这是作者的系列网络安全自学教程，主要是关于网安工具和实践操作的在线笔记，特分享出来与博友共勉，希望您们喜欢，一起进步。上一篇文章分享了Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具；本篇文章将介绍社会工程学中的IP物理位置定位、IP获取、手机和邮箱查找、文件属性等。希望对初学者有帮助，大神请飘过，谢谢各位看官！

下载地址：https://github.com/eastmountyxz/NetworkSecuritySelf-study
百度网盘：https://pan.baidu.com/s/1dsunH8EmOB_tlHYXXguOeA 提取码：izeb

文章目录

前文学习：
[网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
[网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
[网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例
[网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密
[网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
[网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向破解
[网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨
[网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具

前文欣赏：
[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入
[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法
[渗透&攻防] 三.数据库之差异备份及Caidao利器
[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

参考文献：
《安全之路Web渗透技术及实战案例解析》陈小兵老师
《THE ART OF DECEPTION》 By：KEVIN D.MITNICK
https://baike.baidu.com/item/社会工程学/2136830

https://baike.baidu.com/item/网络钓鱼/1401858
https://www.csdn.net/gather_22/MtTaYgxsODUyOC1ibG9n.html
https://blog.csdn.net/gsls200808/article/details/23292149
https://study.163.com/course/courseLearn.htm?courseId=1004016002
记录朋友博客被入侵的日志分析溯源过程

一.社会工程学

> 声明：本人坚决反对利用社会工程学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。

1.什么是社会工程学?

世界第一黑客凯文·米特尼克在《欺骗的艺术》中曾提到，人为因素才是安全的软肋。很多企业、公司在信息安全上投入大量的资金，最终导致数据泄露的原因，往往却是发生在人本身。你们可能永远都想象不到，对于黑客们来说，通过一个用户名、一串数字、一串英文代码，社会工程师就可以通过这么几条的线索，通过社工攻击手段，加以筛选、整理，就能把你的所有个人情况信息、家庭状况、兴趣爱好、婚姻状况、你在网上留下的一切痕迹等个人信息全部掌握得一清二楚。虽然这个可能是最不起眼，而且还是最麻烦的方法。一种无需依托任何黑客软件，更注重研究人性弱点的黑客手法正在兴起，这就是社会工程学黑客技术。

社会工程学（Social Engineering） 是一种通过人际交流的方式获得信息的非技术渗透手段。不幸的是，这种手段非常有效，而且应用效率极高。事实上，社会工程学已是企业安全最大的威胁之一。狭义与广义社会工程学最明显的区别就是是否会与受害者产生交互行为。广义是有针对性的去对某一单一或多一目标进行攻击的行为。

社工三大法宝：网络钓鱼、电话钓鱼、伪装模拟
狭义三大法宝：谷歌、社工库、QQ
社工师的分类：黑客、渗透测试、间die、te工、gov、公司内部员工、诈骗人员、猎头、销售人员、普通人

举个例子：
某黑客知道了小H的手机号，通常QQ号和手机号是一样的，然后我们可以获取小H的QQ昵称，家乡，性别，年龄等一些基本信息。这仅仅是刚开始，然后通过小H的QQ获取空间个人一些相册，自己写的一些文章，自己对别人的评论，别人最自己的评论，留言板等信息，这些可以进行小H的心里分析，看小H是一个怎样的。接着通过看小H的手机号，获取小H 的微信号，进一步获取更多个人信息，再然后通过网站获取小H的所有注册过的网站，通过各个网站进一步获取信息。现在要进行深一步的了解了，利用小H生日组合或者名字进行暴力破解，破解小H注册的一个垃圾网站的号码密码，然后登陆其他的网站。通常防范意识不高的，很多账号密码都是一样，可以获取小H的学历，还有小H里面其他所有的好友，名字，还有和别人的聊天记录，现在开始有交集了，把小H其他人进行收集。最后把小H的所有信息收集，不停的对比和整理。最后基本了解小H的信息了，可以将小H的信息进行贩卖。

那么，信息是如何被泄露的呢？泄露的方式有很多，比如：

- 在网上注册时，垃圾网站被黑客攻入（服务器或者数据库被攻击），黑客获取信息。
- 网站内部人员将信息贩卖，然后获取信息。
- 通讯被窃听，http协议用post或者get提交时，使用火狐进行拦截。
- 撞库，比如你在这个A网站注册时，使用了一个密码，在B网站也使用这个密码，知道A网站的密码，自己也可以用这个密码登录B网站了，这个就是撞库。

为什么攻击者会选择利用社会工程学进行攻击行为？
因为它是最便捷的攻击方式。攻击者在搞定一个极其复杂的内网环境或者高度防御系统的时候，仅凭外网是很难找到突破口，外网的安全是相对安全的。但是，通过社工拿到一个泄露的账户和密码或者一个email来定位实施单一攻击（类似APT的水坑）。还有就说你是安全技术人员，招标公司的，运维，实在不行你就去问问路套路一下里面的员工和看门大爷，只要有机会接触到公司的内网，通过一些工具直接打穿内网，外网代理进内网，一首《凉凉》送给他们。在国内，由于社工造成的信息泄露事件不算多，多是直接sql注入脱库，可能是某些公司被攻击之后没有发现而已，也可能是法网恢恢。

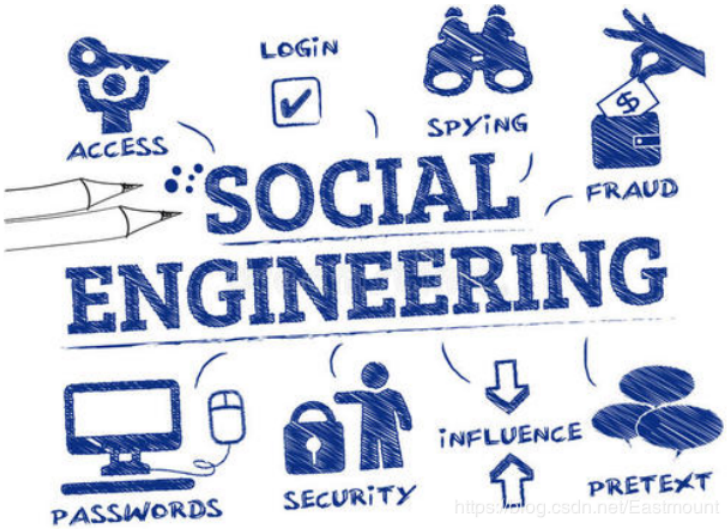
2.社会工程学分类

社会工程学攻击包括四个阶段：

- 研究：信息收集（WEB、媒体、垃圾桶、物理），确定并研究目标
- 钩子：与目标建立第一次交谈（HOOK、下套）
- 下手：与目标建立信任并获取信息
- 退场：不引起目标怀疑的离开攻击现场

通常社会工程学攻击可以划分为两类：

- 基于人的社工：搭载、伪造身份、偷听、窃肩、反社工、垃圾桶工程
- 基于计算机的社工：弹出窗口、内部网络攻击、钓鱼邮件、419尼日利亚骗局、短信诈骗



信息收集是社会工程的一个重要环节。信息收集同时也是一个最费时、最费事、最费力的阶段，但这往往是决定攻击周期内成败的关键要素，具体可以看一下《我是谁，没有绝对的安全》里面的关键环节。

常见信息包括：姓名、性别、出生日期、身份证号、身份证家庭住址、身份证所在公安局、快递收货地址、大致活动范围、qq、手机号、邮箱、银行卡号（银行开户行）、支付宝、贴吧、百度、微博、猎聘、58、同城、网盘、微信、常用ID、学历（小/初/高/大学/履历）、目标性格详细分析、常用密码、照片EXIF信息。

常见可获取信息系统包括：中航信系统、春秋航空系统、12306系统、三大运营商网站、全国人口基本信息资源库、全国机动车/驾驶人信息资源库、各大快递系统（越

权）、全国出入境人员资源库、全国在逃人员信息资源库、企业相关系统、全国安全重点单位信息资源库等。

3.常见方法

(1) 交流模型

在通信交流中，是一个发送器发送给另一个接收器，而交流则是从一个实体传送到另一个实体的过程，交流是一个双向的过程，这个过程发生着信息的交换、传播以及处理。沟通是我们把别人带到思维空间，分享个人的信息，所有的参与者都必须有一种彼此的心理位置概念，他们中间存在一个可沟通的渠道。

人的交流会传送两个层次的信息：语言和非语言，社工就是利用这些语言和非语言的潜在信息，改变目标的感知，从而得到想要的结果。交流的基本含义是发送一个信息包给既定的接受者（通俗解释：说话），信息中会包含多个信息源，用来描述这个“事件”
即：通信过程，有名的通信模型是——“Shannon-weaver模型”鼻祖模型。模型包含“信息源、信息、发送器、信号、信道、噪声、接收器、信息目的地、误差概率、编码、解码、信息率、信息容量”，此模型也被称为传递模型。

(2) 网络钓鱼

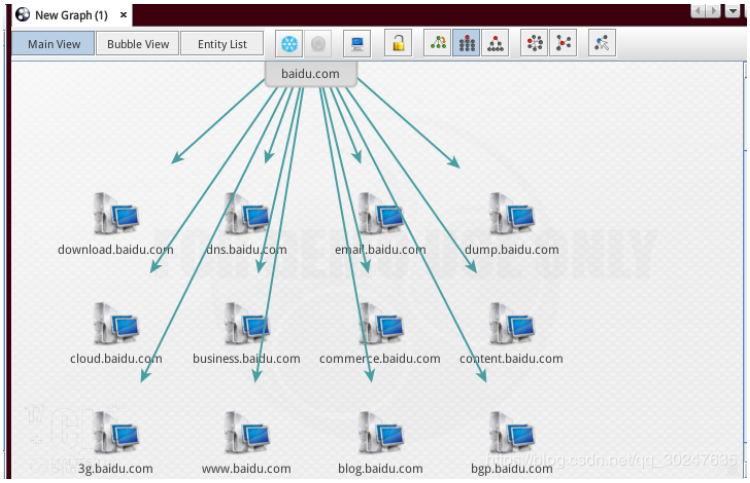
网络钓鱼（Phishing，与钓鱼的英语fishing发音相近，又名钓鱼法或钓鱼式攻击）是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID 、 ATM PIN 码或信用卡详细信息）的一种攻击方式。最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。它是“社会工程攻击”的一种形式。网络钓鱼是一种在线身份盗窃方式。

钓鱼阶段：信息收集-信息分析-钓鱼网络-下饵-上钩。
钓鱼攻击：采用钓鱼的方式向某个特定的目标系统发起攻击，并最终成功获取到被攻击目标中的信息。比如：Adobe reader的漏洞、Word的漏洞、flash漏洞、IE漏洞。

钓鱼可以借助邮件或者信息传播途径，将含有恶意程序的文档发送给目标服务器中，使之有意或无意的点击恶意程序从而控制目标主机。常见的钓鱼手段包括：鱼叉式网络钓鱼攻击、水坑式网络钓鱼攻击、钓鲸、APT等。

(3) Maltego

Maltego作为一款成功的信息收集工具其功能强大，它不仅可以自动收集到所需信息，而且可以将收集的信息可视化，用一种图像化的方式将结果呈现给我们。



(4) 信息刺探

在入侵前，通常都会对目标进行一次较为全面的检测，所谓不打没有把握的仗，入侵前的信息刺探很重要，通过对目标主机的检测，我们可以知道对方主机操作系统类型，开放了哪些网络服务，是否存在漏洞等信息。将搜集到的信息整理起来将会对后面的入侵工作起到事半功倍的效果。同样，社工也需要在入侵前进行踩点。

- 通过QQ号获取信息，包括用户真实姓名、昵称。通过QQ空间获取照片、行为特征、好友。
- 通过社交网络微博、微信、知乎、贴吧、虎扑等获取用户相关信息。
- 通过手机号找出QQ号，腾讯QQ提供了匹配通讯录的功能，这一功能本意是想让你添加通讯录里的好友，但由于手机号匹配之后还是会显示你的部分信息，我们可以通过这部分信息来查找。

一般来说，越是设置得非主流的越容易查找，越是设置得大众的越难查，首先我们可以复制昵称，注意现在手机上的QQ是直接提供复制功能给用户的，如果查到的结果很多，我们可以限制搜索条件，比如年龄、性别等。

二.IP地址获取

前一篇文章详细讲解了Web漏洞扫描工具，包括NMapp、ThreatScan和DirBuster，这里简单回顾下ThreatScan在线扫描工具。

https://scan.top15.cn

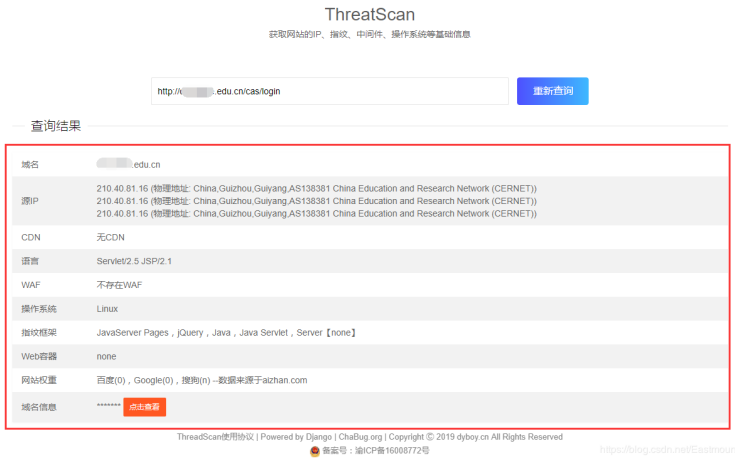
本文以某大学的信息系统为例，进行简单的测试，假设网址为：http://www.xxxxx.com

第一步：基础信息扫描

包括域名、IP地址、有无CDN、编程语言、是否存在WAF（Web应用防护系统）、操作

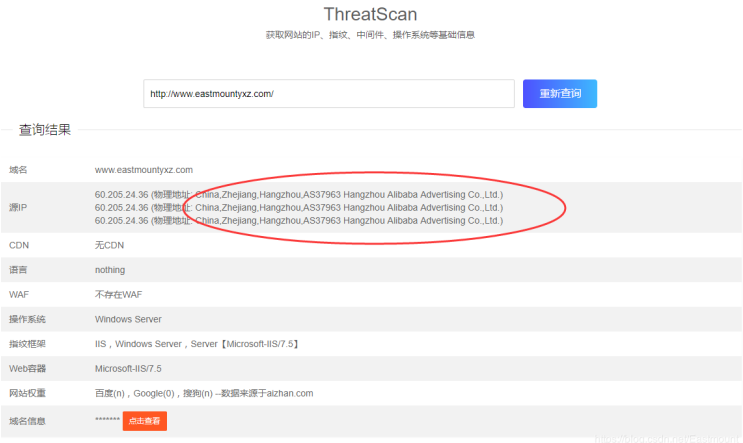
系统、指纹框架、Web容器、网络权重等。注意，ThreatScan通过Web指纹识别，发现该网站采用Java进行开发。

获取的真实IP地址为：210.40.81.16



再如，以作者在阿里云搭建的一个网站为例（http://www.eastmountyxz.com/），其运行结果如下图所示，Hangzhou Alibaba。

IP地址为：60.205.24.36



第二步：端口扫描

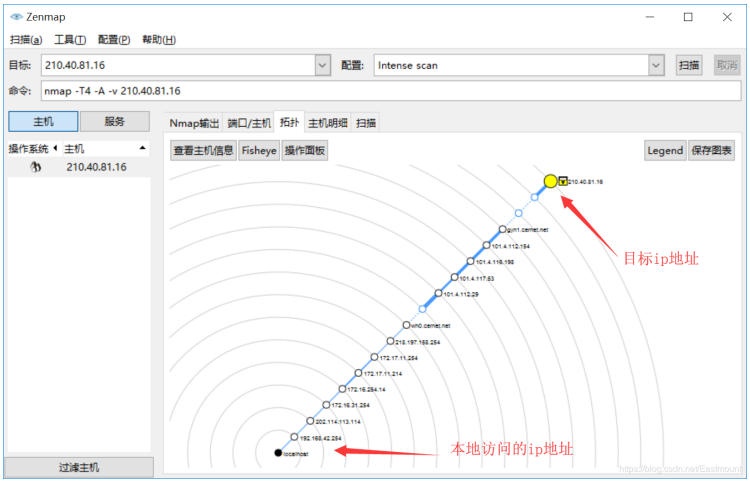
接着将IP地址填写到端口处，进行相关扫描。端口扫描是获取目标主机的端口信息显得十分有必要，通过一些常见端口，可以大致得出目标主机运行的服务，为后续渗透测试薄弱点提供参考。

第三步：旁站扫描

旁站扫描能扫描与该IP地址挂靠的其他网站，这有利于Web渗透，可能旁站存在漏洞。

第四步：信息泄露查询

Namp软件可以获取IP地址拓扑图，方便观察网络跳数，尤其是大的网段。

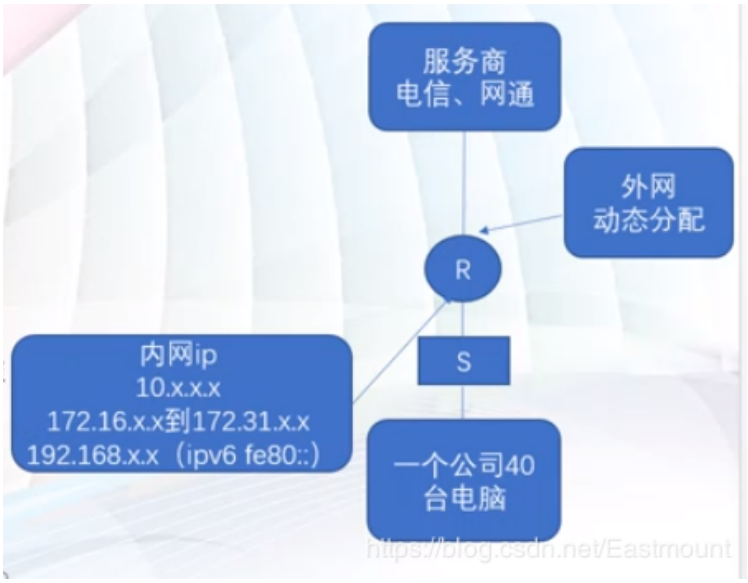


PS：QQ可以通过木子李获取IP地址。

三.IP物理定位

IP物理定位可以通过百度地图开发者服务（web 服务API）、第三方接口、在线网站等进行定位，但不同的接口其精确度也会不同。下图展示内网和外网、服务商之间的关系，服务商通常会按照区域划分ip地址，凡是通过网络接入到服务器，就一定能获取ip和地址定位，从而获取目标的物理位置。

为什么要进行IP物理定位呢?
假设某人发了某个危害的帖子或从事犯罪活动，有关部门就需要抓捕他。此时，首先要获取他的IP地址，通过服务器对比，观察这个时间点它把IP分配给谁（通常实名制）；再通过IP地址进行物理定位。后台日志通常会存储相关的IP地址及行为。现在，通过三大运营商数据、Wifi、基站、社交网络、视频等，都能进行一些更为智能精确的定位，从而维护整个社会的网络安全。



下面作者将介绍在线的IP物理定位的方法，还是以上面获取的IP地址为例。

某网站IP地址：210.40.81.16

作者博客IP地址：60.205.24.36

查询网址：

https://www.opengps.cn/Data/IP/ipplus.aspx

http://www.gpsspg.com/maps.htm

获取的地理位置如下图所示，其结果还是比较精确的。

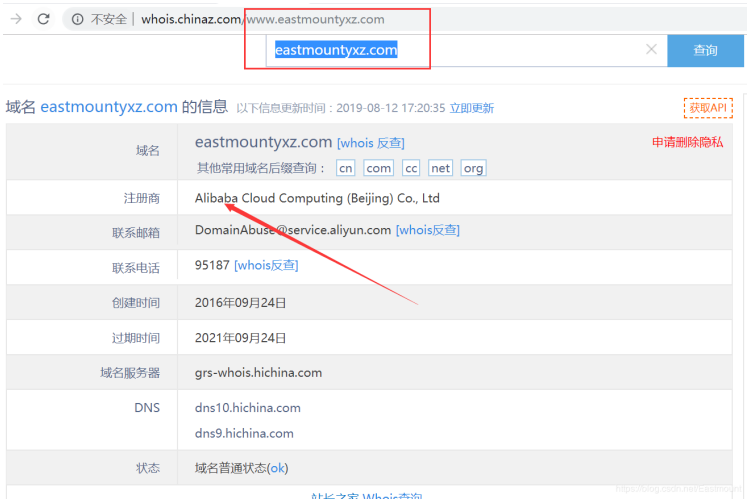
Whois

whois（读作“Who is”，非缩写）是用来查询域名的IP以及所有者等信息的传输协议。简单说，whois就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。通过whois来实现对域名信息的查询。早期的whois查

询多以命令列接口存在，但是现在出现了一些网页接口简化的线上查询工具，可以一次向不同的数据库查询。网页接口的查询工具仍然依赖whois协议向服务器发送查询请求，命令列接口的工具仍然被系统管理员广泛使用。whois通常使用TCP协议43端口。每个域名/IP的whois信息由对应的管理机构保存。

http://whois.chinaz.com/

比如作者的个人博客查询结果如下图所示：

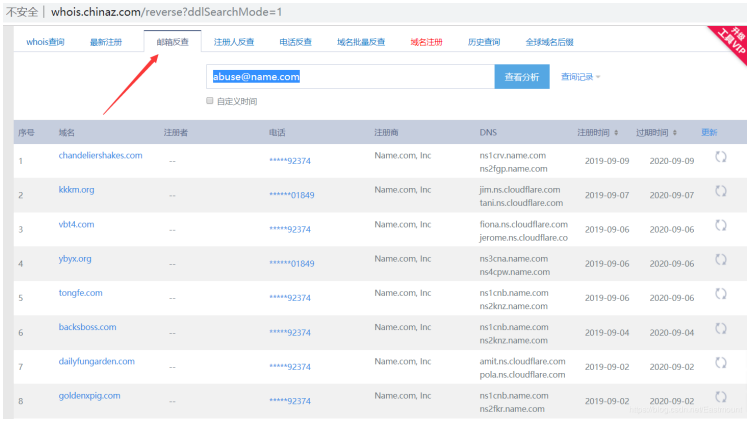


同样，百度地图API也是能创建地理位置获取以及热点区域识别，希望感兴趣的同学可以阅读我的文章。需要申请AK再实现相关应用。

http://lbsyun.baidu.com/apiconsole/key/create
[android] 百度地图开发 (一).申请AK显示地图及解决显示空白网格问题
[android] 百度地图开发 (二).定位城市位置和城市POI搜索
Android百度地图之位置定位和附近查找代码简单实现 (上)
C#调用百度地图API入门&解决BMap未定义问题

再比如阮一峰老师的博客，是不是通过社会工程学发现了些知识。
http://www.ruanyifeng.com/home.html

通过邮件反查，能看到很多知识，如下图所示。



四.手机查找

通过各大网站已知有价值的ID获取其他信息（如电话号码、QQ、微信），通过电话或QQ获取用户的登录账号，是常见的社会工程学手段。常用的步骤如下：

第一步：通过已知信息查找有价值的ID或其他信息，推荐网站 www.reg007.com、www.zhaohuini.com

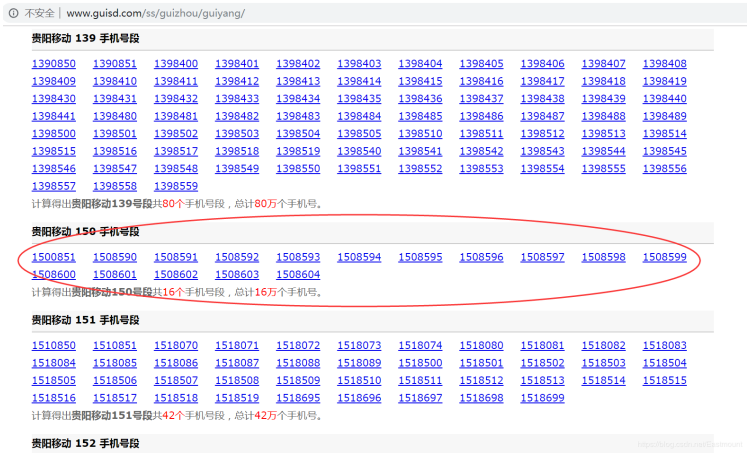
下图是在REG007网站通过QQ邮箱获取他注册过的网站，当然结果不一定准备，并且需要注册。

第二步：用密码找回功能获取部分手机号信息

如下图所示，部分网站可能会手机的部分信息透露，比如开头182、结尾47。

第三步：找出所在城市获得手机号段

通过某些网站获取三大运营商不同城市的手机号段，比如贵阳市：
http://www.guisd.com/ss/

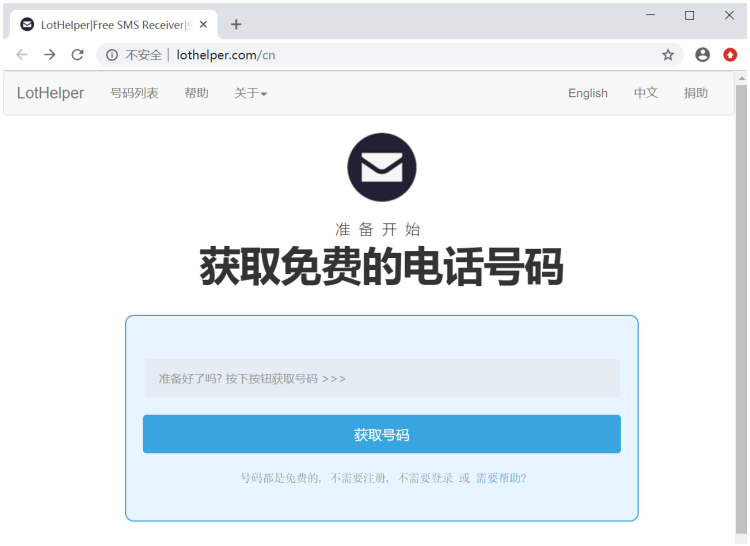


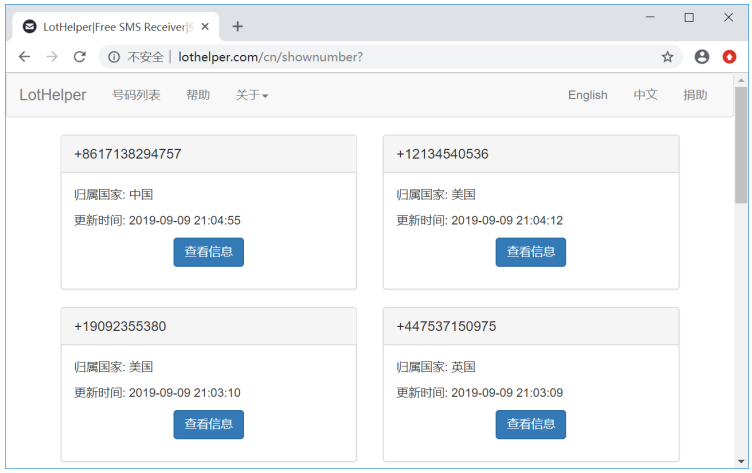
第四步：用手机号码生成器或Python循环遍历生成手机号并导入手机

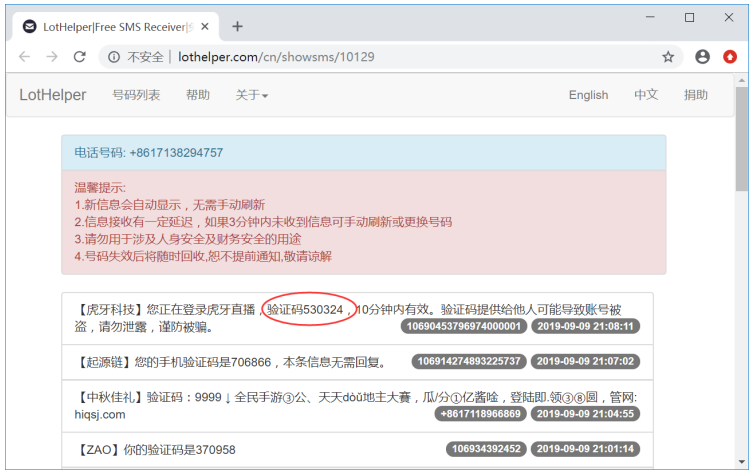
第五步：利用手机号码和物理位置来套路信息，利用手机号继续查找信息

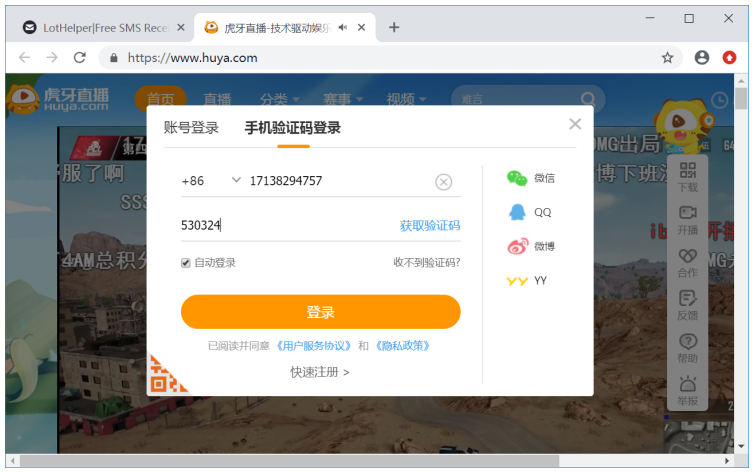
总之，需要不断通过已知信息获取未知信息，获取的信息越多越好、越丰富越好。

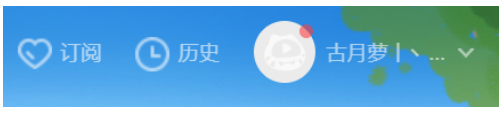
接着补充一个神奇网站（http://lothelper.com/cn），如下图所示，你看看它能做什么。




LotHelper|Free SMS Receiver
不安全 | lothelper.com/cn/shownumber?
LotHelper
号码列表
帮助
关于
English
中文
捐助
+8617138294757
归属国家: 中国
更新时间: 2019-09-09 21:04:55
查看信息
+12134540536
归属国家: 美国
更新时间: 2019-09-09 21:04:12
查看信息
+19092355380
归属国家: 美国
更新时间: 2019-09-09 21:03:10
查看信息
+447537150975
归属国家: 英国
更新时间: 2019-09-09 21:03:09
查看信息

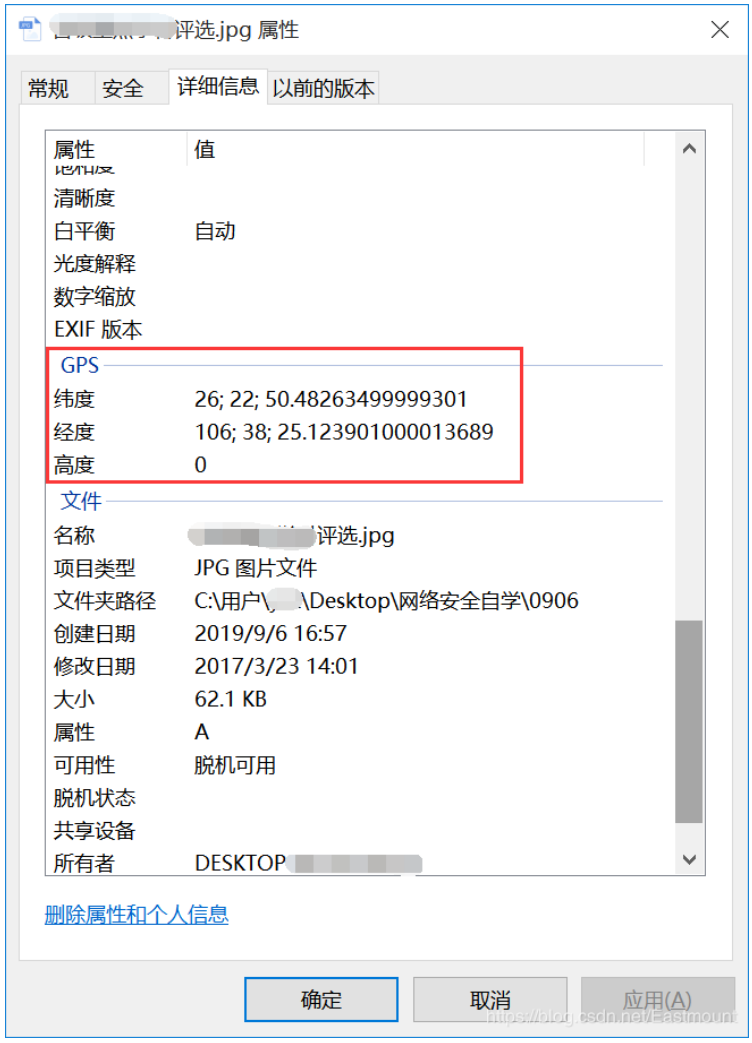

LotHelper|Free SMS Receiver
不安全 | lothelper.com/cn/showsms/10129
LotHelper
号码列表
帮助
关于
English
中文
捐助
电话号码: +8617138294757
温馨提示:
1.新信息会自动显示，无需手动刷新
2.信息接收有一定延迟，如果3分钟内未收到信息可手动刷新或更换号码
3.请勿用于涉及人身安全及财务安全的用途
4.号码失效后将随时回收,恕不提前通知,敬请谅解
【虎牙科技】您正在登录虎牙直播，验证码530324，10分钟内有效。验证码提供给他人可能导致账号被盗，请勿泄露，谨防被骗。
10690453796974000001
2019-09-09 21:08:11
【起源链】您的手机验证码是706866，本条信息无需回复。
106914274893225737
2019-09-09 21:07:02
【中秋佳礼】验证码：9999↓全民手游③公、天天dòu地主大赛，瓜分①亿酱唑，登陆即.领③⑧圆，管网: hiqsj.com
+8617118966869
2019-09-09 21:04:55
【ZAO】你的验证码是370958
106934392452
2019-09-09 21:01:14


LotHelper|Free SMS Rece
虎牙直播-技术驱动娱乐
https://www.huya.com
虎牙直播
huya.com
首页
直播
分类
赛事
视频
账号登录
手机验证码登录
+86
17138294757
530324
获取验证码
自动登录
收不到验证码?
登录
已阅读并同意《用户服务协议》和《隐私政策》
快速注册 >
微信
QQ
微博
YY
下载
开播
合作
反馈
帮助
举报


订阅
历史
古月萝卜

五.其他技巧

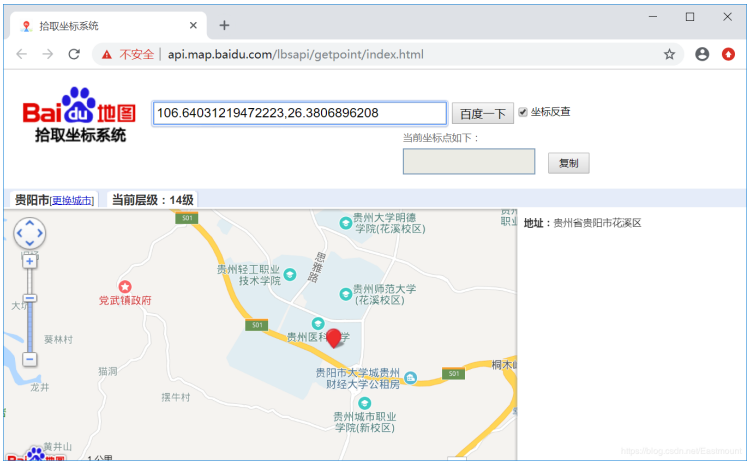
也许有些人经历过，在微信群里晒了一张并没有定位的自拍，却被不在现场的朋友们发现了你的位置，这就是照片原图泄露了你的位置，如下图所示。



其原因是智能手机在拍照的时候，都有一个叫Exif的东西。它包括快门、光圈、iso、白平衡、日期时间等各种图像数据，还有一个重要的信息——位置信息。如果不经过处理，这些Exif参数会一直存在。在拍照的时候软件调用了Exif中的GPS全球定位系统数据。同时，经过各种美图软件处理过的照片都会在相册中显示位置信息，而且不少美颜软件都自带定位功能，打开相机找到“保存地理位置”选项，并选择不打勾。

接着我们将经纬度进行解析，它是以度分秒的格式展示的（度分秒之间以“；”间隔），为了方便定位，我们需要将度分秒转换为度的格式。
纬度为：26；22；50.48263499999301，其计算方法为：26+(22+50.48263499999301/60)/60 = 26.3806896208
经度为：106；38；25.123901000013689，其计算方法为：106+(38+25.123901000013689/60)/60 = 106.64031219472223

接着进行位置定位，如下图所示。



同样，其他文件都会暴露一些信息，包括PPT、Word等，要学会保护自己的隐私及版权。社会工程学的本质是欺骗，不要轻易相信他人，不要到处留下自己的个人信息，要学会设置代理、短信验证、日志记录。

最后希望基础性文章对您有所帮助，作者也是这个领域的菜鸟一枚，希望与您共同进步。同时，明天是教师节，感谢自己所有老师的教育与栽培，也祝自己节日快乐，哈哈！第四个教师节。

(By:Eastmount 2019-09-09 晚上10点 http://blog.csdn.net/eastmount/)