一、信息收集起点

1、主动收集

主动收集指信息收集过程中与目标系统进行直接交互。可能会被目标网站记录IP，留下数字指纹。

2、被动收集

被动收集指信息收集过程中不与目标系统进行直接交互，通过其他途径获取系统遗留的历史数据和记录，则无须向目标系统发送任何数据包

3、信息收集常见目的

1、目标组织架构基本信息
2、目标邮件服务器与邮件列表信息
3、域名相关信息、子域名
4、IP信息
5、目标网站的技术栈、服务器类型版本、常用建站技术
6、目标网络架构信息、路由器、交换机相关信息
7、目标防御措施信息：防火墙、WAF、IDS、蜜罐、杀软、用户行为审计系统

4、前渗透信息收集基本流程

1、子域名
2、robots.txt
3、crossdomain.xml
4、whois
5、Netcraft
6、IP（是否未云服务器或CND服务商，C段是否有其他网站）
7、WAF
8、Web技术栈架构、Web服务器容器
9、网络路由情况

二、不同目的收集

1、组织架构基本信息

```
# 基本信息
    1、企查查：https://www.qcc.com/
    2、天眼查：https://www.tianyancha.com/
    3、爱企查：https://aiqicha.baidu.com/
```

```
# 常见社交网站
    1、微博：https://weibo.com/
    2、知乎：https://www.zhihu.com/
    3、脉脉：https://maimai.cn/
    4、CSDN：https://www.csdn.net/
    5、Twitter：https://twitter.com/
    6、Facebook：https://www.facebook.com/
    7、Linkedin：https://www.linkedin.com/
```

```
# 常见企业组织架构
    IT  技术支持
    HR  人事
    BD  商务拓展
    PR  公关
    Marketing   市场推广
    内部系统：bi、crm、edm、jenkins、wiki
```

```
# 常见招聘网站
    BOSS直聘：https://www.zhipin.com/
    智联招聘：https://www.zhaopin.com/
```

```
# 查人网站
    1、专家查询：https://cn.aminer.org/
    2、国外信息：
        https://www.beenverified.com/
        https://www.nndb.com/
        https://www.corporationwiki.com/
        https://www.yatedo.com/
```

```
# 邮箱信息
    1、TheHarvester（搜索引擎邮箱记录爬取工具）：
        https://github.com/laramies/theHarvester
    2、Google Groups：
        https://groups.google.com/search?q=%40163.com
```

2、crossdomain.xml

```
# 跨域策略文件
    子域名或敏感信息泄露
```

3、robots.txt

```
# 爬虫文件
    指定网络爬虫允许和禁止爬取的文件，其中可能包括网站内部的敏感文件/目录。
```

4、nslookup

```
# 常见参数
    nslookup -type=ptr 8.8.8.8           # 查询一个IP地址对应的域名
    nslookup -type=ns http://baidu.com  # 查询http://baidu.com使用的DNS服务器名称
    nslookup                            # 进入交互式Shell
    server http://ns2.baidu.com          # Server设定查询使用的DNS服务器
    ls http://baidu.com                  # ls命令列出某个域中的所有域名
```

```
# 获取DNS服务器
    nslookup
    > set type=ns
    > http://baidu.com
```

```
# 获取邮件服务器
    nslookup
    > set type=mx
    > http://baidu.com
```

```
# SPF记录
    SPF全称为Sender Policy Frameword，用于防止别人伪造你来发邮件，当你定义了你的授权地址之后，接收邮件的一方根据定义的SPF记录来确定IP是否包含在SPF里面，包含在内的话就是正常邮件，反之就是伪造的。所以我们可以根据SPF获取到一些目标的IP段。
    nslookup
    > set type=txt
    > http://aliyun.com
```

5、错误页面

```
    Dirsearch：https://github.com/maurosoria/dirsearch
    URL Fuzzer：https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files
    OpenDoor：https://github.com/stanislav-web/OpenDoor
```

6、Google Hacking

```
# 常用搜索
    1、网站开发语言     site:xxx.com inurl:php|asp|aspx|jsp
    2、文件泄露         intitle:index.of
    3、报错信息         error | warning
    4、登录入口         login | logon
    5、用户名           usernaem | userid | employee.ID "your username is"
    6、密码             password | passcode | "your password is" reminder forgotten
    7、管理员           admin | administrator
    8、否定             -ext:html | -ext:htm | -ext:sap | -ext:php
    9、临时文件         inurl:temp | inurl:tmp | inurl:backup | inurl:bak
    10、局域网入口      intranet | help.desk
```

7、Whois反查关联域名

```
    1、爱站Whois：https://whois.aizhan.com/reverse-whois/
    2、站长Whois：http://whois.chinaz.com/
    3、微步在线：https://x.threatbook.cn/
```

8、Netcraft report

```
    https://sitereport.netcraft.com/
```

9、子域名

```
# 方法
    1、子域名枚举
    2、DNS解析记录
    3、搜索引擎
```

```
# 工具
    RapidDNS：https://www.dnsscan.cn/http_code2.html
    网址HTTP标题批量检测：https://www.dnsscan.cn/http_code2.html
```

10、CND

```
# CND检测
    1、17.ce：https://www.17ce.com/
    2、指定区域Ping：https://tools.ipip.net/cdn.php
    3、站长Ping：https://ping.chinaz.com/
    4、全球Ping：https://www.wepcc.com/
```

```
# CND绕过
    1、针对邮件服务器，通过退信或其他邮件，获得邮件服务器真实IP
    2、针对网站命令执行漏洞，直接ipconfig
    3、全球ping
```

11、元数据

```
# MetaGooFil
    如Office文件，其修改记录可暴露大量信息
    https://github.com/opsdisk/metagoofil
```

12、网络路由情况

```
# 路由情况
# Linux
    tracert http://baidu.com
# Windows
    traceroute http://baidu.com
```

```
# 判断有无防火墙
    tracert后，若有缺省的UDP包，即表明被防火墙拦截了。
```

13、开源项目平台敏感信息

```
# 开源平台
    码云：http://code.taobao.org
    Github：https://github.com/
    Coding：https://coding.net/
```

```
# Github信息收集工具
    GitMiner：https://github.com/UnkL4b/GitMiner
    Trufflehog：https://github.com/trufflesecurity/trufflehog
```

```
# .DS_Store文件利用
    https://www.lijiejie.com/ds_store_exp_ds_store_file_disclosure_exploit/
```

14、网络空间搜索引擎

```
    1、Shodan：https://www.shodan.io/
    2、Fofa：https://fofa.info/
    3、360quake：https://quake.360.cn/quake/#/index
    4、Zoomeye：https://www.zoomeye.org/
```

15、指纹识别

```
    1、潮汐：http://finger.tidesec.com/
    2、What CMS：https://whatcms.org/
    3、bugscaner：http://whatweb.bugscaner.com/look/
    4、WhatWeb：https://github.com/urbanadventurer/WhatWeb
```

16、WAF

```
# WAF检测
    wafw00f：https://github.com/EnableSecurity/wafw00f
```

17、社会工程学

```
    1、物理接近。手抱重物，寻求其他人刷门禁
    2、常见冷读技巧。故意提供错误的答案以期望得到纠正
    3、收集目标组织架构信息，伪装成目标组织员工，向IT支持部门申请重置密码
    4、USB摆渡攻击。丢U盘；抽奖送U盘、平板、手机
    5、致电域名服务商客户，修改域名解析
    6、根据收集到的邮箱，批量发送钓鱼邮件，例如系统升级需要员工回复账号密码等
```

三、信息收集报告

1、子域名与域名列表

2、IP列表

3、域名和IP对应关系

4、员工Email列表

5、其他杂项（可选）