漏洞信息收集之——子域名探测

原创

温柔小薛 于 2020-04-10 13:41:51 发布 417 收藏 1
分类专栏： web渗透测试与代码审计 #+ 漏洞信息收集 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43079958/article/details/105431783


web渗透测试与代码审计 同时被 2 个专栏收录

113 篇文章 19 订阅

订阅专栏


#+ 漏洞信息收集

6 篇文章 0 订阅

订阅专栏

子域名探测

什么是 C 段

比如在：127.127.127.4 这个 IP 上面有一个网站 127.4 这个服务器上面有网站
这是一个非常大的站几乎没什么漏洞
但是在他同 C 段
127.127.127.1~127.127.127.255 这 1~255 上面也有服务器而且也有网站并且存在漏洞,那么
我们就可以来渗透 1~255 任何一个站
之后提权来嗅探得到 127.4 这台服务器的密码 甚至
3389 连接的密码后台登录的密码 如果运气好会得到很多的密码

C段不是指C网段，内网地址

k8工具

前提条件记得注册 bing 接口（其实就是查80端口）
输入解析查询
API查询
搜索查询

挖掘机工具

```
提取关键字指定URL地址
```

APP提取

```
下载他提供的APP反编译APP
利用Androidkiller反编译
搜索http或者8080端口等关键字
```

微信公众号

```
可以用Burp APP抓包
 手机和电脑在同一个wifi
  在手机代理设置手动 填写电脑ip地址和端口
   电脑端在burp suite代理服务器
    代理选项添加
     代理截断 本机ip
```

字典枚举法暴力破解获取二级域名

```
DNSReconcile
 Layer 子域名挖掘机
  DirBuster
```

公开DNS源

```
Rapid7 下 Sonar 项目发布的： https://scans.io/study/sonar.fdns_v2。
DNS 历史解析： https://dnsdb.io/zh-cn/
```

威胁情报查询

```
华为安全情报查询 https://isecurity.huawei.com
```