【网络取证篇】suy网络工具包

原创

NDASH 于 2020-11-16 21:26:23 发布 546 收藏 2

分类专栏： 物联网取证 # 网络取证 文章标签： 网络安全 信息安全

本文链接：https://blog.csdn.net/NDASH/article/details/109729918

物联网取证 同时被 2 个专栏收录

4 篇文章 2 订阅

订阅专栏

网络取证

9 篇文章 1 订阅

订阅专栏

suy网络工具包及补充说明

经常查询各类信息用网页收藏夹不是太方便，偷了个懒，把常用的一些查询网站借助Rolan工具汇总成工具箱，没什么介绍的，所见即所得，在文档里补充了其它一些网络安全资源，请忽用于非法用途，仅供研究学习。 —【suy】

一、Whois查询

主要是查询网站的whois信息

二、域名查询

查询域名、子域名等信息，根据相关信息如手机号、QQ号、邮箱等进行下一步的反查。

（一）子域名

1.https://github.com/We5ter/Scanners-Box/blob/master/README_CN.md 子域名枚举类

2.https://github.com/lijiejie/subDomainsBrute (经典的子域名爆破枚举脚本)

3.https://github.com/ring04h/wydomain (子域名字典穷举)

4.https://github.com/le4f/dnsmaper (子域名枚举与地图标记)

5.https://github.com/0xbug/orangescan (在线子域名信息收集工具)

6.https://github.com/TheRook/subbrute （根据DNS记录查询子域名)

7.https://github.com/We5ter/GoogleSSLdomainFinder (基于谷歌SSL透明证书的子域名查询脚本)

8.https://github.com/mandatoryprogrammer/cloudflare_enum （使用CloudFlare进行子域名枚举的脚本）

9.https://github.com/18F/domain-scan (A domain scanner）

10.https://github.com/Evi1CLAY/Cool … Python/DomainSeeker（多方式收集目标子域名信息）

11.子域名扫描器

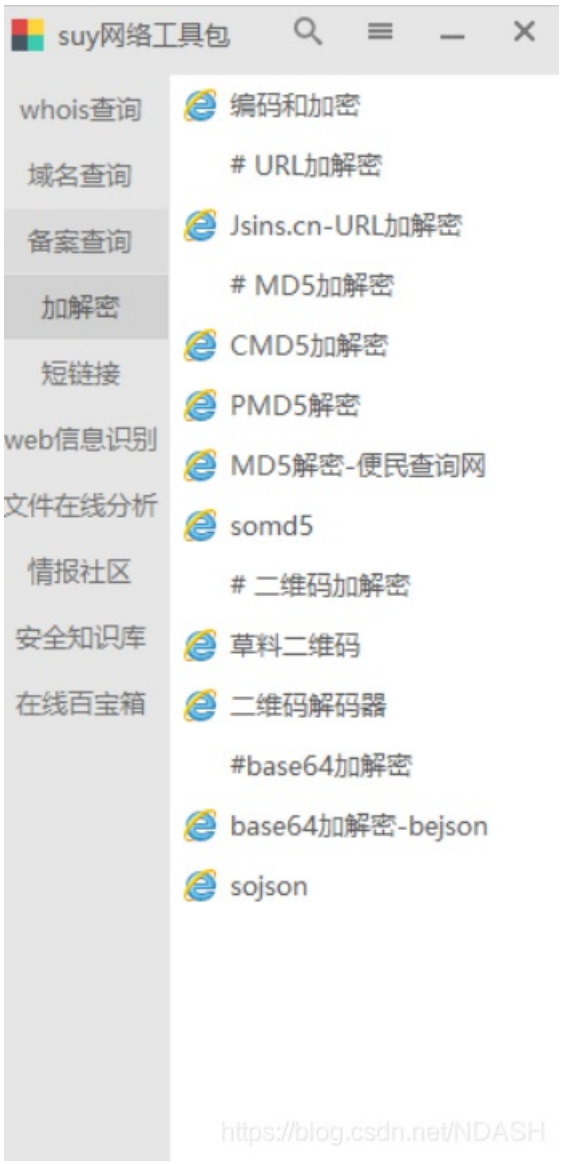
https://github.com/lijiejie/subDomainsBrute

三、备案查询

查询网站备案信息等

四、加解密

对一些网站或应用中涉及到的抓包数据进行解密，常见有MD5、base64加密。



（一）密码破解

1、密码破解工具

https://github.com/shinnok/johnny

2、本地存储的各类密码提取利器

https://github.com/AlessandroZ/LaZagne

（二）URL加解密

（三）MD5加解密

（四）二维码加解密

可对二维码解密获取真实链接

（五）信息隐写

1、隐写检测工具

https://github.com/abeluck/stegdetect

五、短链接

列举了一些网站短链接生成还原的网站，主要针对抓包获取到的网站，发现域名查询不到，且链接较短的情况下，判断是否被转换为了短链接。

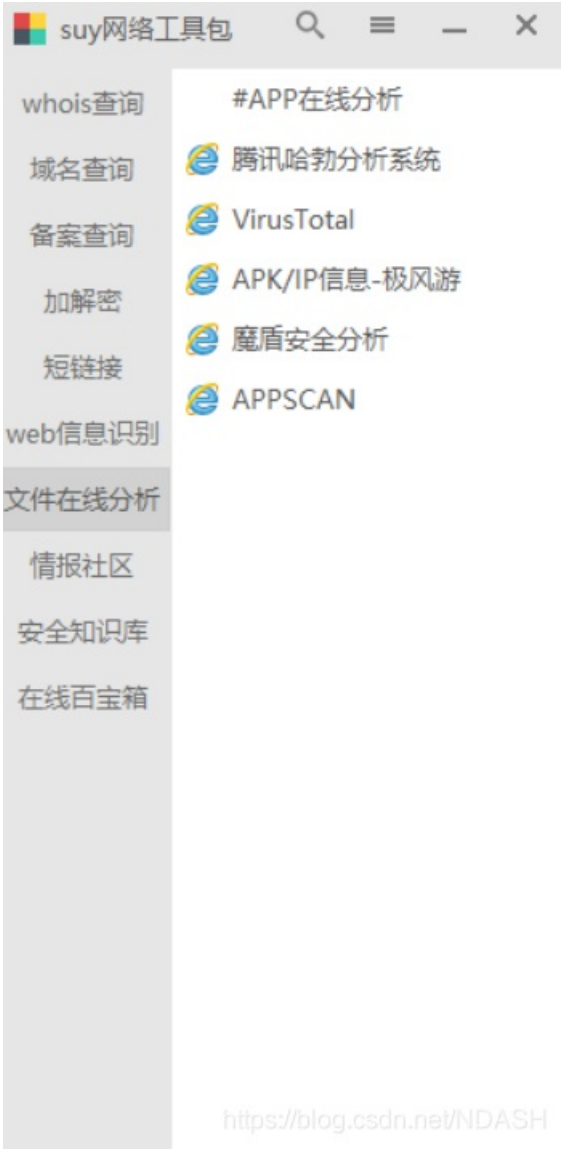
六、web信息识别

（一）端口扫描

（二）SSL证书查询

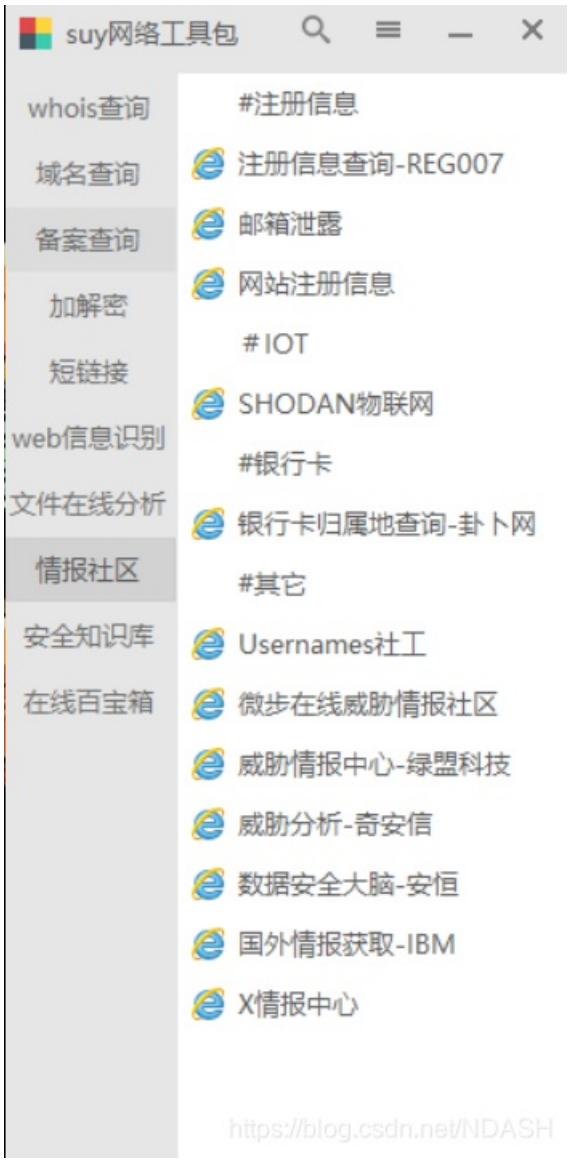
七、文件在线分析

可以简单在线分析一些文件、APP信息，不建议涉案的APP在上面分析，会有记录！



八、情报社区

信息收集能力


suy网络工具包
whois查询
域名查询
备案查询
加解密
短链接
web信息识别
文件在线分析
情报社区
安全知识库
在线百宝箱
#注册信息
注册信息查询-REG007
邮箱泄露
网站注册信息
#IOT
SHODAN物联网
#银行卡
银行卡归属地查询-卦卜网
#其它
Usernames社工
微步在线威胁情报社区
威胁情报中心-绿盟科技
威胁分析-奇安信
数据安全大脑-安恒
国外情报获取-IBM
X情报中心
https://blog.csdn.net/NDASH

九、安全知识库

（一）CTF资源

1、ctf和安全工具大合集

https://github.com/zardus/ctf-tools

2、近年ctf writeup大全

https://github.com/ctfs/write-ups-2016

https://github.com/ctfs/write-ups-2015

https://github.com/ctfs/write-ups-2014

3、fbctf竞赛平台Demo

https://github.com/facebook/fbctf

4、ctf Resources

https://github.com/ctfs/resources

（二）Python资源

1、python框架，库，资源大合集

https://github.com/vinta/awesome-python

https://github.com/jobbole/awesome-python-cn

2、python 正则表达式库（用于简化构造复杂的python正则表达式）

https://github.com/VerbalExpressions/PythonVerbalExpressions

3、python任务管理以及命令执行库

https://github.com/pyinvoke/invoke

4、python exe打包库

https://github.com/pyinstaller/pyinstaller

5、py3 爬虫框架

https://github.com/orf/cyborg

6、一个提供底层接口数据包编程和网络协议支持的python库

https://github.com/CoreSecurity/impacket

7、python requests 库

https://github.com/kennethreitz/requests

8、python 实用工具合集

https://github.com/mahmoud/boltons

9、python爬虫系统

https://github.com/binux/pyspider

10、ctf向 python工具包

https://github.com/P1kachu/v0lt

（三）其它

1.大礼包

https://github.com/bayandin/awesome-awesomeness

2.git学习资料

https://github.com/xirong/my-git

3.JS 正则表达式库（用于简化构造复杂的JS正则表达式）

https://github.com/VerbalExpressions/JSVerbalExpressions

4.一些信息安全标准及设备配置

https://github.com/luyg24/IT_security

参考文献

收集于网络，仅供研究学习！

【百度网盘链接：https://pan.baidu.com/s/1SFazHYQp6iyP4vME0bYvxg
提取码：7nki 】解压密码：NDASH
链接如失效请联系我补发或者到我的资源下载。

名称	时间
最后编辑日期：	2020 年 11 月 02 日