CND识别以及绕过

判断

使用ping工具，如果目标存在多个IP情况则有可能使用了CDN

使用nslookup查看目标IP情况，多个IP则可能存在CDN

使用在线网站进行查询：https://www.cdnplanet.com/tools/cdnfinder/

使用python脚本，需要在kali上运行https://github.com/3xp10it/xcdn

```
python3 xcdn.py www.baidu.com
```

绕过CDN查看目真实IP

使用工具进行查询：https://github.com/Pluto-123/Bypass_cdn

通过国外进行ping操作，可能会得到目标真实IP https://tools.ipip.net/cdn.php

查询DNS历史记录 https://dnsdb.io/zh-cn/

通过邮件服务查询，当目标存在邮件服务时，可通过对方发送回来的邮件源码，查看目标的真实IP

查询遗留文件："site:xxx.com inurl:phpinfo.php" phpinfo文件中可能会存在目标真实ip

通过favicon.ico图标的hash值进行查询:

shodan: http:favicon.hash:hash值

fofa : icon_hash="hash值"

Whois收集信息

https://x.threatbook.cn/

https://who.is/

重点关注邮箱，注册人，电话号码，DNS解析服务器等信息

如果网站悬挂备案号，可以通过查询备案获得网站公司信息，再通过公司查询子公司，寻找更多的根域名

天眼查：https://www.tianyancha.com/

ICP备案查询网：http://www.beianbeian.com/

国家企业信用信息公示系统：http://www.gsxt.gov.cn/index.html

企查查，通过股权穿透图一直往下寻找，资产大于51%即为自身资产，可列入攻击对象

目标是为了获得较多的根域名，以及个人信息等，可用于社工，钓鱼等

收集子域名

https://x.threatbook.com/ 关键词搜索

使用工具：

oneforall:

基本使用方法：

```
python3 oneforall.py --target xxx.com run
```

得到的结果会储存在表内；一般关注表example_com_now_result

需要使用fofa等账户才能搜索到较多的信息

layer子域名挖掘机:
使用默认字典，自定义字典后缀规则为.dic

JSFinder

参考使用,收集js信息

```
python JSFinder.py -u http://www.mi.com -d -ou mi_url.txt -os mi_subdomain.txt
```

ksubdomain

信息准确且速度快，使用时无法进行上网

指纹探测与资产识别

指纹识别

指纹识别用于帮助我们对网站的web容器或者是cms进行识别，为后面寻找相应的漏洞做铺垫

Eholes

```
EHole -l url.txt   //URL地址需带上协议,每行一个
```

Finger

```
python3 Finger.py -f url.txt
```

对重要资产进行识别

端口，C段扫描

fcan

https://github.com/shadow1ng/fscan.git

集端口扫描，C段识别等功能

```
fscan.exe -h 192.168.1.1/24  (默认使用全部模块)
```

namp

namp除了用作端口扫描以外，还能用于主机探测，操作系统监测，脚本引擎等等

```
====几个常用的参数====
-sV 服务版本识别，在进行端口扫描的时候检测服务端软件的版本信息
-O 操作系统的识别
-Pn 禁用主机检测，如果对方主机禁用了ping检测，nmap可能会认为对方主机关机，从而无法获得更多的信息
-A 强力检测选项，包含前两个参数并且添加-sC(脚本扫描),-traceroute
-sT TCP握手选项，每一次请求都会经过TCP的三次握手连接
-sS 半开连接选项，通过发送SYN数据包进行端口嗅探，如果对方回复SYN包说明端口开放，反之端口屏蔽或未开放
-sl 通过僵尸主机进行请求
此外还有-sA/-sW/-sM等基于tcp连接的请求方式
    ==基于UDP的扫描选项==
    -sU 为了提升扫描速度我们需要自行-p指定扫描端口，完成一次完整的UDP扫描需要大量的时间
    ==目标端口选项==
    -p 扫描指定端口或者端口范围 eg:
                                -p 1-1024 (扫描1~1024端口)
                                -p- (扫描1~65535端口)
    -F(快速扫描，仅扫描100个常用端口)
    -r(顺序扫描，按照从小到大进行端口扫描)
    -top-ports <1 or="" greater="">：扫描nmap-services 里排名前N的端口。
    ==输出选项==
    -oN(正常输出) 不显示runtime和警告信息
    -oX 生成xml文件，可转换为html文件
    -oG gerp文件
    -oA 以标准格式输出所有文件，包括.nmap/.xml/.gnmap
    ==时间线程控制选项==
    -T 选择时间控制模式
-6 扫描IPv6主机
    ==脚本引擎功能==
    uth：此类脚本使用暴力破解等技术找出目标系统上的认证信息。
    default：启用--sC 或者-A 选项时运行此类脚本。这类脚本同时具有下述特点：执行速度快；输出的信息有指导下一步操作的价 值；输出信息内容丰富、形式简洁；必须可靠；不会侵入目标系统；能泄露信息给第三方。
    discovery：该类脚本用于探索网络。
    dos：该类脚本可能使目标系统拒绝服务，请谨慎使用。
    exploit：该类脚本利用目标系统的安全漏洞。在运行这类脚本之前，渗透测试人员需要获取 被测单位的行动许可。
    external：该类脚本可能泄露信息给第三方。
    fuzzer：该类脚本用于对目标系统进行模糊测试。
    instrusive：该类脚本可能导致目标系统崩溃，或耗尽目标系统的所有资源。
    malware：该类脚本检查目标系统上是否存在恶意软件或后门。
    safe：该类脚本不会导致目标服务崩溃、拒绝服务且不利用漏洞。
    version：配合版本检测选项（-sV），这类脚本对目标系统的服务程序进行深入的版本检 测。
    vuln：该类脚本可检测检查目标系统上的安全漏洞。
    在Kali Linux系统中，Nmap脚本位于目录/usr/share/nmap/scripts。
    -sC 或--script=default：启动默认类NSE 脚本。
    --script <filename>|<category>|<directories>：根据指定的文件名、类别名、目录名，执行 相应的脚本。
    --script-args <args>：这个选项用于给脚本指定参数。例如，在使用认证类脚本时，可通过 这个选项指定用户名和密码
    ==规避检测的选项==
```

```
目标主机存在waf时，使用默认选项扫描不仅会被发现，也扫描不出什么东西，就需要使用这些选项
-f 使用小数据包，对方可能无法识别我方的数据包
--mtu 调整数据包的大小，必须是8的整数
-D 诱饵选项 指定诱饵IP，在发送数据包时惨杂这些IP数据包来混淆
--source-port <portnumber> or -g 当某些waf仅允许指定端口有入站流量时使用
--data-length: 改变nmap发送数据包的默认数据长度，避免被识别出是nmap的扫描
--max-parallelism 限制nmap并发扫描的最大连接数
--scan-delay <time> 控制发送数据的时间间隔，避免达到IDS/IPS扫描规则的阈值
```

waf探测

wafw00f

https://github.com/EnableSecurity/wafw00f

使用方法

```
wafwoof http://...........
```

whatwaf

https://github.com/Ekultek/WhatWaf

敏感信息收集

Googlehack语法

1. 后台地址

- site:xxx.com intitle:管理|后台|登陆|管理员|系统|内部
- site:xxx.com inurl:login|admin|system|guanli|denglu|manage|admin_login|auth|dev

1. 敏感文件

- site:xxx.com (filetype:doc OR filetype:ppt OR filetype:pps OR filetype:xls OR filetype:docx OR filetype:pptx OR filetype:ppsx OR filetype:xlsx OR filetype:odt OR filetype:ods OR filetype:odg OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetype:sql OR filetype:xml OR filetype:db OR filetype:mdb OR filetype:sqlite OR filetype:log OR filetype:conf)

1. 测试环境

- site:xxx.com inurl:test|ceshi
- site:xxx.com intitle:测试

1. 邮箱

- site:xxx.com (intitle:"Outlook Web App" OR intitle:"邮件" OR inurl:"email" OR inurl:"webmail")

1. 其他

- site:xxx.com inurl:api|uid=|id=|userid=|token|session
- site:xxx.com intitle:index.of "server at"

Github

- @xxx.com password/secret/credentials/token/config/pass/login/ftp/ssh/pwd
- @xxx.com security_credentials/connetionstring/JDBC/ssh2_auth_password/send_keys

APP

如果存在APP可以测试APP中的内容

https://github.com/cqkenuo/appinfoscanner

公众号

https://weixin.sogou.com/

同样公众号中的功能点可以进行手动测试

漏洞扫描

Xray

批量化的进行漏洞扫描，方便，需要将线程设置较低

awvs

可使用脚本批量导入进行扫描

参考链接

https://github.com/Paper-Pen/GatherInfo/blob/master/%E6%B8%97%E9%80%8F%E6%9C%AC%E8%B4%A8%E4%B9%8B%E4%BF%A1%E6%81%AF%E6%94%B6%E9%9B%86.md

https://www.anquanke.com/post/id/274493

https://blog.csdn.net/m0_51191308/article/details/128064964