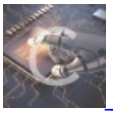
信息收集篇——子域名的探测

转载

小 白 渣 于 2019-11-28 21:01:55 发布 1826 收藏 5
分类专栏： 子域名探测 文章标签： 渗透篇
原文链接：https://blog.csdn.net/chest_/article/details/102605357
版权

子域名探测 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

一. 实验目的

信息收集对于渗透测试前期来说是非常重要的，因为只有掌握了目标网站或目标主机足够多的信息之后，才能更好地对其进行漏洞检测, 当我们要对一个目标进行渗透时，我们往往需要去尽可能的挖掘目标可能存在的攻击面。就拿一个域名来说，当主站防御的比较死的时候，通常就会考虑其子站。因为相对主站而言，子站的安全性做的可能不那么全面,而且dns是目前最主要的服务信息暴露来源，总的来说子域名探测是我们在信息收集中重要的一环，帮助我们扩大渗透测试的范围以及开阔我们视野，所以我们有必要对dns进行详细的子域名探测分析

二. 实验原理

通过收集一个域的信息，能够通过谷歌或者字典文件猜测可能存在的域名，以及对一个网段进行反向查询。它可以查询网站的主机地址信息、域名服务器，由此得到查询出子域名的效果

三. 实验环境

谷歌浏览器
Kali渗透测试平台
网络环境：nat模式

四. 实验过程

一、整站分析

1.检测是否为cdn网站

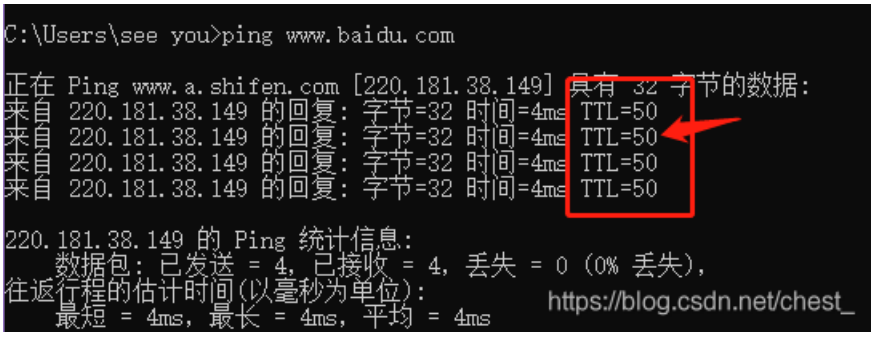
首先，我们要判断该域名是否存在CDN的情况,cmd输入nslookup www.baidu.com检测百度是否使用了cdn

查询出的ip数量大于一个的，说明该ip地址不是真实的服务器地址

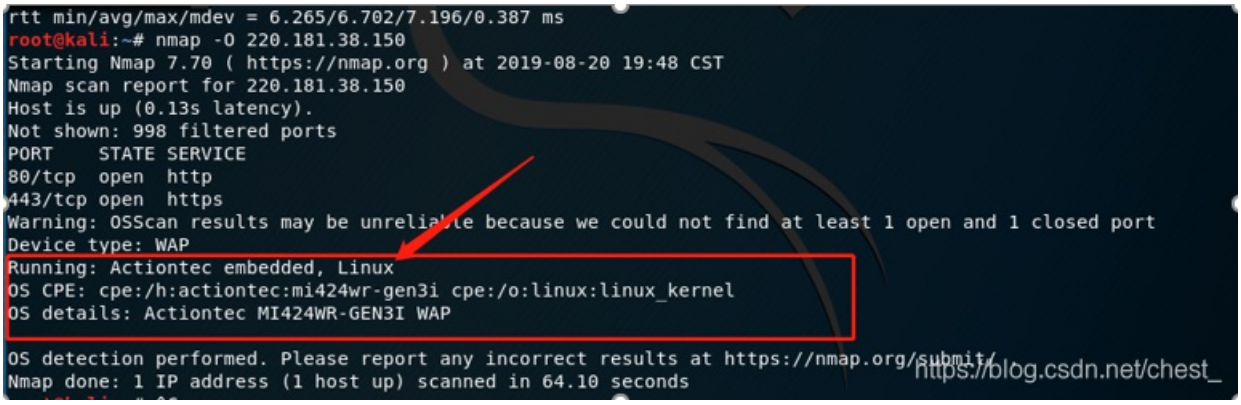
2. 判断服务器类型

先说说ttl, TTL的作用是限制IP数据包在计算机网络中的存在的时间。TTL的最大值是255，TTL的一个推荐值是64。每过一个 路由设备 TTL-1，所以到了本机后得到的TTL值肯定比目标的默认值小

通过ping来探测判断是服务器是Linux还是Windows，Windows的TTL值都是一般是128，Linux则是64。所以大于100的肯定是Windows，而几十的肯定是Linux。



如果要判断目标网站服务器的具体的版本的话，可以采用 nmap 进行扫描， -O 和 -A 参数都能扫描出来，这里采用-O参数 -o是列出操作系统版本



可以清楚的看出，这个服务器的操作系统为linux，具体信息如上

3. 查看web服务器的类型

在Kali终端通过命令whatweb www.baidu.com可以看到该服务器为阿帕奇

分析完毕后，我们就可以进行下一步的子域名探测了

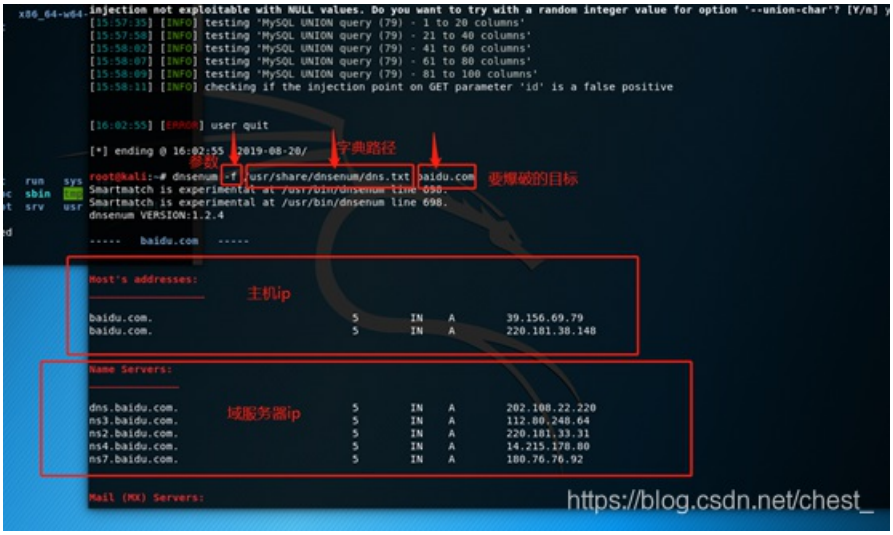
二.子域名探测

一.爆破子域名

搜集完以上信息，我们就可以暴力破解目标域中的子域，一般用dnsenum这个工具来配合字典爆破子域名

终端输入命令:dnsenum -f /usr/share/dnsenum/dns.txt baidu.com

这次用的字典是Kali自带的字典，如果觉得威力不够，爆破失败可以自行去匹配别的字典



爆破后的子域名

服务器的的c段网络

当然也可用其它的子域名爆破工具或者谷歌语法来检索主站下的子域名

如inurl去检索含有baidu.com的URL域名