**社工-信息收集**

**1域名信息**

* 1. Whois

**Whois 可以查询域名是否被注册，以及注册域名的详细信息的数据库，其中可能会存在一些有用的信息，例如域名所有人、域名注册商、邮箱等。**

* 1. 搜索引擎搜索

**搜索引擎通常会记录域名信息，可以通过 site: domain （谷歌hack语法）的语法来查询。**

1.3 第三方查询

**网络中有相当多的第三方应用提供了子域的查询功能，下面有一些例子，更多的网站可以在 8.1 工具列表 中查找。DNSDumpster,Virustotal,CrtSearch,threatminer,Censys**

<https://dnsdumpster.com/> <https://www.virustotal.com/gui/>

1.4. ASN信息关联

**在网络中一个自治系统(Autonomous System, AS)是一个有权自主地决定在本系统中应采用何种路由协议的小型单位。这个网络单位可以是一个简单的网络也可以是一个由一个或多个普通的网络管理员来控制的网络群体，它是一个单独的可管理的网络单元（例如一所大学，一个企业或者一个公司个体）。**

**一个自治系统有时也被称为是一个路由选择域（routing domain）。一个自治系统将会分配一个全局的唯一的16位号码，这个号码被称为自治系统号（ASN）。因此可以通过ASN号来查找可能相关的IP，例如：**

**whois -h whois.radb.net -- '-i origin AS111111' | grep -Eo "([0-9.]+){4}/[0-9]+" | uniq**

**nmap --script targets-asn --script-args targets-asn.asn=15169**

1.5. 域名相关性

**同一个企业/个人注册的多个域名通常具有一定的相关性，例如使用了同一个邮箱来注册、使用了同一个备案、同一个负责人来注册等，可以使用这种方式来查找关联的域名。一种操作步骤如下：**

**---查询域名注册邮箱**

**---通过域名查询备案号**

**---通过备案号查询域名**

**---反查注册邮箱**

**---反查注册人**

**---通过注册人查询到的域名在查询邮箱**

**---通过上一步邮箱去查询域名**

**---查询以上获取出的域名的子域名**

1.6. 网站信息利用

**网站中有相当多的信息，网站本身、各项安全策略、设置等都可能暴露出一些信息。**

**网站本身的交互通常不囿于单个域名，会和其他子域交互。对于这种情况，可以通过爬取网站，收集站点中的其他子域信息。这些信息通常出现在JavaScript文件、资源文件链接等位置。**

**网站的安全策略如跨域策略、CSP规则等通常也包含相关域名的信息。有时候多个域名为了方便会使用同一个SSL/TLS证书，因此有时可通过证书来获取相关域名信息。**

1.7. 证书透明度

**为了保证HTTPS证书不会被误发或伪造，CA会将证书记录到可公开验证、不可篡改且只能附加内容的日志中，任何感兴趣的相关方都可以查看由授权中心签发的所有证书。因此可以通过查询已授权证书的方式来获得相关域名。**

1.8. 域传送漏洞

**DNS域传送（zone transfer）指的是冗余备份服务器使用来自主服务器的数据刷新自己的域（zone）数据库。这是为了防止主服务器因意外不可用时影响到整个域名的解析。**

**一般来说，域传送操作应该只允许可信的备用DNS服务器发起，但是如果错误配置了授权，那么任意用户都可以获得整个DNS服务器的域名信息。这种错误授权被称作是DNS域传送漏洞。**

1.9. Passive DNS

**Passive DNS被动的从递归域名服务器记录来自不同域名服务器的响应，形成数据库。利用Passive DNS数据库可以知道域名曾绑定过哪些IP，IP曾关联到哪些域名，域名最早/最近出现的时间，为测试提供较大的帮助。Virustotal、passivetotal、CIRCL等网站都提供了Passive DNS数据库的查询。**

1.10. SPF记录

**SPF(Sender Policy Framework)是为了防止垃圾邮件而提出来的一种DNS记录类型，是一种TXT类型的记录，用于登记某个域名拥有的用来外发邮件的所有IP地址。通过SPF记录可以获取相关的IP信息。**

1.11. CDN

**1.1.1. CDN验证**

**可通过多地ping的方式确定目标是否使用了CDN，常用的网站有 http://ping.chinaz.com/ https://asm.ca.com/en/ping.php 等。1.12. 子域爆破**

**1.1.2. 域名查找**

**使用了CDN的域名的父域或者子域名不一定使用了CDN，可以通过这种方式去查找对应的IP。**

**1.1.3. 历史记录查找**

**CDN可能是在网站上线一段时间后才上线的，可以通过查找域名解析记录的方式去查找真实IP。**

**1.1.12. 子域爆破**

**在内网等不易用到以上技巧的环境，或者想监测新域名上线时，可以通过批量尝试的方式，找到有效的域名。**

1.1.2. 域名查找

**在内网等不易用到以上技巧的环境，或者想监测新域名上线时，可以通过批量尝试的方式，找到有效的域名。**

**2端口信息**

2.1. 常见端口及其脆弱点

--F**TP 21**

**默认用户名密码 anonymous:anonymous**

**暴力破解密码**

**VSFTP某版本后门**

**--SSH 22**

**暴力破解密码**

**--Telent 23**

**暴力破解密码**

**--SMTP 25**

**无认证时可伪造发件人**

**--DNS 53 UDP**

**测试域传送漏洞**

**SPF / DMARC Check**

**DDoS**

**DNS Query Flood**

**DNS 反弹**

**--SMB 137/139/445**

**未授权访问**

**弱口令**

**--SNMP 161**

**Public 弱口令**

**--LDAP 389**

**匿名访问**

**注入**

**--Rsync 873**

**任意文件读写**

**--RPC 1025**

**NFS匿名访问**

**--MSSQL 1433**

**弱密码**

**--Java RMI 1099**

**RCE**

**--Oracle 1521**

**弱密码**

**--NFS 2049**

**权限设置不当**

**--ZooKeeper 2181**

**无身份认证**

**--MySQL 3306**

**弱密码**

**--RDP 3389**

**弱密码**

**--Postgres 5432**

**弱密码**

**--CouchDB 5984**

**未授权访问**

**--Redis 6379**

**无密码或弱密码**

**--Elasticsearch 9200**

**代码执行**

**--Memcached 11211**

**未授权访问**

**--MongoDB 27017**

**无密码或弱密码**

**--Hadoop 50070**

**除了以上列出的可能出现的问题，暴露在公网上的服务若不是最新版，都可能存在已经公开的漏洞**

2.2. 常见端口扫描方式

2.2.1全扫描

**扫描主机尝试使用三次握手与目标主机的某个端口建立正规的连接，若成功建立连接，则端口处于开放状态，反之处于关闭状态。全扫描实现简单，且以较低的权限就可以进行该操作。但是在流量日志中会有大量明显的记录**。

2.2.2 半扫描

**在半扫描中，仅发送SYN数据段，如果应答为RST，则端口处于关闭状态，若应答为SYN/ACK，则端口处于监听状态。不过这种方式需要较高的权限，而且部分防火墙已经开始对这种扫描方式做处理。**

2.2.3. FIN扫描

**FIN扫描是向目标发送一个FIN数据包，如果是开放的端口，会返回RST数据包，关闭的端口则不会返回数据包，可以通过这种方式来判断端口是否打开。**

**这种方式并不在TCP三次握手的状态中，所以不会被记录，相对SYN扫描要更隐蔽一些**。

2.3. Web服务

Jenkins

未授权访问

Gitlab

对应版本CVE

Zabbix

权限设置不当

2.4. 批量搜索

Censys

Shodan

ZoomEye

**3站点信息**

3.1判断网站操作系统

Linux大小写敏感

Windows大小写不敏感

3.2扫描敏感文件

robots.txt

crossdomain.xml

sitemap.xml

xx.tar.gz

xx.bak

等

3.3确定网站采用的语言

如PHP / Java / Python等

找后缀，比如php/asp/jsp

3.4前端框架

如jQuery / BootStrap / Vue / React / Angular等

查看源代码

3.5中间服务器

如 Apache / Nginx / IIS 等

查看header中的信息

根据报错信息判断

根据默认页面判断

3.6Web容器服务器

如Tomcat / Jboss / Weblogic等

3.7后端框架

根据Cookie判断

根据CSS / 图片等资源的hash值判断

根据URL路由判断

如wp-admin

根据网页中的关键字判断

根据响应头中的X-Powered-By

3.8 CDN信息

常见的有Cloudflare、yunjiasu

3.9探测有没有WAF，如果有，什么类型的

有WAF，找绕过方式

没有，进入下一步

3.10扫描敏感目录，看是否存在信息泄漏

扫描之前先自己尝试几个的url，人为看看反应

使用爬虫爬取网站信息

拿到一定信息后，通过拿到的目录名称，文件名称及文件扩展名了解网站开发人员的命名思路，确定其命名规则，推测出更多的目录及文件名

3.11常见入口目标

关注度低的系统

业务线较长的系统

1. **搜索引擎利用**

恰当地使用搜索引擎（Google/Bing/Yahoo/Baidu等）可以获取目标站点的较多信息。

* 1. 搜索引擎处理流程

数据预处理

长度截断

大小写转化

去标点符号

简繁转换

数字归一化，中文数字、阿拉伯数字、罗马字

同义词改写

拼音改写

处理

分词

关键词抽取

非法信息过滤

* 1. 搜索技巧

site:www.hao123.com

返回此目标站点被搜索引擎抓取收录的所有内容

site:www.hao123.com keyword

返回此目标站点被搜索引擎抓取收录的包含此关键词的所有页面

此处可以将关键词设定为网站后台，管理后台，密码修改，密码找回等

site:www.hao123.com inurl:admin.php

返回目标站点的地址中包含admin.php的所有页面，可以使用admin.php/manage.php或者其他关键词来寻找关键功能页面

link:www.hao123.com

返回所有包含目标站点链接的页面，其中包括其开发人员的个人博客，开发日志，或者开放这个站点的第三方公司，合作伙伴等

related:www.hao123.com

返回所有与目标站点”相似”的页面，可能会包含一些通用程序的信息等

intitle:"500 Internal Server Error" "server at"

搜索出错的页面

inurl:"nph-proxy.cgi" "Start browsing"

查找代理服务器

除了以上的关键字，还有allintile、allinurl、allintext、inanchor、cache等。

* 1. 快照

搜索引擎的快照中也常包含一些关键信息，如程序报错信息可以会泄漏网站具体路径，或者一些快照中会保存一些测试用的测试信息，比如说某个网站在开发了后台功能模块的时候，还没给所有页面增加权限鉴别，此时被搜索引擎抓取了快照，即使后来网站增加了权限鉴别，但搜索引擎的快照中仍会保留这些信息。

另外也有专门的站点快照提供快照功能，如 Wayback Machine 和 Archive.org 等。

4.4. tips

查询不区分大小写

\* 代表某一个单词

默认用and

OR 或者 | 代表逻辑或

单词前跟+表强制查询

引号引起来可以防止常见词被忽略

括号会被忽略

1. **社会工程学**

5.1. 企业信息收集

一些网站如天眼查等，可以提供企业关系挖掘、工商信息、商标专利、企业年报等信息查询，可以提供企业的较为细致的信息。公司主站中会有业务方向、合作单位等信息。

5.2. 人员信息收集

针对人员的信息收集考虑对目标重要人员、组织架构、社会关系的收集和分析。其中重要人员主要指高管、系统管理员、运维、财务、人事、业务人员的个人电脑。

人员信息收集较容易的入口点是网站，网站中可能包含网站的开发、管理维护等人员的信息。从网站联系功能中和代码的注释信息中都可能得到的所有开发及维护人员的姓名和邮件地址及其他联系方式。

在获取这些信息后，可以在Github/Linkedin等网站中进一步查找这些人在互联网上发布的与目标站点有关的一切信息，分析并发现有用的信息。

此外，可以对获取到的邮箱进行密码爆破的操作，获取对应的密码。

1. **参考链接**