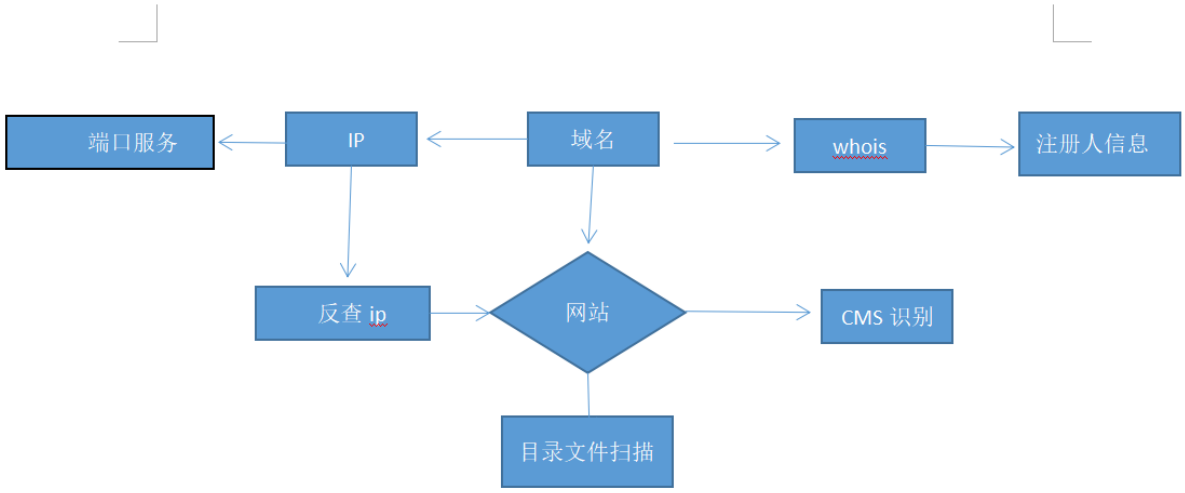
1. 简介

渗透的本质是信息收集

信息收集也叫做资产收集

信息收集是渗透测试的前期主要工作，是非常重要的环节，收集足够多的信息才能方便接下来的测试，信息收集主要是收集网站的域名信息、子域名信息、目标网站信息、目标网站真实IP、敏感/目录文件、开放端口和中间件信息等等。通过各种渠道和手段尽可能收集到多的关于这个站点的信息，有助于我们更多的去找到渗透点，突破口。

小项目：



信息收集

大项目：

某个集团的资产收集：

查询公司集团旗下的网站

备案号备案名查询公司相关的减名查询子域名域名下的网站cms识别判断网站类型原创开发二次开发还是使现成网站管理系统oa版本系统

ip的分布服务器信息包括端口和开发的服务器。

线上系统业务相关系统企业邮箱oa版本系统生产环境测试环境边界设备 Vpn

集团有没有防火墙有的话是防火墙的类型wifi进入公司内部收集资产

社工客户、销售发连接脉脉招聘hr qq钉钉微信群长期蹲点获取更多有用的有价值的信息社交关系网

根据需求制定不同的渗透测试手段

网络空间的搜索github谷歌hacking fofa sohdan钟道之眼

2. 信息收集的分类

1. 服务器的相关信息（真实ip，系统类型，版本，开放端口，WAF等）
2. 网站指纹识别（包括，cms，cdn，证书等） dns记录
3. whois信息，姓名，备案，邮箱，电话反查（邮箱丢社工库，社工准备等）
4. 子域名收集，旁站，C段等
5. google hacking针对化搜索，word/电子表格/pdf文件，中间件版本，弱口令扫描等
6. 扫描网站目录结构，爆后台，网站banner，测试文件，备份等敏感文件泄漏等
7. 传输协议，通用漏洞，exp，github源码等

3. 常见的方法有

1. whois查询

域名在注册的时候 需要填入个人或者企业信息 如果没有设置隐藏属性可以查询出来 通过备案号 查询个人或者企业信息 也可以whois反查注册人 邮箱 电话 机构 反查更多得域名和需要得信息。

2. 收集子域名

域名分为根域名和子域名

moonsec.com 根域名 顶级域名

www.moonsec.com子域名 也叫二级域名

www.wiki.moonsec.com 子域名 也叫三级域名 四级如此类推

3. 端口扫描

服务器需要开放服务，就必须开启端口，常见的端口是tcp 和udp两种类型

范围 0-65535 通过扫得到的端口，访问服务 规划下一步渗透。

4. 查找真实ip

企业的网站，为了提高访问速度，或者避免黑客攻击，用了cdn服务，用了cdn之后真实服务器ip会被隐藏。

5. 探测旁站及C段

旁站:一个服务器上有多个网站 通过ip查询服务器上的网站

c段:查找同一个段 服务器上的网站。可以找到同样网站的类型和服务器，也可以获取同段服务器进行下一步渗透。

6. 网络空间搜索引擎

通过这些引擎查找网站或者服务器的信息，进行下一步渗透。

7. 扫描敏感目录/文件

通过扫描目录和文件，大致了解网站的结构，获取突破点，比如后台，文件备份，上传点。

8. 指纹识别

获取网站的版本，属于那些cms管理系统，查找漏洞exp，下载cms进行代码审计。

4. 在线whois查询

通过whois来对域名信息进行查询，可以查到注册商、注册人、邮箱、DNS解析服务器、注册人联系电话等，因为有些网站信息查得到，有些网站信息查不到，所以推荐以下信息比较全的查询网站，直接输入目标站点即可查询到相关信息。

站长之家域名WHOIS信息查询地址 http://whois.chinaz.com/

爱站网域名WHOIS信息查询地址 https://whois.aizhan.com/

腾讯云域名WHOIS信息查询地址 https://whois.cloud.tencent.com/

美橙互联域名WHOIS信息查询地址 https://whois.cndns.com/

爱名网域名WHOIS信息查询地址 https://www.22.cn/domain/

易名网域名WHOIS信息查询地址 https://whois.ename.net/

中国万网域名WHOIS信息查询地址 https://whois.aliyun.com/

西部数码域名WHOIS信息查询地址 https://whois.west.cn/

新网域名WHOIS信息查询地址 http://whois.xinnet.com/domain/whois/index.jsp

纳网域名WHOIS信息查询地址 http://whois.nawang.cn/

中资源域名WHOIS信息查询地址 https://www.zzy.cn/domain/whois.html

三五互联域名WHOIS信息查询地址 https://cp.35.com/chinese/whois.php

新网互联域名WHOIS信息查询地址 http://www.dns.com.cn/show/domain/whois/index.do

国外WHOIS信息查询地址 https://who.is/

4.1. 在线网站备案查询

网站备案信息是根据国家法律法规规定，由网站所有者向国家有关部门申请的备案，如果需要查询企业备案信息（单位名称、备案编号、网站负责人、电子邮箱、联系电话、法人等），推荐以下网站查询

1. 天眼查 https://www.tianyancha.com/
2. ICP备案查询网http://www.beianbeian.com/
3. 爱站备案查询https://icp.aizhan.com/
4. 域名助手备案信息查询 http://cha.fute.com/index

5. 收集子域名

5.1. 子域名作用

收集子域名可以扩大测试范围，同一域名下的二级域名都属于目标范围。

5.2. 常用方式

子域名中的常见资产类型一般包括办公系统，邮箱系统，论坛，商城，其他管理系统，网站管理后台也有可能出现子域名中。

首先找到目标站点，在官网中可能会找到相关资产（多为办公系统，邮箱系统等），关注一下页面底部，也许有管理后台等收获。

查找目标域名信息的方法有：

1. FOFA title="公司名称"
2. 百度 intitle=公司名称
3. Google intitle=公司名称
4. 站长之家，直接搜索名称或者网站域名即可查看相关信息：

http://tool.chinaz.com/

5. 钟馗之眼 site=域名即可

https://www.zoomeye.org/

找到官网后，再收集子域名，下面推荐几种子域名收集的方法，直接输入domain即可查询

5.3. 域名的类型

A记录、别名记录(CNAME)、MX记录、TXT记录、NS记录：

5.3.1. A (Address) 记录：

是用来指定主机名（或域名）对应的IP地址记录。用户可以将该域名下的网站服务器指向到自己的web server上。同时也可以设置您域名的二级域名。

5.3.2. 别名(CNAME)记录：

也被称为规范名字。这种记录允许您将多个名字映射到同一台计算机。通常用于同时提供WWW和MAIL服务的计算机。例如，有一台计算机名为“host.mydomain.com”（A记录）。它同时提供WWW和MAIL服务，为了便于用户访问服务。可以为该计算机设置两个别名（CNAME）：WWW和MAIL。这两个别名的全称就是“www.mydomain.com”和“mail.mydomain.com”。实际上他们都指向“host.mydomain.com”。同样的方法可以用于当您拥有多个域名需要指向同一服务器IP，此时您就可以将一个域名做A记录指向服务器IP然后将其他的域名做别名到之前做A记录的域名上，那么当您的服务器IP地址变更时您就可以不必麻烦的一个一个域名更改指向了 只需要更改做A记录的那个域名其他做别名的那些域名的指向也将自动更改到新的IP地址上了。

5.3.3. 如何检测CNAME记录?

1、进入命令状态；（开始菜单 - 运行 - CMD[回车]）；

2、输入命令" nslookup -q=cname 这里填写对应的域名或二级域名"，查看返回的结果与设置的是否一致即可。

5.3.4. MX（Mail Exchanger）记录：

是邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据 收信人的地址后缀来定位邮件服务器。例如，当Internet上的某用户要发一封信给 user@mydomain.com 时，该用户的邮件系统通过DNS查找mydomain.com这个域名的MX记录，如果MX记录存在， 用户计算机就将邮件发送到MX记录所指定的邮件服务器上。

5.3.5. 什么是TXT记录？：

TXT记录一般指为某个主机名或域名设置的说明，如：

1）admin IN TXT "jack, mobile:13800138000";

2）mail IN TXT "邮件主机, 存放在xxx ,管理人：AAA"，Jim IN TXT "contact: abc@mailserver.com"

也就是您可以设置 TXT ，以便使别人联系到您。

如何检测TXT记录?

1、进入命令状态；（开始菜单 - 运行 - CMD[回车]）；

2、输入命令" nslookup -q=txt 这里填写对应的域名或二级域名"，查看返回的结果与设置的是否一致即可。

5.3.6. 什么是NS记录?

ns记录全称为Name Server 是一种域名服务器记录，用来明确当前你的域名是由哪个DNS服务器来进行解析的。

5.3.7. 子域名在线查询1

https://phpinfo.me/domain/

5.3.8. 子域名在线查询2

https://www.t1h2ua.cn/tools/

5.3.9. dns侦测

https://dnsdumpster.com/

5.3.10. IP138查询子域名

https://site.ip138.com/moonsec.com/domain.htm

5.3.11. FOFA搜索子域名

https://fofa.so/

语法：domain="baidu.com"

提示：以上两种方法无需爆破，查询速度快，需要快速收集资产时可以优先使用，后面再用其他方法补充。

5.3.12. Hackertarget查询子域名

https://hackertarget.com/find-dns-host-records/

注意：通过该方法查询子域名可以得到一个目标大概的ip段，接下来可以通过ip来收集信息。

5.4. 360测绘空间

https://quake.360.cn/

domain:"*.freebuf.com"

5.4.1. Layer子域名挖掘机

5.4.2. SubDomainBrute

pip install aiodns)

运行命令subDomainsBrute.py freebuf.com

subDomainsBrute.py freebuf.com --full -o freebuf2.txt

5.4.3. Sublist3r

https://github.com/aboul3la/Sublist3r

pip install -r requirements.txt

提示：以上方法为爆破子域名，由于字典比较强大，所以效率较高。

帮助文档

usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]]
[-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:

-h, --help show this help message and exit

-d DOMAIN, --domain DOMAIN

Domain name to enumerate it's subdomains

-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]

Enable the subbrute bruteforce module

-p PORTS, --ports PORTS

Scan the found subdomains against specified tcp ports

-v [VERBOSE], --verbose [VERBOSE]

Enable Verbosity and display results in realtime

-t THREADS, --threads THREADS

Number of threads to use for subbrute bruteforce

-e ENGINES, --engines ENGINES

Specify a comma-separated list of search engines

-o OUTPUT, --output OUTPUT

Save the results to text file

-n, --no-color Output without color

Example: python sublist3r.py -d google.com

中文翻译

-h： 帮助

-d： 指定主域名枚举子域名

-b： 调用subbrute暴力枚举子域名

-p： 指定tpc端口扫描子域名

-v： 显示实时详细信息结果

-t： 指定线程

-e： 指定搜索引擎

-o： 将结果保存到文本

-n： 输出不带颜色

默认参数扫描子域名

python sublist3r.py -d baidu.com

使用暴力枚举子域名

python sublist3r -b -d baidu.com

5.4.4. python2.7.14 环境

;C:\Python27;C:\Python27\Scripts

5.4.5. OneForALL

pip3 install --user -r requirements.txt -i https://mirrors.aliyun.com/pypi/simple/

python3 oneforall.py --target baidu.com run /*收集*/

爆破子域名

Example:

brute.py --target domain.com --word True run

brute.py --targets ./domains.txt --word True run

brute.py --target domain.com --word True --concurrent 2000 run

brute.py --target domain.com --word True --wordlist subnames.txt run

brute.py --target domain.com --word True --recursive True --depth 2 run

brute.py --target d.com --fuzz True --place m.*.d.com --rule '[a-z]' run

brute.py --target d.com --fuzz True --place m.*.d.com --fuzzlist subnames.txt run

5.4.6. Wydomain

dnsburte.py -d aliyun.com -f dnspod.csv -o aliyun.log

wydomain.py -d aliyun.com

5.4.7. FuzzDomain

5.4.8. 隐藏域名hosts碰撞

隐藏资产探测-hosts碰撞

https://mp.weixin.qq.com/s/fuASZODw1rLvgT7GySMC8Q

很多时候访问目标资产IP响应多为：401、403、404、500，但是用域名请求却能返回正常的业务系统（禁止IP直接访问），因为这大多数都是需要绑定host才能正常请求访问的 （目前互联网公司基本的做法）（域名删除了A记录，但是反代的配置未更新），那么我们就可以通过收集到的目标的 域名 和 目标资产 的IP段组合起来，以 IP段+域名 的形式进行捆绑碰撞，就能发现很多有意思的东西。

在发送http请求的时候，对域名和IP列表进行配对，然后遍历发送请求 （就相当于修改了本地的hosts文件一样），并把相应的title和响应包大小拿回 来做对比，即可快速发现一些隐蔽的资产。

进行hosts碰撞需要目标的域名和目标的相关IP作为字典

域名就不说了

相关IP来源有：

目标域名历史解析IP

https://site.ip138.com/

https://ipchaxun.com/

ip正则

https://www.aicesu.cn/reg/

6. 端口扫描

当确定了目标大概的ip段后，可以先对ip的开放端口进行探测，一些特定服务可能开起在默认端口上，探测开放端口有利于快速收集目标资产，找到目标网站的其他功能站点。

6.1. msscan端口扫描

msscan -p 1-65535 ip --rate=1000

https://gitee.com/youshusoft/GoScanner/

6.2. 御剑端口扫描工具

6.3. nmap扫描端口和探测端口信息

常用参数，如：

nmap -sV 192.168.0.2

nmap -sT 92.168.0.2

nmap -Pn -A -sC 192.168.0.2

nmap -sU -sT -p0-65535 192.168.122.1

用于扫描目标主机服务版本号与开放的端口

如果需要扫描多个ip或ip段，可以将他们保存到一个txt文件中

nmap -iL ip.txt

来扫描列表中所有的ip。

Nmap为端口探测最常用的方法，操作方便，输出结果非常直观。

6.4. 在线端口检测

http://coolaf.com/tool/port

6.5. 端口扫描器

御剑，msscan，zmap等

御剑高速端口扫描器：

填入想要扫描的ip段（如果只扫描一个ip，则开始IP和结束IP填一个即可），可以选择不改默认端口列表，也可以选择自己指定端口。

6.6. 渗透端口

21,22,23,1433,152,3306,3389,5432,5900,50070,50030,50000,27017,27018,11211,9200,9300,7001,7002,6379,5984,873,443,8000-9090,80-89,80,10000,8888,8649,8083,8080,8089,9090,7778,7001,7002,6082,5984,4440,3312,3311,3128,2601,2604,2222,2082,2083,389,88,512,513,514,1025,111,1521,445,135,139,53

6.7. 渗透常见端口及对应服务

1.web类(web漏洞/敏感目录)

第三方通用组件漏洞struts thinkphp jboss ganglia zabbix

80 web

80-89 web

8000-9090 web

2.数据库类(扫描弱口令)

1433 MSSQL

1521 Oracle

3306 MySQL

5432 PostgreSQL

3.特殊服务类(未授权/命令执行类/漏洞)

443 SSL心脏滴血

873 Rsync未授权

5984 CouchDB http://xxx:5984/_utils/

6379 redis未授权

7001,7002 WebLogic默认弱口令，反序列

9200,9300 elasticsearch 参考WooYun: 多玩某服务器ElasticSearch命令执行漏洞

11211 memcache未授权访问

27017,27018 Mongodb未授权访问

50000 SAP命令执行

50070,50030 hadoop默认端口未授权访问

4.常用端口类(扫描弱口令/端口爆破)

21 ftp

22 SSH

23 Telnet

2601,2604 zebra路由，默认密码zebra

3389 远程桌面

5.端口合计详情

21 ftp

22 SSH

23 Telnet

80 web

80-89 web

161 SNMP

389 LDAP

443 SSL心脏滴血以及一些web漏洞测试

445 SMB

512,513,514 Rexec

873 Rsync未授权

1025,111 NFS

1433 MSSQL

1521 Oracle:(iSqlPlus Port:5560,7778)

2082/2083 cpanel主机管理系统登陆 （国外用较多）

2222 DA虚拟主机管理系统登陆 （国外用较多）

2601,2604 zebra路由，默认密码zebra

3128 squid代理默认端口，如果没设置口令很可能就直接漫游内网了

3306 MySQL

3312/3311 kangle主机管理系统登陆

3389 远程桌面

4440 rundeck 参考WooYun: 借用新浪某服务成功漫游新浪内网

5432 PostgreSQL

5900 vnc

5984 CouchDB http://xxx:5984/_utils/

6082 varnish 参考WooYun: Varnish HTTP accelerator CLI 未授权访问易导致网站被直接篡改或者作为代理进入内网

6379 redis未授权

7001,7002 WebLogic默认弱口令，反序列

7778 Kloxo主机控制面板登录

8000-9090 都是一些常见的web端口，有些运维喜欢把管理后台开在这些非80的端口上

8080 tomcat/WDCP主机管理系统，默认弱口令

8080,8089,9090 JBOSS

8083 Vestacp主机管理系统 （国外用较多）

8649 ganglia

8888 amh/LuManager 主机管理系统默认端口

9200,9300 elasticsearch 参考WooYun: 多玩某服务器ElasticSearch命令执行漏洞

10000 Virtualmin/Webmin 服务器虚拟主机管理系统

11211 memcache未授权访问

27017,27018 Mongodb未授权访问

28017 mongodb统计页面

50000 SAP命令执行

50070,50030 hadoop默认端口未授权访问

7. 查找真实ip

如果目标网站使用了CDN，使用了cdn真实的ip会被隐藏，如果要查找真实的服务器就必须获取真实的ip，根据这个ip继续查询旁站。

注意：很多时候，主站虽然是用了CDN，但子域名可能没有使用CDN，如果主站和子域名在一个ip段中，那么找到子域名的真实ip也是一种途径。

7.1. 多地ping确认是否使用CDN

http://ping.chinaz.com/

http://ping.aizhan.com/

7.2. 查询历史DNS解析记录

在查询到的历史解析记录中，最早的历史解析ip很有可能记录的就是真实ip，快速查找真实IP推荐此方法，但并不是所有网站都能查到。

7.2.1. DNSDB

https://dnsdb.io/zh-cn/

7.2.2. 微步在线

https://x.threatbook.cn/

7.2.3. Ipip.net

https://tools.ipip.net/cdn.php

7.2.4. viewdns

https://viewdns.info/

7.3. phpinfo

如果目标网站存在phpinfo泄露等，可以在phpinfo中的SERVER_ADDR或_SERVER[“SERVER_ADDR"]找到真实ip

7.4. 绕过CDN

绕过CDN的多种方法具体可以参考 https://www.cnblogs.com/qiudabai/p/9763739.html

8. 旁站和C段

旁站往往存在业务功能站点，建议先收集已有IP的旁站，再探测C段，确认C段目标后，再在C段的基础上再收集一次旁站。

旁站是和已知目标站点在同一服务器但不同端口的站点，通过以下方法搜索到旁站后，先访问一下确定是不是自己需要的站点信息。

8.1.1. 站长之家

同ip网站查询http://stool.chinaz.com/same

https://chapangzhan.com/

8.2. google hacking

https://blog.csdn.net/qq_36119192/article/details/84029809

8.2.1. 网络空间搜索引擎

如FOFA搜索旁站和C段

该方法效率较高，并能够直观地看到站点标题，但也有不常见端口未收录的情况，虽然这种情况很少，但之后补充资产的时候可以用下面的方法nmap扫描再收集一遍。

8.2.2. 在线c段 webscan.cc

webscan.cc

https://c.webscan.cc/

c段利用脚本

pip install requests

```
#coding:utf-8
import requests
import json

def get_c(ip):
    print("正在收集{}".format(ip))
    url="http://api.webscan.cc/?action=query&ip={}".format(ip)
    req=requests.get(url=url)
    html=req.text
    data=req.json()
    if 'null' not in html:
        with open("resulit.txt", 'a', encoding='utf-8') as f:
        f.write(ip + '\n')
```

```
            f.close()
        for i in data:
            with open("resulit.txt", 'a',encoding='utf-8') as f:
            f.write("\t{} {}\n".format(i['domain'],i['title']))
            print("   [+] {} {}[+]".format(i['domain'],i['title']))
            f.close()

def get_ips(ip):
    iplist=[]
    ips_str = ip[:ip.rfind('.')]
    for ips in range(1, 256):
        ipadd=ips_str + '.' + str(ips)
        iplist.append(ipadd)
    return iplist

ip=input("请你输入要查询的ip:")
ips=get_ips(ip)
for p in ips:
    get_c(p)
```

8.2.3. Nmap,Msscan扫描等

例如：nmap -p 80,443,8000,8080 -Pn 192.167.0.0/24

8.2.4. 常见端口表

21,22,23,80-90,161,389,443,445,873,1099,1433,1521,1900,2082,2083,2222,2601,2604,3128,3306,3311,3312,3389,4440,4848,5432,5560,5900,5901,5902,6082,6379,7001-7010,7778,8080-8090,8649,8888,9000,9200,10000,11211,27017,28017,50000,50030,50060,135,139,445,53,88

注意：探测C段时一定要确认ip是否归属于目标，因为一个C段中的所有ip不一定全部属于目标。

9. 网络空间搜索引擎

如果想要在短时间内快速收集资产，那么利用网络空间搜索引擎是不错的选择，可以直观地看到旁站，端口，站点标题，IP等信息，点击列举出站点可以直接访问，以此来判断是否为自己需要的站点信息。
FOFA的常用语法:

1、同IP旁站：ip="192.168.0.1"

2、C段：ip="192.168.0.0/24"

3、子域名：domain="baidu.com"

4、标题/关键字：title="百度"

5、如果需要将结果缩小到某个城市的范围，那么可以拼接语句

title="百度"&& region="Beijing"

6、特征：body="百度"或header="baidu"

10. 扫描敏感目录/文件

扫描敏感目录需要强大的字典，需要平时积累，拥有强大的字典能够更高效地找出网站的管理后台，敏感文件常见的如.git文件泄露，.svn文件泄露，phpinfo泄露等，这一步一半交给各类扫描器就可以了，将目标站点输入到域名中，选择对应字典类型，就可以开始扫描了，十分方便。

10.1. 御剑

https://www.fujieace.com/hacker/tools/yujian.html

10.2. 7kbstorm

https://github.com/7kbstorm/7kbscan-WebPathBrute

10.3. bbscan

https://github.com/lijiejie/BBScan

在pip已经安装的前提下，可以直接：

pip install -r requirements.txt

使用示例：

1. 扫描单个web服务 www.target.com

python BBScan.py --host www.target.com

2. 扫描www.target.com和www.target.com/28下的其他主机

python BBScan.py --host www.target.com --network 28

3. 扫描txt文件中的所有主机

python BBScan.py -f wandoujia.com.txt

4. 从文件夹中导入所有的主机并扫描

python BBScan.py -d targets/

–network 参数用于设置子网掩码，小公司设为28~30，中等规模公司设置26~28，大公司设为24~26

当然，尽量避免设为24，扫描过于耗时，除非是想在各SRC多刷几个漏洞。

该插件是从内部扫描器中抽离出来的，感谢 Jekkay Hu<34538980[at]qq.com>

如果你有非常有用的规则，请找几个网站验证测试后，再 pull request

脚本还会优化，接下来的事:

增加有用规则，将规则更好地分类，细化

后续可以直接从 rules\request 文件夹中导入HTTP_request

优化扫描逻辑

10.4. dirmap

pip install -r requirement.txt

https://github.com/H4ckForJob/dirmap

单个目标

python3 dirmap.py -i https://target.com -lcf

多个目标

python3 dirmap.py -iF urls.txt -lcf

10.5. dirsearch

https://gitee.com/Abaomianguan/dirsearch.git

unzip dirsearch.zip

python3 dirsearch.py -u http://m.scabjd.com/ -e *

10.6. gobuster

sudo apt-get install gobuster

gobuster dir -u https://www.servyou.com.cn/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -t 50

dir -u 网址 w字典 -x 指定后缀 -t 线程数量

dir -u https://www.servyou.com.cn/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x "php,html,rar,zip" -d --wildcard -o servyou.log | grep ^"3402"

10.7. 网站文件

1. robots.txt
2. crossdomin.xml
3. sitemap.xml
4. 后台目录
5. 网站安装包
6. 网站上传目录

7. mysql管理页面
8. phpinfo
9. 网站文本编辑器
10. 测试文件
11. 网站备份文件(.rar、zip、.7z、.tar.gz、.bak)
12. DS_Store 文件
13. vim编辑器备份文件(.swp)
14. WEB—INF/web.xml文件

15 .git

16 .svn

https://www.secpulse.com/archives/55286.html

11. 扫描网页备份

例如

config.php

config.php~

config.php.bak

config.php.swp

config.php.rar

conig.php.tar.gz

12. 网站头信息收集

1、中间件： web服务【Web Servers】 apache iis7 iis7.5 iis8 nginx WebLogic tomcat

2.、网站组件： js组件jquery、vue 页面的布局bootstrap

通过浏览器获取

http://whatweb.bugscaner.com/look/

火狐的插件Wappalyzer

curl命令查询头信息

curl https://www.moonsec.com -i

13. 敏感文件搜索

13.1. GitHub搜索

in:name test #仓库标题搜索含有关键字test

in:descripton test #仓库描述搜索含有关键字

in:readme test #Readme文件搜素含有关键字

搜索某些系统的密码

https://github.com/search?q=smtp+58.com+password+3306&type=Code

github 关键词监控

https://www.codercto.com/a/46640.html

谷歌搜索

site:Github.com sa password

site:Github.com root password

site:Github.com User ID='sa';Password

site:Github.com inurl:sql

SVN 信息收集

site:Github.com svn

site:Github.com svn username

site:Github.com svn password

site:Github.com svn username password

综合信息收集

site:Github.com password

site:Github.com ftp ftppassword

site:Github.com 密码

site:Github.com 内部

https://blog.csdn.net/qq_36119192/article/details/99690742

http://www.361way.com/github-hack/6284.html

https://docs.github.com/cn/github/searching-for-information-on-github/searching-code

https://github.com/search?q=smtp+bilibili.com&type=code

13.2. Google-hacking

site:域名

inurl: url中存在的关键字网页

intext：网页正文中的关键词

filetype:指定文件类型

13.3. wooyun漏洞库

https://wooyun.website/

13.4. 网盘搜索

凌云搜索 https://www.lingfengyun.com/

盘多多：http://www.panduoduo.net/

盘搜搜：http://www.pansoso.com/

盘搜：http://www.pansou.com/

13.5. 社工库

名字/常用id/邮箱/密码/电话 登录 网盘 网站 邮箱 找敏感信息

tg机器人

13.6. 网站注册信息

www.reg007.com 查询网站注册信息

一般是配合社工库一起来使用。

13.7. js敏感信息

1.网站的url连接写到js里面

2.js的api接口 里面包含用户信息 比如 账号和密码

13.7.1. jsfinder

https://gitee.com/kn1fes/JSFinder

python3 JSFinder.py -u http://www.mi.com

python3 JSFinder.py -u http://www.mi.com -d

python3 JSFinder.py -u http://www.mi.com -d -ou mi_url.txt -os mi_subdomain.txt

当你想获取更多信息的时候，可以使用-d进行深度爬取来获得更多内容，并使用命令 -ou, -os来指定URL和子域名所保存的文件名

批量指定URL和JS链接来获取里面的URL。

指定URL：

python JSFinder.py -f text.txt

指定JS：

python JSFinder.py -f text.txt -j

13.7.2. Packer-Fuzzer

寻找网站交互接口 授权key

随着WEB前端打包工具的流行，您在日常渗透测试、安全服务中是否遇到越来越多以Webpack打包器为代表的网站 这类打包器会将整站的API和API参数打包在一起供Web集中调用，这也便于我们快速发现网站的功能和API清单，但往往这些打包器所生成的JS文件数量异常之多并且总JS代码量异常庞大（多达上万行），这给我们的手工测试带来了极大的不便，Packer Fuzzer软件应运而生。

本工具支持自动模糊提取对应目标站点的API以及API对应的参数内容，并支持对：未授权访问、敏感信息泄露、CORS、SQL注入、水平越权、弱口令、任意文件上传七大漏洞进行模糊高效的快速检测。在扫描结束之后，本工具还支持自动生成扫描报告，您可以选择便于分析的HTML版本以及较为正规的doc、pdf、txt版本。

sudo apt-get install nodejs && sudo apt-get install npm

git clone https://gitee.com/keyboxdzd/Packer-Fuzzer.git

pip3 install -r requirements.txt

python3 PackerFuzzer.py -u https://www.liaoxuefeng.com

13.7.3. SecretFinder

一款基于Python脚本的JavaScript敏感信息搜索工具

https://gitee.com/mucn/SecretFinder

python3 SecretFinder.py -i https://www.moonsec.com/ -e

14. cms识别

收集好网站信息之后，应该对网站进行指纹识别，通过识别指纹，确定目标的cms及版本，方便制定下一步的测试计划，可以用公开的poc或自己累积的对应手法等进行正式的渗透测试。

14.1. 云悉

http://www.yunsee.cn/info.html

14.2. 潮汐指纹

http://finger.tidesec.net/

14.3. CMS指纹识别

http://whatweb.bugscaner.com/look/

https://github.com/search?q=cms识别

14.4. whatcms

14.5. 御剑cms识别

https://github.com/ldbfpiaoran/cmscan

https://github.com/theLSA/cmsIdentification/

15. 非常规操作

1、如果找到了目标的一处资产，但是对目标其他资产的收集无处下手时，可以查看一下该站点的body里是否有目标的特征，然后利用网络空间搜索引擎（如fofa等）对该特征进行搜索，如：body=”XX公司”或body=”baidu”等。

该方式一般适用于特征明显，资产数量较多的目标，并且很多时候效果拔群。

2、当通过上述方式的找到test.com的特征后，再进行body的搜索，然后再搜索到test.com的时候，此时fofa上显示的ip大概率为test.com的真实IP。

3、如果需要对政府网站作为目标，那么在批量获取网站首页的时候，可以用上

http://114.55.181.28/databaseInfo/index

之后可以结合上一步的方法进行进一步的信息收集。

16. SSL/TLS证书查询

SSL/TLS证书通常包含域名、子域名和邮件地址等信息，结合证书中的信息，可以更快速地定位到目标资产，获取到更多目标资产的相关信息。

https://myssl.com/

https://crt.sh

https://censys.io

https://developers.facebook.com/tools/ct/

https://google.com/transparencyreport/https/ct/

SSL证书搜索引擎：

https://certdb.com/domain/github.com

https://crt.sh/?Identity=%.moonsec.com

https://censys.io/

GetDomainsBySSL.py

17. 查找厂商ip段

http://ipwhois.cnnic.net.cn/index.jsp

18. 移动资产收集

18.1. 微信小程序支付宝小程序

现在很多企业都有小程序，可以关注企业的微信公众号或者支付宝小程序，或关注运营相关人员，查看朋友圈，获取小程序。

https://weixin.sogou.com/weixin?type=1&ie=utf8&query=%E6%8B%BC%E5%A4%9A%E5%A4%9A

18.2. app软件搜索

https://www.qimai.cn/

19. 社交信息搜索

QQ群 QQ手机号

微信群

领英

https://www.linkedin.com/

脉脉招聘

boss招聘

20. js敏感文件

https://github.com/m4ll0k/SecretFinder

https://github.com/Threezh1/JSFinder

https://github.com/rtcatc/Packer-Fuzzer

21. github信息泄露监控

https://github.com/0xbug/Hawkeye

https://github.com/MiSecurity/x-patrol

https://github.com/VKSRC/Github-Monitor

22. 防护软件收集

安全防护 云waf、硬件waf、主机防护软件、软waf

23. 社工相关

微信或者QQ 混入内部群，蹲点观测。加客服小姐姐发一些连接。进一步获取敏感信息。测试产品，购买服务器，拿去测试账号和密码。

24. 物理接触

到企业办公层连接wifi，连同内网。丢一些带有后门的usb 开放免费的wifi截取账号和密码。

25. 社工库

在tg找社工机器人 查找密码信息 或本地的社工库查找邮箱或者用户的密码或密文。组合密码在进行猜解登录。

26. 资产收集神器

ARL(Asset Reconnaissance Lighthouse)资产侦察灯塔系统

https://github.com/TophantTechnology/ARL

AssetsHunter

https://github.com/rabbitmask/AssetsHunter

一款用于src资产信息收集的工具

https://github.com/sp4rkw/Reaper

domain_hunter_pro

https://github.com/bit4woo/domain_hunter_pro

LangSrcCurise

https://github.com/shellsec/LangSrcCurise

网段资产

https://github.com/colodoo/midscan

27. 工具

Fuzz字典推荐：https://github.com/TheKingOfDuck/fuzzDicts

BurpCollector(BurpSuite参数收集插件)：https://github.com/TEag1e/BurpCollector

Wfuzz：https://github.com/xmendez/wfuzz

LinkFinder：https://github.com/GerbenJavado/LinkFinder

PoCBox：https://github.com/Acmesec/PoCBox