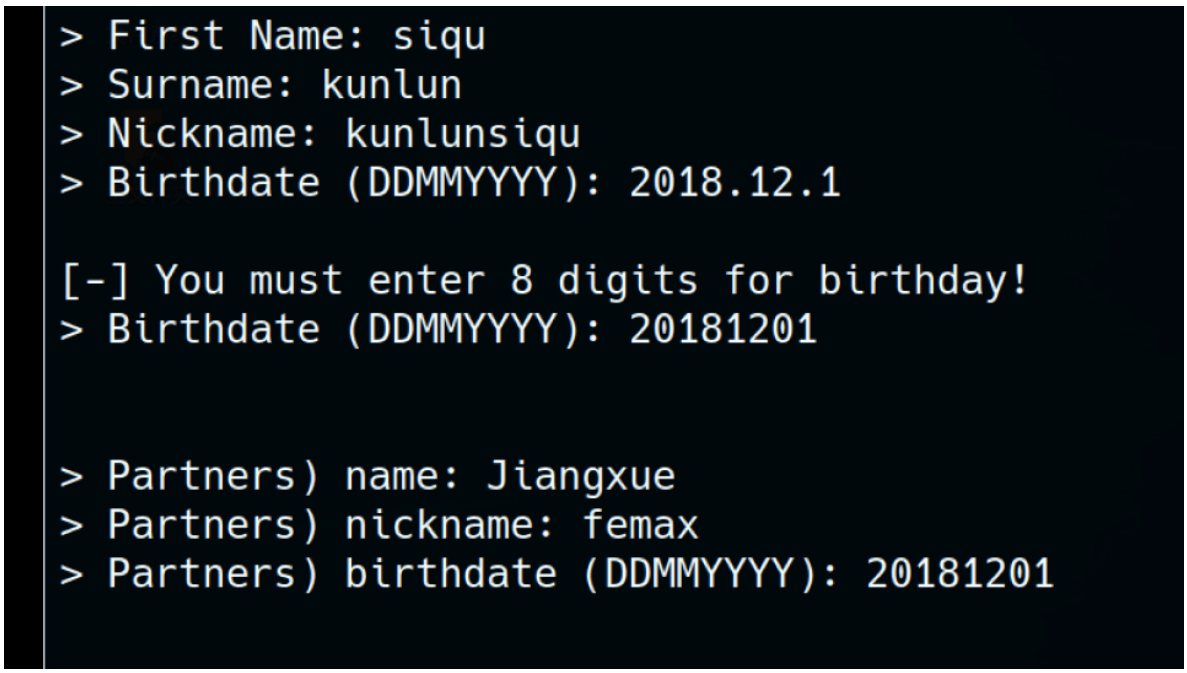
-v Version of the program
-v版本的程序

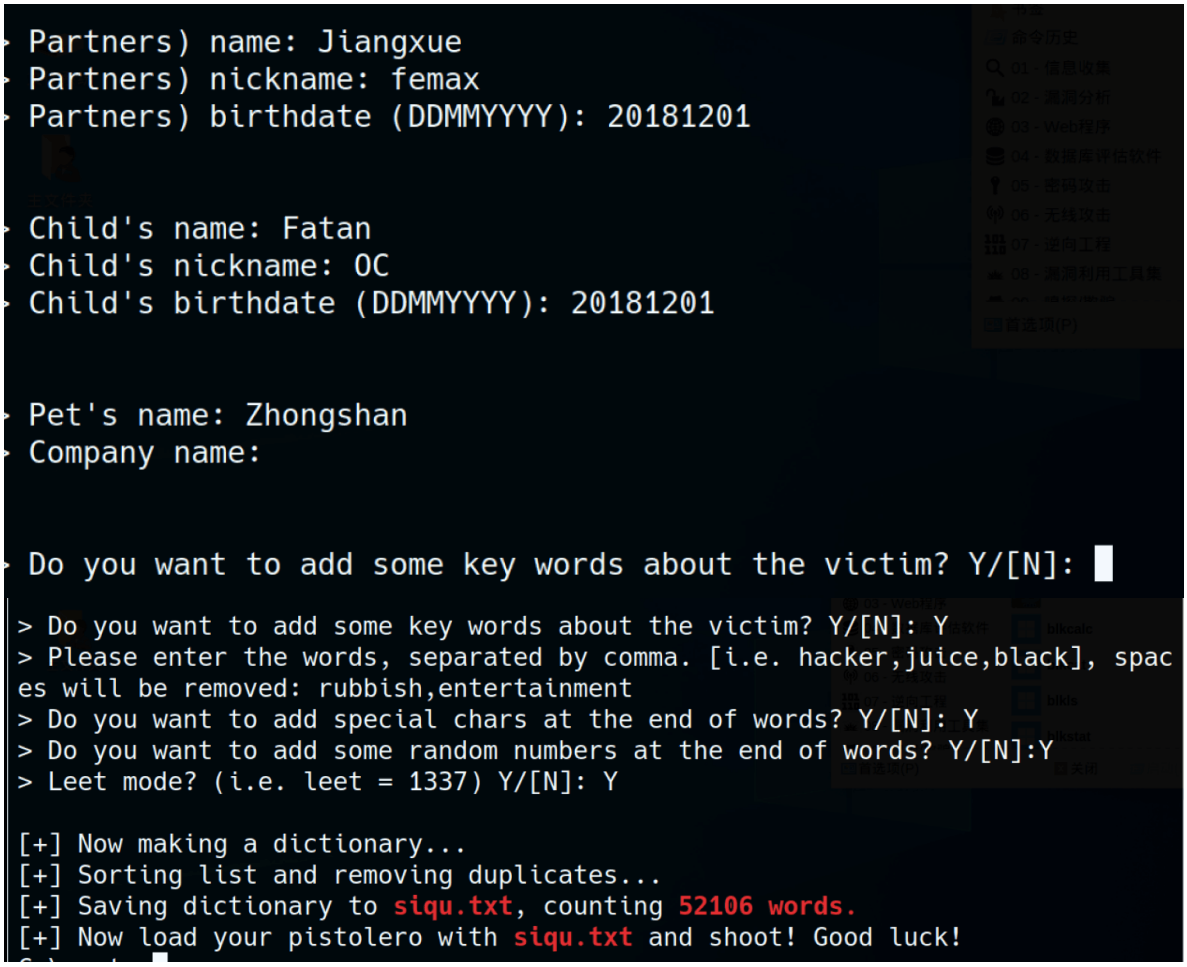
四，命令演示
cupp -i
使用交互式进行生成密码字典

当你看到以下图片则表明你运行成功了，按照CUPP进行回答你想生成对应人的问题即可。
此时他会提醒你两句话：

[+]插入受害者的信息，制作一本字典
[+]如果你不知道所有的信息，请按回车键!,)







五，命令翻译
[+]插入受害者的信息，制作一本字典
Insert victim information and make a dictionary

[+]如果你不知道所有的信息，请按回车键!
[+] if you don't know all the information, press enter!

>名:siqu
> name: siqu

>姓:昆仑
> surname: kunlun

>昵称:klsq
> nickname: KLSQ

出生日期(DDMMYYYY): 20181201
Date of birth (DDMMYYYY): 20181201

姓名:jan
Name: jan

昵称:xuxu
Nickname: xuxu

出生日期(DDMMYYYY): 20201201
Date of birth (DDMMYYYY): 20201201

宝宝的名字:笑笑
Baby name: xiaoxiao

>孩子的昵称:Zangli
>'s nickname :Zangli

出生日期(DDMMYYYY): 20171201
Date of birth (DDMMYYYY): 20171201

>宠物的名字:王彩
> pet name: wangcai

公司名称:江雪
Company name: jiang xue

你想添加一些关于受害者的关键词吗? Y / [N] : Y
Do you want to add some keywords about victims? Y / [N]: Y

请输入用逗号分隔的单词。
Please enter comma-separated words.

(即。(i.e.黑客，果汁，黑]，空格将被删除:狗，洞，嘿，jx，江雪，fatan,oc
Hacker, juice, black], Spaces will be removed: dog, hole, hey, jx, jiangxue, fatan,oc

你想在单词后面加上特殊的字符吗? Y / [N]: Y
Do you want to put special characters after words? Y / [N] : Y

你想在单词后面加一些随机数吗? Y / [N]: Y
Do you want to add random Numbers after words? Y / [N] : Y

>民事法庭模式? Y/[N]: 2020
> civil court model? Y / [N] : 2020

现在编一本字典.....
Now make up a dictionary...

[+]排序列表和删除重复...
[+] sort lists and delete duplicates...

[+]保存字典给四渠。
[+] save the dictionary to the four channels.

txt，一共有33872个单词。
TXT, 33,872 words.

[+]现在加载您的手枪与siqu.txt和射击!
[+] now load your pistol with siqu.txt and shoot!

好运！
Good luck!

六，查看字典

more siqu.txt

查看siqu.txt文件