信息收集中的搜索引擎 Hacking

搜索引擎

搜索引擎是一个爬虫机器人，不停的在爬世界所有网站，有可能在爬的过程中，就把你重要的文档给爬出来了，尽管你没有对外公布该文档。

所以在做渗透测试的时候，就可以通过搜索引擎对测试目标做一个搜索。现在，对测试目标做一个搜索引擎hacking的行为，已经成为了一门科学。

谷歌有谷歌hacking 百度有百度hacking 必应有必应hacking 都是专门做搜索用的。有时候一个搜索引擎，就能给出对方的CMS或者其他软件结构。比如已开源漏洞，就能用搜索引擎直接拿下目标控制权。

作为渗透测试者要用的，就是利用搜索引擎获取目标信息，必要时应该学会利用各个搜索引擎的语法。

搜索引擎能搜到什么

1. 公司新闻动态
2. 重要员工信息
3. 机密文档
4. 用户名密码、邮箱
5. 目标系统软硬件技术架构。

以上都是能用搜索引擎搜索到的，尽管你并没有公开一些文档，但是只要放在互联网上就可能会被爬到。

接下来，介绍第一个。

shodan

shodan和我们国内的钟馗之眼是一种搜索引擎，他们区别于百度等引擎，他们只爬设备，只爬联网设备。

网址为：

https://www.shodan.io/

Shodan，也有人把他叫撒旦，是和百度谷歌不一样的，谷歌百度爬的网页信息，而shodan爬的是互联网设备，也包括端口。

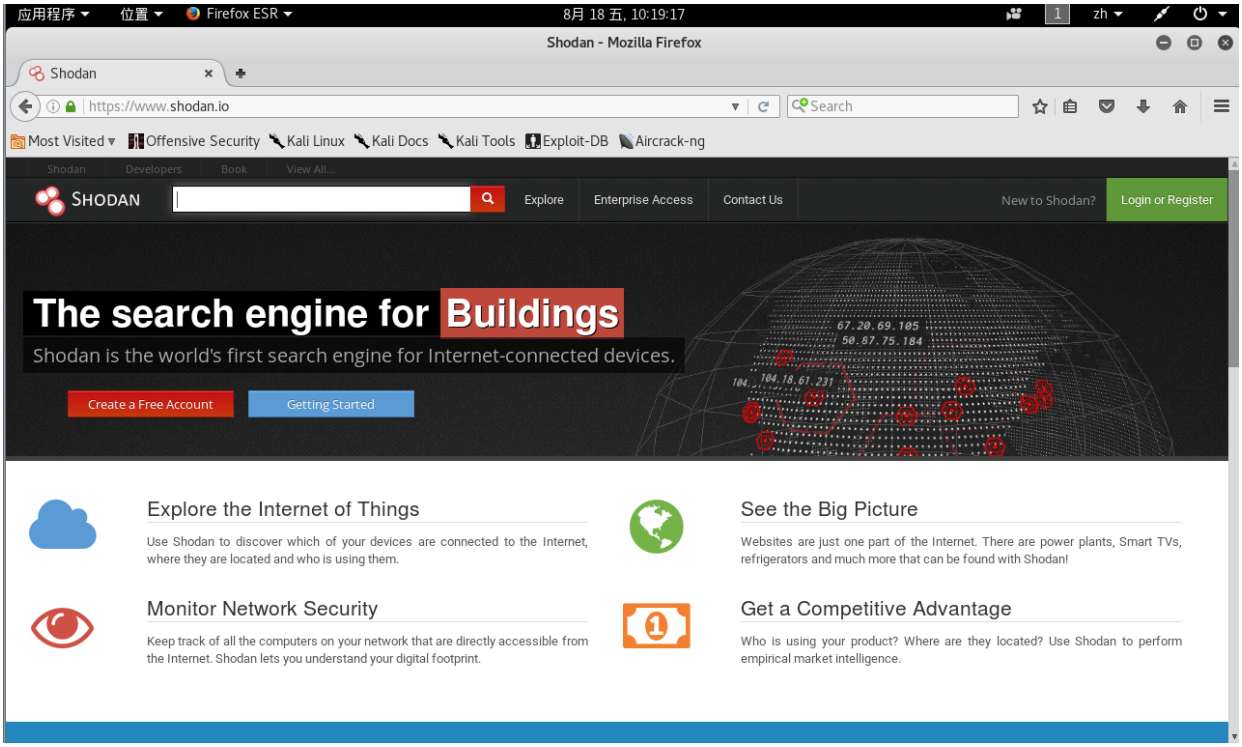
智能家电越来越多，能连上互联网就可能被shodan这种引擎爬到。

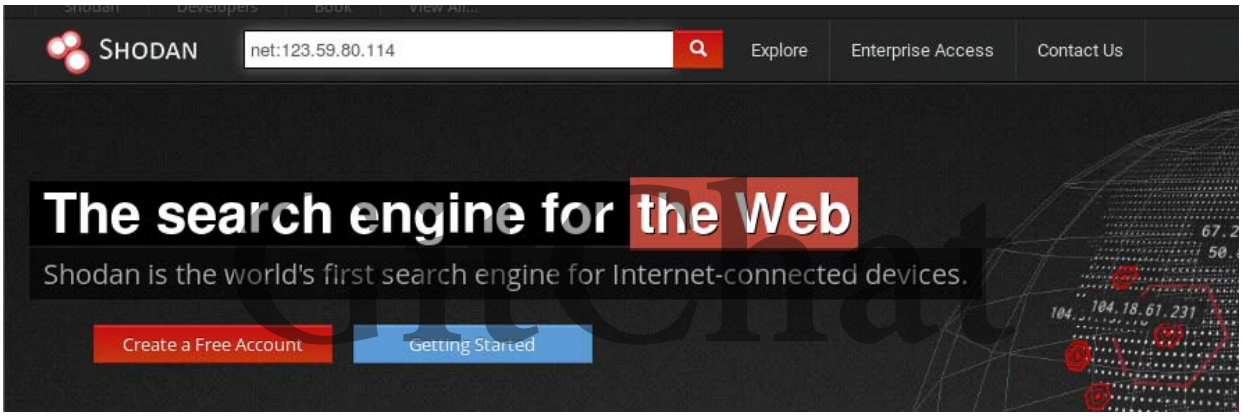
Shodan的语法

- Net
- Cify
- Country
- Post
- Os
- Hostname
- Server

如何利用shodan去搜索

直接在shodan搜索框里输入指定的目标，可以是IP地址或者域名。



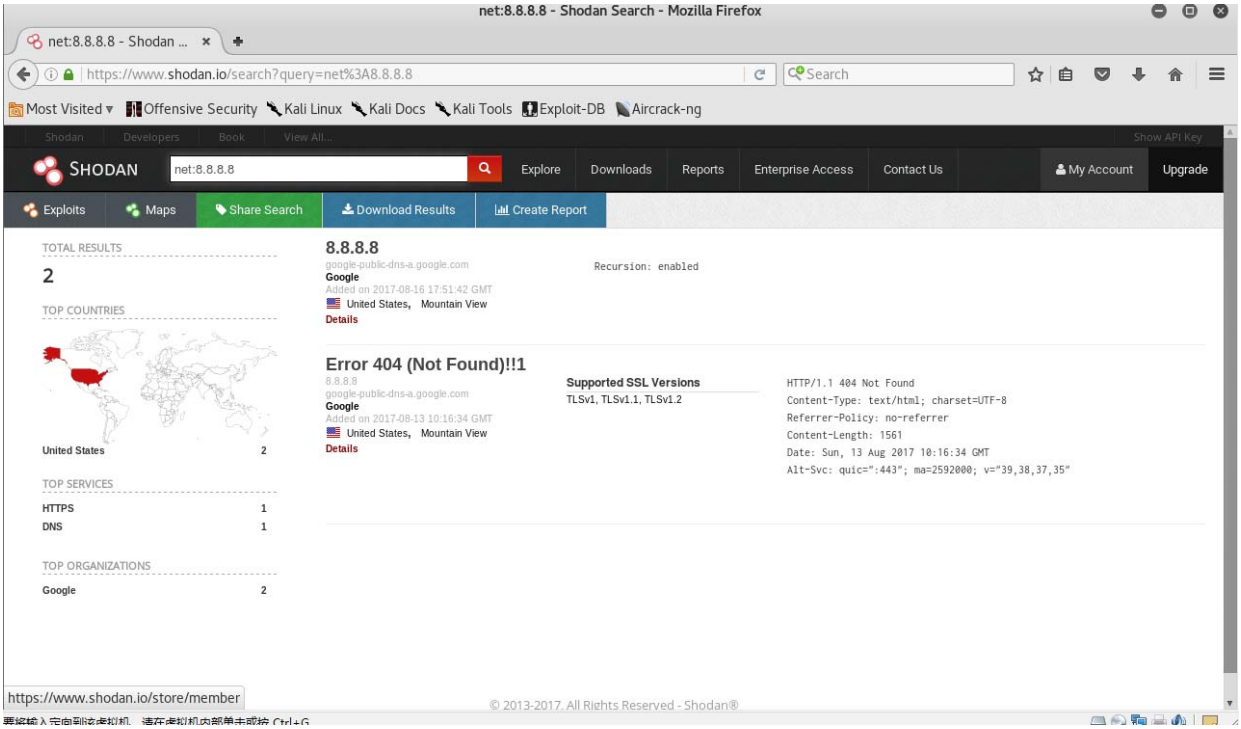


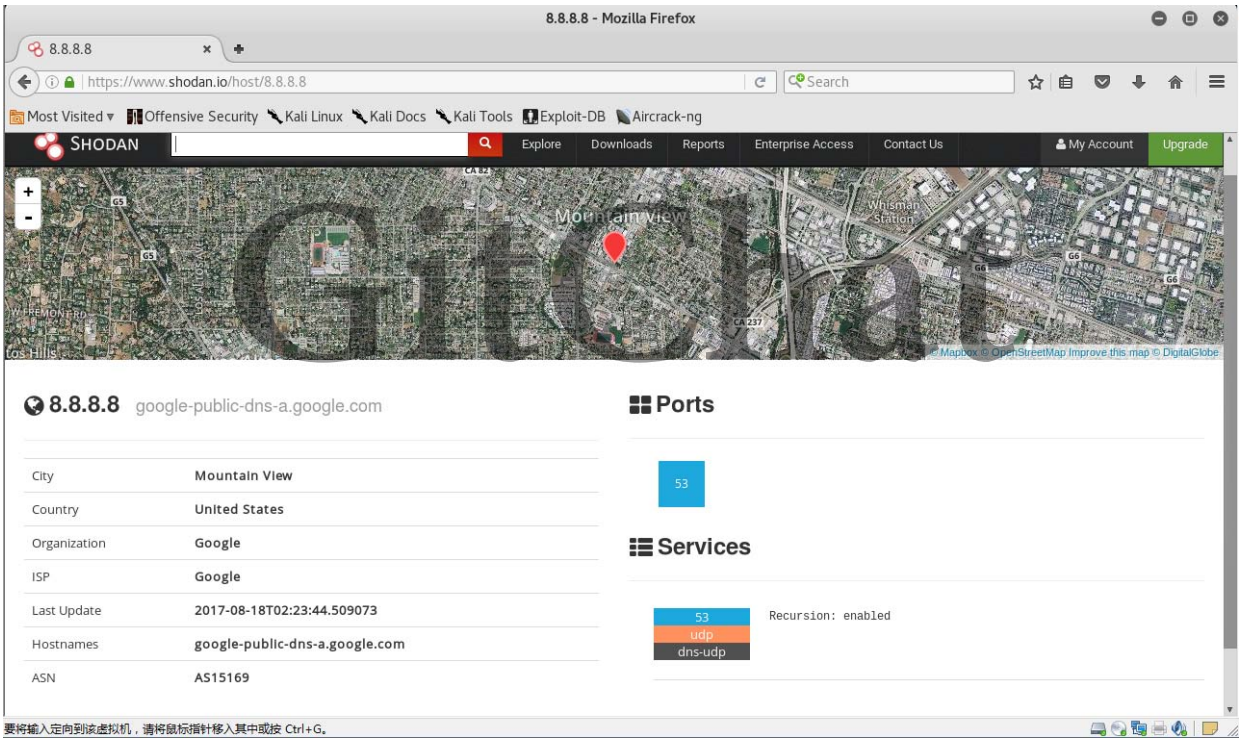
比如gitchat.cn的域名，通过解析得出IP为：123.59.80.114

Shodan搜索IP的语法就是 net：123.59.80.114

但为了更好的演示效果，我搜索的是8.8.8.8

搜索结果如下图：





通过shodan得出，这个IP位于美国。网页状态码是404。

如果看详细信息，请点击他的IP。

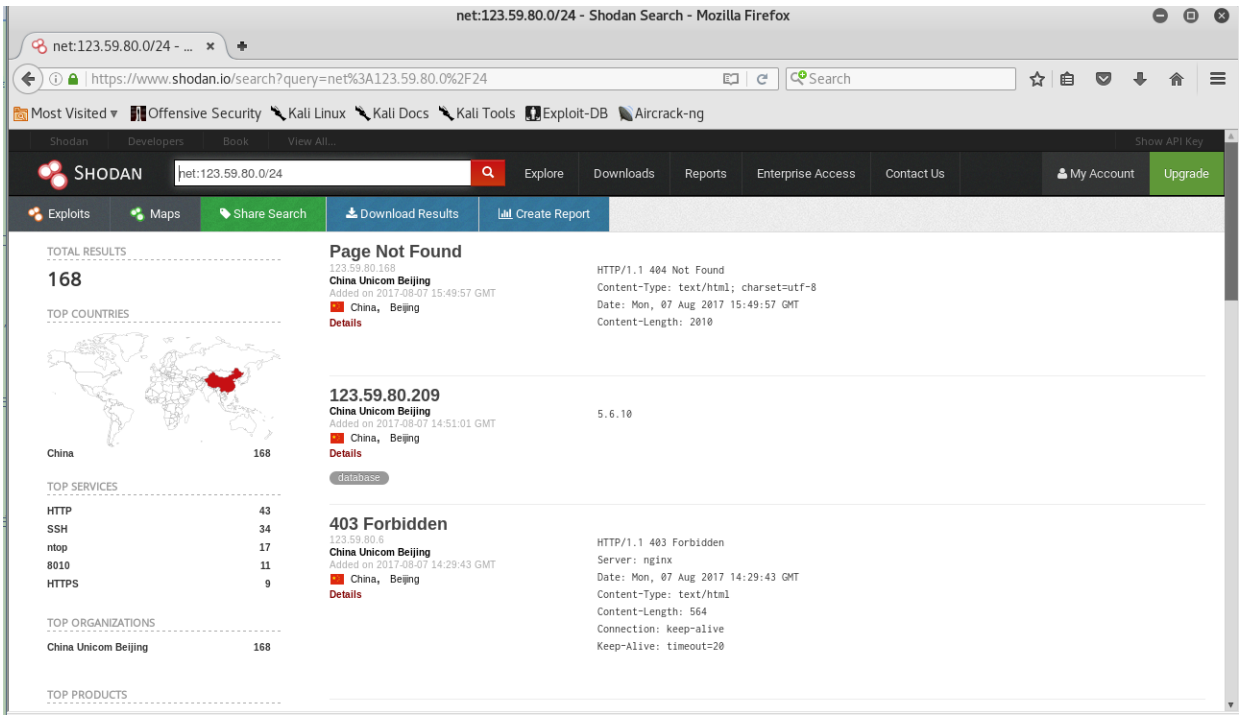
可以看出他是属于谷歌，ports,也就是开放了多少端口，这里显示53.也就是开放了53端口。

上面可以看实际的物理地址，但我并不认识美国路标，就不做介绍了。

这是shodan的基础利用，但如果我想查8.8.8.8所在的C位。

语法就应该变为：net:8.8.8.0/24

gitchat的IP为;123.59.80.114,但并没有搜到其他的主机，所以我搜索的是 net：123.59.80.0/24 搜索这一个C段。结果如下：



给出了很多信息，http状态码，网站程序语言等等。

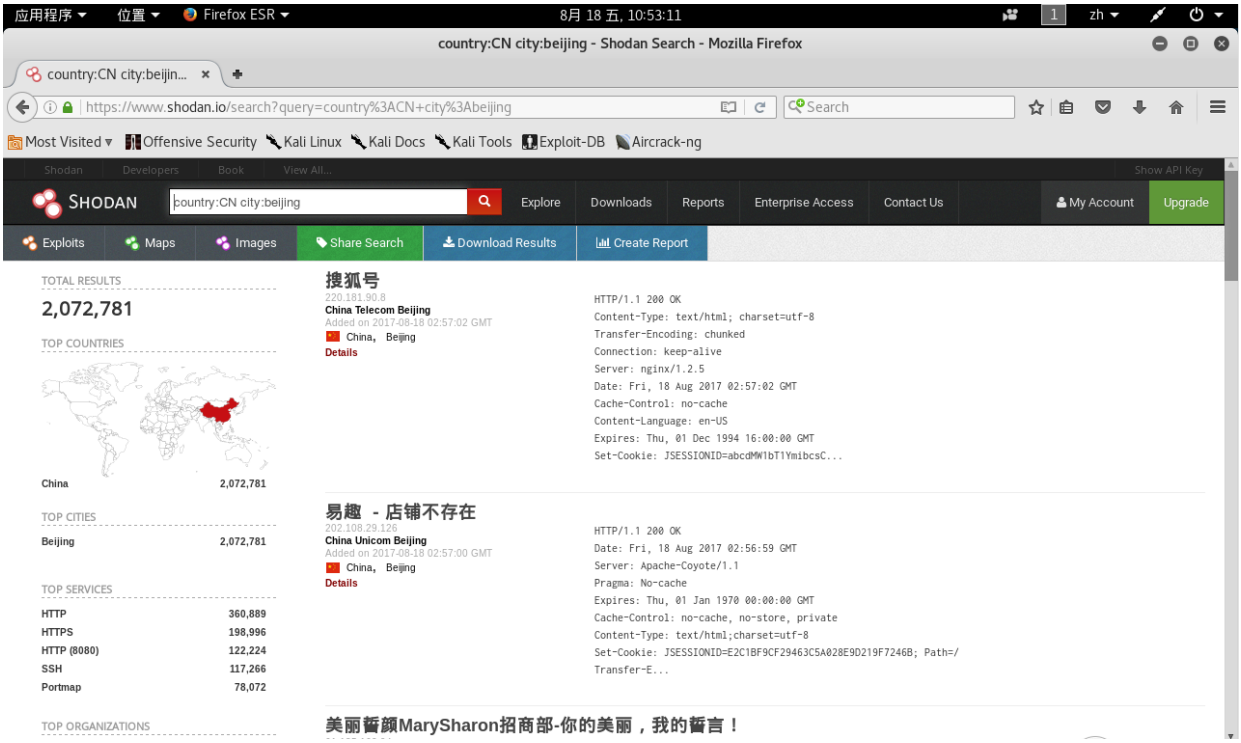
但是信息太杂乱了，我希望将信息过滤。

Shodan：country参数

如何将信息过滤，正确的做法应该是在原有的参数上加上：country:CN 美国就是US 标准语句为：net:8.8.8.0/24 country:CN

Country：CN 就是全中国。

Country：CN city:beijing 就是中国北京的IP地址。



从上图可以看出，shodan爬到的所有中国北京的IP地址

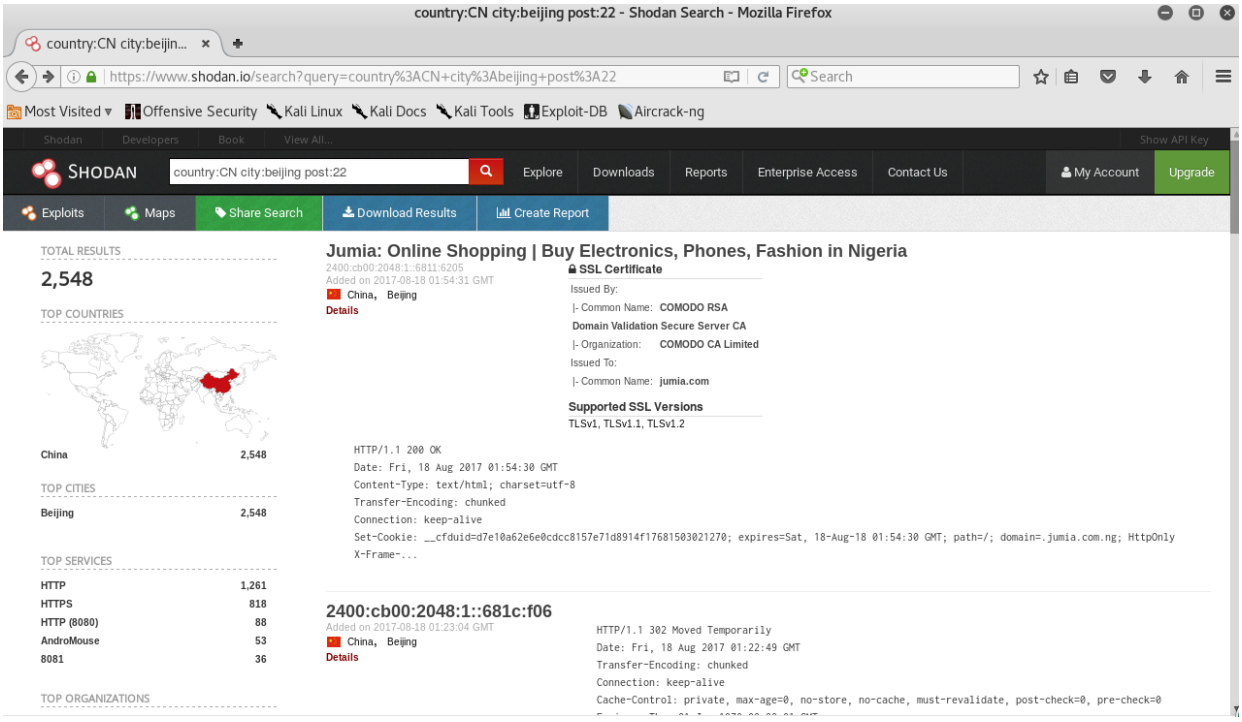
Shodan：Post参数

上面我们是搜索的中国北京的IP地址，那么post：22的功能就是筛选所有中国北京开放了22端口的地址。

正确的语法是：Country：CN city:beijing post:22

22是端口号，根据实际的不同可以改为80等等。

搜索结果如下图所示：



这就是开放了所有22端口的服务器。

Shodan：os参数

os的操作系统的意思，比如我想搜索北京所有windows2008的系统。

Country：CN city:beijing os:”windows 2008”

这里就不做截图了，和上面的是一个概念。

Shodan：hostname参数

Hostname的功能是爬出所有基于目标的网站。

比如：hostname:baidu.com

这里也不做截图了，通过上面的阅读应该能使用shodan引擎了。

Shodan：Server参数

Server:appche/2.2.3

这个语句是意思是搜索所有是appche2.2.3版本的服务器。

Shodan的常用语法就结束了，如果要更多的，请查阅shodan参数手册。

Google引擎

谷歌基础搜索不作说明，只解释Googlehacking.

加减字符的使用

比如我想搜索支付，出来了很多页面但不想出现充值关键词，就要利用如下

+支付 -充值

这个语句就是过滤掉所有包含支付单不包含充值的页面

Intitle参数

这个语句的作用是搜索带有该关键词的标题的所有页面

Intext参数

这个语句的作用是搜索带有所有该关键词的内容页面。

inURL参数

这个语句的作用是搜索包含关键词的URL内容。

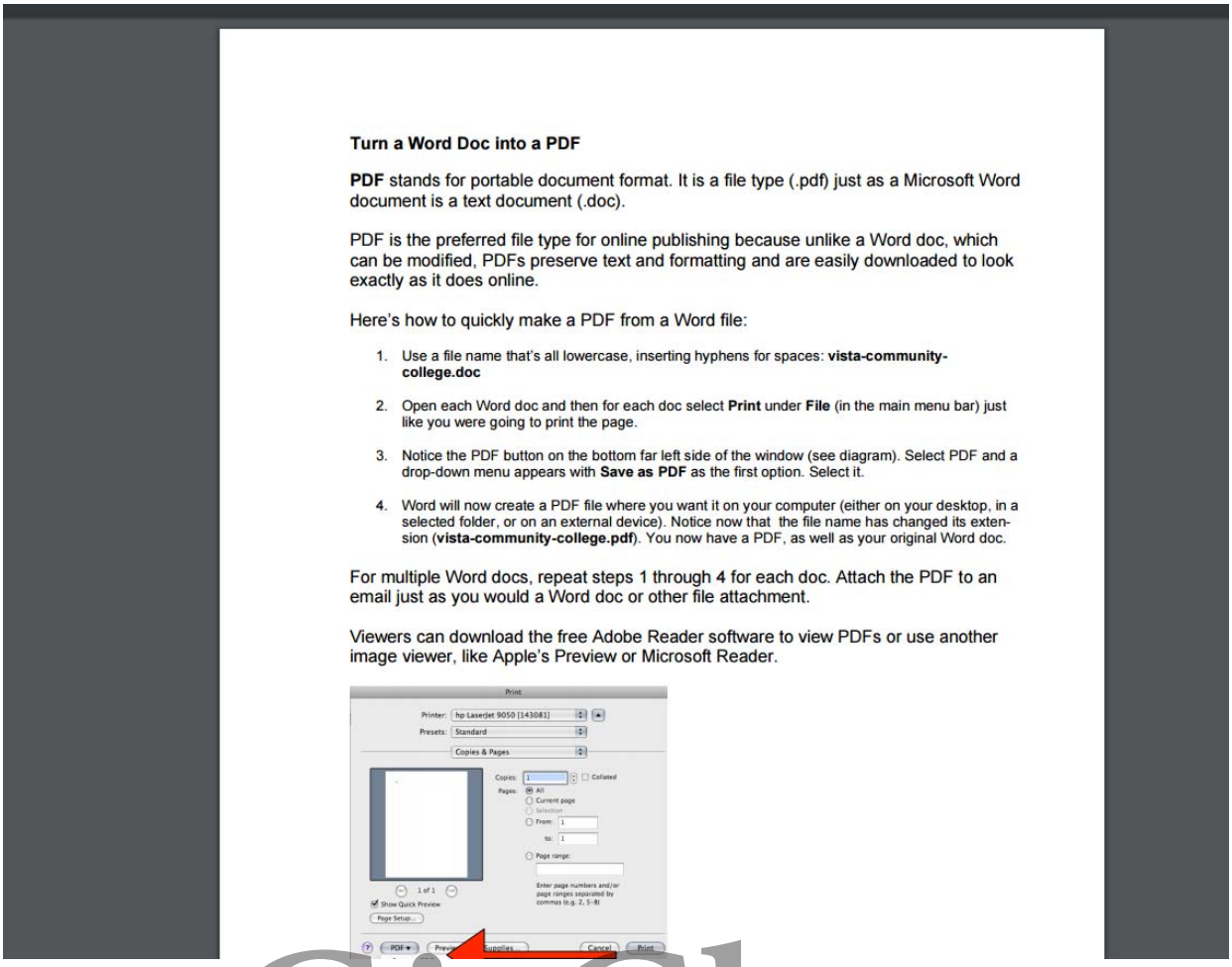
结合使用的实例就是 北京 site:alibaba.com inurl:contact

这这个语句的意思是，搜索在阿里巴巴的所有在北京 URL中包括contact的页面。

文件搜索参数

语句为：filefype:PDF(doc等)

比如，baidu filefype:PDF



Turn a Word Doc into a PDF

PDF stands for portable document format. It is a file type (.pdf) just as a Microsoft Word document is a text document (.doc).

PDF is the preferred file type for online publishing because unlike a Word doc, which can be modified, PDFs preserve text and formatting and are easily downloaded to look exactly as it does online.

Here's how to quickly make a PDF from a Word file:

1. Use a file name that's all lowercase, inserting hyphens for spaces: **vista-community-college.doc**
2. Open each Word doc and then for each doc select **Print** under **File** (in the main menu bar) just like you were going to print the page.
3. Notice the PDF button on the bottom far left side of the window (see diagram). Select PDF and a drop-down menu appears with **Save as PDF** as the first option. Select it.
4. Word will now create a PDF file where you want it on your computer (either on your desktop, in a selected folder, or on an external device). Notice now that the file name has changed its extension (**vista-community-college.pdf**). You now have a PDF, as well as your original Word doc.

For multiple Word docs, repeat steps 1 through 4 for each doc. Attach the PDF to an email just as you would a Word doc or other file attachment.

Viewers can download the free Adobe Reader software to view PDFs or use another image viewer, like Apple's Preview or Microsoft Reader.

-

这是谷歌搜到的一个PDF文档，但并不是百度页面的。

具体内容需要自己设置关键词，进行组合。参考方法和shodan搜索一样。

谷歌语法使用：

http://exploit-db.com/google-dorks

详细文档，值得阅读。

其余搜索引擎

国内：百度

国外：Google 必应

国内空间搜索设备：钟馗之眼

http://www.zoomeye.org/

国外空间搜索设备：shodan

https://www.shodan.io/

毛子的搜索引擎，号称世界第四大:

https://www.yandex.com/

总结，搜索引擎行为多种，万变不离其宗。关键时刻还是得靠人为肉眼检索，还没人工智能到那个地步。