Censys搜索语法

本课程仅用于教学用途

中华人民共和国网络安全法

中华人民共和国刑法

社会主义核心价值观

详情百度搜索以上“关键词”+site:gov.cn

参考资料

1~censys博客
https://censys.io/blog

2~censys团队
https://censys.io/company

3~zmap，ZGrab与Censys
https://zmap.io/
https://github.com/zmap

4~Censys架构论文
https://censys.io/static/censys.pdf

5~深入认识Censys
https://censys.io/integrations
https://censys.io/censys-resources/whitepapers
https://censys.io/censys-resources/publications-and-research

第一部分

1~https://censys.io/ipv4，IPv4查询

2~china， 关键词搜索，不区分大小写

3~"not found" 精确搜索

3~80.http.get.status_code: 200 端口80，http协议，响应码

4~80.http.get.title:beijing 标题包含

5~80.http.get.status_line:"302 Found" 双引号，精准化

6~80.http.get.body:china 返回吧里包含china

7~80.http.get.headers.server:apache 服务器是apache的

第二部分

1~ip:206.188.252.173　单一IP

2~ip:23.20.1.0/24　C段

3~ ip:[23.20.1.0 TO 23.20.1.100]　IP范围，{}，[]

4~ports:3389　端口

5~protocols: "22/ssh"　一定添加双引号，protocols:"443/https"

6~protocols:"443/https" protocols:"22/ssh"　开22或443

7~protocols:"443/https" not protocols:"22/ssh"　逻辑运算符and，or，not

第三部分

1~ a:www.google.com　A记录

2~"not foun?"　?表示1个字符，通配符

3~"not foun*"　*表示多个字符，通配符

4~80.http.get.body:/(302|404).*found/

5~80.http.get.title:/beijing.*\(.*\)/

6~80.http.get.status_code: 200^2 or "not found"　前者优先级更高

+ - = & || > < ! ( ) { } [ ] ^ " ~ * ? : \ /　表达原意都要转义

https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#regexp-syntax

第四部分

1~autonomous_system.asn:14618　自治系统号

2~autonomous_system.country_code:CN　国家代码
location.registered_country_code

3~autonomous_system.description:alibaba　自治系统描述包含alibaba
autonomous_system.name:alibaba

5~location.continent:Asia　大洲

6~location.country:China　国家
location.registered_country

7~location.province:guangdong　省份

8~location.city:beijing　城市

第五部分

1~location.postal_code:100001　邮编

2~location.timezone:"America/Mexico_City"　时区，一定要加引号

3~tags:ssh　标签协议是ssh的

4~metadata.os:linux　系统类型

5~可查端口指纹
102,110,11211,143,1433,1521,161,16992,16993,1883,1900,1911,20000,21,22,23,2323,25,27017,3306,3389,443,445,465,47808,502,53,5432,5632,5672,587,5900,5901,5902,5903,623,631,6379,6443,7547,80,8080,8883,8888,9090,9200,993,995

第六部分

搜索样例

1~23.0.0.0/8 or 8.8.8.0/24

2~location.country_code: DE and protocols: ("23/telnet" or "21/ftp")

3~not 443.https.tls.validation.browser_trusted: true

4~80.http.get.headers.server: Apache and protocols: "443/https"

5~validation.nss.valid: true and validation.nss.type: intermediate

第七部分

搜索样例

1~location.country_code: US and tags: scada

2~autonomous_system.description: University

3~alexa_rank: [1000 TO 1010]

4~github.com and tags: trusted

5~location.country_code:CN ports:"443" and gov.cn

第八部分

1~https://censys.io/domain，tmall.com

2~443.https.tls.certificate.parsed.names
*.m.yao.95095.com, feizhu.cn, 1688.com, xiami.com, *.dongting.com, fliggy.com, taopiaopiao.com, *.tmall.hk, *.1688.com, *.aliexpress.com, *.juhuasuan.com, *.alibaba.com, *.aliqin.tmall.com, *.fliggy.hk, *.cainiao.com, m.intl.taobao.com, *.m.1688.com, fliggy.hk, *.taobao.com, cainiao.com, *.m.tmall.hk, taobao.com, feizhu.com, ttpod.com, *.feizhu.cn, *.mei.com, *.tmall.com, *.chi.taobao.com, *.m.taopiaopiao.com, aliyun.com, *.chi.tmall.com, *.ttpod.com, *.m.taobao.com, *.taopiaopiao.com, cainiao.c

3~443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names
*.tmall.com, *.1688.com, m.intl.taobao.com, feizhu.com, *.yao.95095.com, *.feizhu.com, juhuasuan.com, *.chi.taobao.com, *.aliexpress.com, *.alitrip.com, *.m.cainiao.com, tmall.hk, *.ju.taobao.com, dongting.com, *.m.taopiaopiao.com, *.juhuasuan.com, feizhu.cn, *.alibaba.com, *.china.taobao.com, 1688.com, ttpod.com, alibaba.com, *.aliyun.com, *.feizhu.cn, *.jia.tmall.com, aliyun.com, aliexpress.com, *.m.1688.com, *.chi.tmall.com, xiami.com, *.taopiaopiao.com, *.aliqin.tmall.com, cainiao.com, *.xia

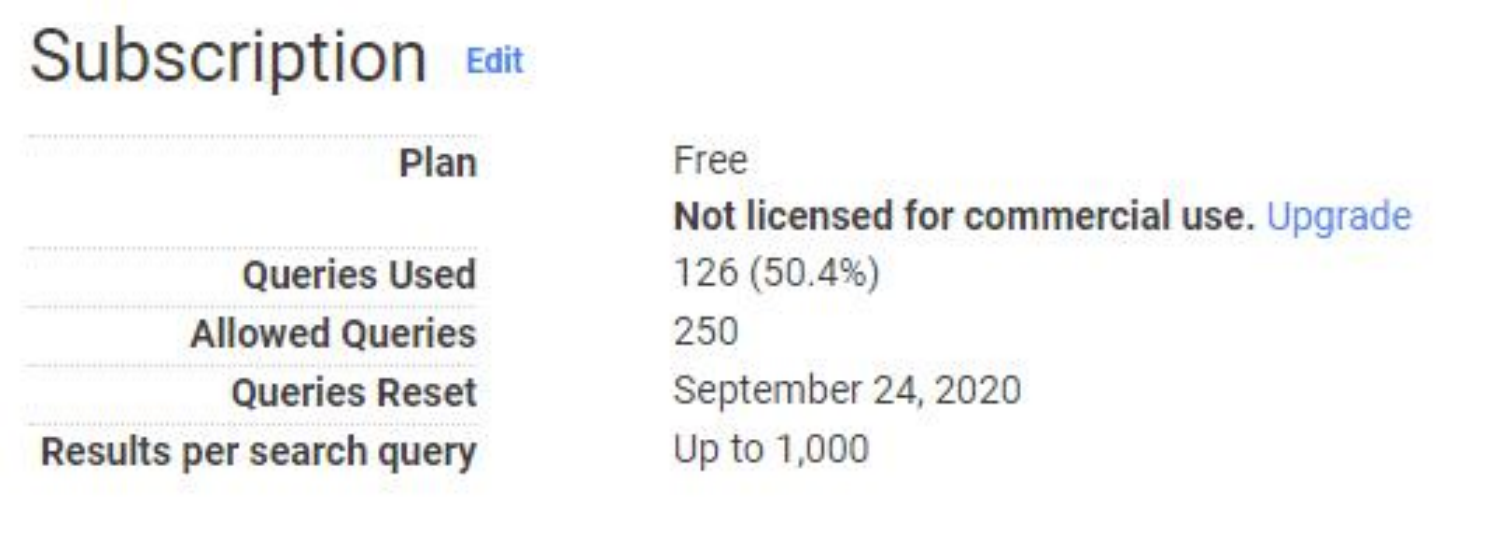
第九部分

domain:baidu.com

alexa_rank:1000

alexa_rank:[1000 TO 2000]

80.http_www.get.body:wordpress



Subscription Edit

Plan	Free **Not licensed for commercial use.** Upgrade
Queries Used	126 (50.4%)
Allowed Queries	250
Queries Reset	September 24, 2020
Results per search query	Up to 1,000

第十部分

1~Subject DN，Subject Distinguished Name，数字证书唯一标识符主题

2~Issuer DN　数字证书唯一标识符发布者

3~https数字证书

版本，序列号，签名算法，签名哈希算法，颁发者，有效期，使用者，公钥，公钥参数，授权信息访问，证书策略，基本约束，CRL分发点，使用者可选名称，增强型密钥用法，授权密钥标识符，使用者密钥标识符，SCT列表，密钥用法，指纹

4~浏览器的证书管理

5~公开密钥证书，EV SSL证书，客户端证书

6~数字签名（又称公钥数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

第十一部分

数字证书认证机构业务流程

1~网站运营者向数字证书机构申请服务器公开密钥，数字证书机构在确认对方身份之后，对公开密钥进行数字签名并分配给网站运营者，将公开密钥和公钥证书（服务器的公开密钥+数字证书认证机构的数字签名）绑定。

2~网站运营者发送公钥证书给客户端，便于进行加密通信。

3~客户端使用数字证书认证机构的公开密钥，向数字证书认证机构验证证书上的数字签名，如果验证通过，则说明服务器提供的公开密钥是来自数字证书认证机构，公开密钥是值得信赖的。

私钥用于解密，签名，用户知道，公钥用于加密，签名验证，公开的。

第十二部分

发送方
1~张三对要发送给李四的数据进行哈希计算，得到一个哈希值（消息摘要）。
2~张三用自己的私钥对哈希值加密，得到签名，附加到数据上。
3~张三随机生成一个密钥，并对数据加密。
4~张三用李四的公钥加密随机密钥，加密后的密钥和密文发给李四。

接收方
1~李四用自己的私钥解密，获得随机密钥。
2~李四用随机密钥进行解密，获得明文数据。
3~李四使用张三的公钥解密数字签名，得到数据哈希。
4~再次计算数据哈希，与接收到的

制作视频相关软件

1-WPS Office

2~迅捷屏幕录像工具

3~迅捷视频转换器

共勉

早睡早起，学好英语。
少看手机，多多实践。

感谢筒子们观看咯！