Shodan

一，基础类
1.1 根据IP进行搜索：118.184.170.37
1.2 根据域名进行搜索：sogo.com
1.3 根据名称进行搜索：思科

1.2 根据服务/协议搜索

telnet
telnet default password
搜索telnet服务，含有password字段的关键词

telnet default password “NTT PC Communications”
搜索telnet服务，含有password字段的关键词，并且是NTT PC Communications公司内的

http
http product:"Aache httpd"
搜索http开启阿帕奇服务的网站/内容

http product:"Aache httpd" country:"CN"
仅搜索中国http开启阿帕奇服务的网站/内容

http product:"Aache httpd" country:"CN" os "Linux"
仅搜索中国Linux系统，且http开启阿帕奇服务的网站/内容

ssh
ssh product:"Aache httpd"
搜索shh开启阿帕奇服务的网站/内容

http product:"Aache httpd" country:"CN"
仅搜索中国ssh开启阿帕奇服务的网站/内容

ssh product:"Aache httpd" country:"CN" os "Linux"
仅搜索中国Linux系统，且ssh开启阿帕奇服务的网站/内容

1.3 关键词搜索
default password
“default password” country:"TH"
搜索泰国可能使用默认密码登入的设备

“default password”
搜索含有password内容关键字

cisco
200 OK cisco
搜索相关cisco相关设备 且开启http web服务

200 OK cisco country:"CN"
搜索中国相关cisco相关设备 且开启http web服务

FTP
FTP anon successful
搜索开启匿名服务且登入服务的FTP服务器

FTP anon
搜索可登入服务的FTP服务器

二，过滤词
1.1 country 根据国家搜索
country: 国家
仅搜索位于 - - 的网站
country:CN
仅搜索位于中国的网站

country:TH
仅搜索位于泰国的网站

country:JP
仅搜索位于日本的网站

counrty:US
仅搜索位于美国的网站

1.2 product 搜索指定的服务
product:"nginx"
仅搜索使用nginx服务的所有网站

product:"Microsoft IIS"
仅搜索使用Microsoft IIS服务的所有网站

product:"Mysql"
仅搜索使用Mysql服务的所有网站

1.3 version 搜索指定的版本
product:MySQL version:"5.1.2"
搜索5.1.2版本的MySQL

product:Microsoft IIS version:"7.5"
搜索1.7版本的Microsoft IIS

1.4 hostname 搜索特定的域名
hostname:cn
仅搜索cn域名的网站

hostname:gov
仅搜索gov域名的网站

hostname:com
仅搜索com域名的网站

hostname:org.cn
仅搜索org.cn域名的网站

hostname:sogo.com
仅搜索sogo.com域名旗下的二级或含有sogo的网站

1.5 os 搜索特定的操作系统
os: "Windows 7"
搜索Windows 7 系统服务的网站

os:"Linux"
搜索Linux操作系统的网站

os:"Windows server 2012"
搜索Windows server 2012系统的网站

1.6 net 搜索特定网段地址
net:36.110.73.48/24
搜索36.110.73.48/24该地址下所有网段

1.7 port 搜索特定端口
port:8080
搜索仅开放8080端口的网站

port:445
搜索仅开放445端口的网站

port:25
搜索仅开放25端口的网站

port:3389
搜索仅开放3389端口的网站