登录

"安全帮"大型目标渗透 - 01信息搜集

菲哥哥 / 2017-06-04 06:34:59 / 浏览数 21005 安全技术 漏洞分析 顶(1) 踩(0)

---

author：菲哥哥（安全帮）

在入侵渗透一个大型目标网络时我一般分为4个大步骤，信息搜集 - 扫描查点 - 攻击获取权限—清除日志
我看了很多网上的文章或者视频做的都不是太系统。也不太详细。所以我打算做一个系列系统的教程。此次我打算把每个步骤详细的做一次梳理与总结方便想要学习网络安全
公开课QQ群 ：338552043
什么是信息收集

收集目标的情报信息是一个非常重要的环节。可以大大提高渗透测试的成功性。收集渗透目标情报一般是对目标系统的分析，扫描探测，服务查点，查找对方系统IP等，社会
00x1 whois信息搜集

1.WHOIS查点

WHOIS可以理解为是一个可以查询域名注册详细信息的大数据，WHOIS中包含域名注册者的姓名,邮箱 ,电话,地址,dns服务器
等信息这些对我们渗透目标都很有用，然后在通过whois获取到的注册者和邮箱进行域名反差可以获取更多的信息。
以"douban,com"为例 liunx下用 whois http://douban.com 可以看到详细的 邮箱，注册人 等注册信息。

也可以通过相关网站进行whois查询如：
https://www.whois.com/whois/douban.com

2.whois反查

可根据whois获取到的 域名所有人、域名注册商、域名注册日期和过期日期等
,使用邮箱，电话等进行反差获取更多关联的域名等信息,方便我们扩大目标范围。可在 域名Whois反查 - 站长之家进行反向查询

以上获取的信息在进行社工的时候很有用。

00x2 DNS查点
DNS的作用就是把主机映射为ip地址，或者是把ip地址映射为主机名的分布式数据库.。

1. nslookup 命令基础参数解析
   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设定查询将要使用的DNS服务器

ls http://baidu.com #ls命令列出某个域中的所有域名
MX记录 电子邮件交换记录，记录一个邮件域名对应的IP地址，比如my[at]http://seclines.com
后面的部分seclinescom，邮件服务器对应的IP地址
NS记录 域名服务器记录 ,记录该域名由哪台域名服务器解析
PTR记录 反向记录，也即从IP地址到域名的一条记录
TXT记录 记录域名的相关文本信息

1. nslookup获取DNS服务器

以http://thaicatgo.com为例使用

localhost:~ root# nslookup //执行nslooup命令
> set type=ns //设置查询类型
> http://thaicargo.com //设置要查询的网站
Server: 202.106.195.68Non-authoritative answer:
http://thaicargo.com nameserver = ns-1708.awsdns-21.co.uk. //dns服务器
http://thaicargo.com nameserver = ns-1015.awsdns-62.net.
http://thaicargo.com nameserver = ns-75.awsdns-09.com.
http://thaicargo.com nameserver = ns-1306.awsdns-35.org.

3.获取邮件服务器

邮件服务器大都是在防火墙所在的系统，就算不是和防火墙在同一个系统最起码和目标网络也在同一个网络中。我们可以使用nslookup和host命令来获取邮件服务器地址。
nslookup命令

root# nslookup
> set type=mx //设置要查询的类型
> http://thaicargo.com //设置目标网站

Server: 202.106.195.68
Address: 202.106.195.68#53
Non-authoritative answer:
http://thaicargo.com mail exchanger = 10 http://mx1-us1.ppe-hosted.com //对应的邮箱服务器.
http://thaicargo.com mail exchanger = 10 http://mx2-us1.ppe-hosted.com //对应的邮箱服务器.

host命令
host http://thaicargo.com

00x3 网络侦察

网络侦查用到windows下tracert命令，liunx下traceroute命令追踪路由查看整个网络的拓扑用windows来实例演示下。

C:\>tracert http://seclines.com
Tracert to http://seclines.com (10.10.10.1),30 hops max,40byte packets
1 gate2 (192.168.10.1) 5.391ms 5.107ms 5.559ms
2 http://rtr1.bigisp.net (10.10.12.13) 33.374ms 33.443ms 33.137ms
3 http://rtr2.bigisp.net (10.10.12.14) 35.100ms 34.427ms 34.813ms
4 http://hssitrt.bigisp.net (10.11.31.14) 43.030ms 43.941ms 43.244ms
5 http://seclines.com(10.10.10.1) 43.803ms 44.041ms 47.835ms

看命令执行结果数据到达目标需要经过5跳才能到达，中间没有UDP分组的丢失，而到达目标之前的第四跳很可能是主机http://seclines.com的边界路由设备，也有可能是
如果存在防火墙又怎么知道呢？下面还是用一个例子说明吧：

C:\>tracert 10.10.13.5
Tracert to (10.10.13.5),30 hops max,40byte packets
1 xss2(192.168.10.1) 5.391ms 5.107ms 5.559ms
2 http://r1.net (10.10.13.13) 33.374ms 33.443ms 33.137ms
3 http://r2.net (10.10.13.14) 35.100ms 34.427ms 34.813ms
4 http://sss.wome.net (10.11.31.14) 43.030ms 43.941ms 43.244ms
5
6
可以看出，缺省的5，6跳 UDP数据包被防火墙拦截了。
00x4.二级域名

大型目标域名收集

1、二级/子域名收集

比如：http://mail.example.com和http://calendar.example.com是二级域http://example.com的两个子域，而http://example.com则是顶级域com的子域

1.1 域传送漏洞
使用域传送漏洞可快速查询目标服务器上的所有域名
dig命令
假设http://test.com的DNS服务器为192.168.5.6，
使用dig
@192.168.5.6 http://test.com axfr即可如果目标存在域传送漏洞的话就可查看所有域名了.

nmap检测传送漏洞

nmap --script dns-zone-transfer --script-args dns-zone-transfer.domain=http://test.com -p 53 -Pn 192.168.5.6

域名爆破

我常用的两个工具

fierce -dns http://test.com
python subDomainsBrute.py http://test.com //可以递归爆破三级四级域名

2、关联域名收集（在whois中已经有说明）

关联域名是指同一个邮箱所注册的所有域名。 但是收集到的关联域名不一定就是同一个企业的域名，但是可能性很高。
域名Whois反查 - 站长之家 可完成关联域名反查。

3.corrs.xml文件

corrs.xml文件作用是设置对主域名flash文件访问权限控制，文件里面会记录主域名下的子域名。

3.IP地址旁注

根据获取到的目标ip地址反向查询，获取ip地址上所有域名我常用的又以下两个
Find websites hosted on the same ip

ip:31.220.110.42 - 必应

4.googlehack

1.使用site:.http://test.com 来匹配所有的子域名 ,获取到子域名http://admin.test.com
2.然后在用site:.http://test.com -admin
在查询结果中去除掉admin域的记录，反复使用 - 参数查询可获取大量域名，已有开源程序theHarvester.py可以做到自动搜集。引擎除了Google之外还有bing、shodan、
钟馗之眼等等，

1. spider

Spider信息除了利用公开的搜索引擎之外，也可以自己写爬虫爬目标企业的网站，遇到其子域名继续爬下去。这样可以收集到所有该网站上有链接过去的子域名（和搜索引

00x6.IP范围

1.ip比较法

比较大型的目标会有比较多IP地址，大型目标网络ip地址通常分配在一个C段或多个c段中。
例目标顶级域名为http://www.seclines.com 其IP地址为222.222.222.222 ，bbs.seclines.com 其ip为222.222.222.223 wiki.seclines.con
其ip为222.222.222.224由此可以推测222.222.222.1-255的IP地址都为该公司IP地址，但最后的确定还要根据其他的信息进行判断

2.http头

有些服务器维护人员喜欢打上自己的标签，例如特殊的HTTP头。 我们可以通过shodan或钟馗之眼 来进行搜索拥有同样标签的服务器。

- - - 根据ip查询as号

3.AS号查询IP地址范围

自治系统号码自治系统：autonomous
system。在互联网中，一个自治系统(AS)是一个有权自主地决定在本系统中应采用何种路由协议的小型单位。这个网络单位可以是一个简单的网络也可以是一个由一个或多
domain）。一个自治系统将会分配一个全局的唯一的16位号码，有时我们把这个号码叫做自治系统号（ASN）。利用AS号来寻找IP的方式

$ dig +short 32.http://152.112.17.origin.asn.shadowserver.org TXT
dig +short 117.http://122.213.158.peer.asn.shadowserver.org TXT //根据ip查询as号
whois -h http://whois.cymru.com 117.122.213.158 //根据ip查询as号
whois -h http://asn.shadowserver.org prefix 8075 //根基as查询ip段

关于 AS/ASN 号查询ip范围参考文档
AS号码查询,ASN查询, Autonomous System Number (ASN) 查询, BGP查询,网络路由查询
Shadowserver Foundation - Services - IP-BGP
通过IP和AS自治系统号判断数据中心是几线BGP接入-数据中心-华为企业互动社区
【转】网络中的AS自治域 - myLittleGarden - 博客园
Shadowserver Foundation - Services - IP-BGP

- - - 根据as号查询ip 红色条目是没生效ip

AS Report

4.spf记录获取ip地址

spf全称为Sender Policy Framework，它的作用是防止别人伪造你来发邮件，反伪造性邮件的解决方案.当你定义了你的domain
name也就是授权的地址。（域名txt记录也就是spf记录））之后，接收邮件的一方根据定义的spf记录来确定ip地址受否包含在spf里面，包含在内的话就是正常邮件反之就是
localhost:~ root# nslookup
> set type=txt
> http://aliyun.com

00x7. cdn真实ip地址

tools有个帖子写的很详细了我就 不啰嗦了地址如下
绕过CDN查找网站真实IP方法收集 - 无法自拔 - 博客园 http://www.cnblogs.com/jsq16/p/5948849.html

00x8. 信息泄漏

1.员工信息搜集

通过社交网站发现一些心怀不满的员工,和前雇员，这些人是一个不错的切入点通过这些不满的员工获取重要的信息还是比较靠谱的。以及关注高管或者网络管理员的社交账

- - 社交网站

http://twitter.com
http://facebook.com
myspace .com

http://reunion.com
http://sina.com
http://instagram.com

通过求职网站查询现在就职或者曾经就职的员工进行,信息搜集。

- - 求职网站

http://linkedin.com
http://plaxo.com

可以通过查人网站查询一些详细的个人信息资料，这些网站可以查询到，家庭电话号码，家庭地址，社会保障号，信用记录等。掌握这些信息对apt攻击很有用。

- - 查人网站
AMiner
Background Checks & Public Records
Tracking the entire world
Corporation Wiki - Find Connections between People and Companies
Free People Search

2.邮箱搜集

邮箱也可在求职网站进行搜集，但是似乎http://groups.googole.com更好用一些，我经常用比如搜索泰国航空后缀的邮箱 @http://thaiairways.com
可以查看到一些历史邮件内容。网站如下。

https://groups.google.com/forum/#!search/@thaiairways.com$20
从邮箱服务器获取信息

在渗透中通过直接与邮件服务器进行交互来获取更多信息，我们可以试探性的给目标发送一封空的邮件，或者是发送0kb的文件，或者是非恶意文件，比如计算器等正常杀软是什么，杀软版本号，电子邮件服务的型号品牌，服务器ip，软件版本，这些信息在漏洞利用的时候是很有用的。

3.代码泄漏

http://github.com
http://code.google.com
码云 - 开源中国代码托管平台

在以上3个站中搜索目标关键字由于开发人员的疏忽导致代码或者敏感信息泄漏参看如下实例
github-hacker之TCL一万五千多名员工信息泄漏（git泄密新场景） | WooYun-2015-141726 | WooYun.org
咕咚网github信息泄露 | WooYun-2016-177720 | WooYun.org

4.组建密码字典

通过以上步骤搜集到的信息 如 电话号码,邮箱id,用户id等信息组成字典，遇到登录的地方进行暴力破解

关于信息搜集就先写这些。下一节是扫描查点。

上一篇：《阿里巴巴Java开发手册v1.2.0》 下一篇：Fucking勒索软件分析
1. 16 条回复


菠菜 2017-06-04 09:50:37

厉害了，我的菲哥，就服你。。

0 回复Ta


hades 2017-06-04 12:04:23

哈哈 竟然菠菜哥也来了

0 回复Ta


hades 2017-06-05 04:49:33

可以把相关地址整理一个URL列表

0 回复Ta


simeon 2017-06-05 13:16:09

我觉得应该有一个总结的文档像checklist更好。便于渗透时使用。

0 回复Ta


hades 2017-06-05 14:31:44

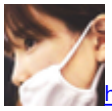
有的

0 回复Ta


0sec 2017-06-06 03:59:53

参考;黑客大曝光第7版

0 回复Ta


hades 2017-06-06 05:13:47

哈哈 现在这样内容基本还和n年前的变化不大

0 回复Ta


hades 2017-06-12 02:18:32

菲哥多来捧场

0 回复Ta


bistoury 2017-06-21 07:46:12

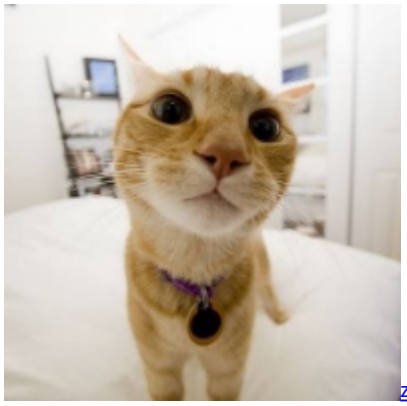
文章写得比较全面，也写了目前仅有的一些方法，但是针对国内现状，一般是直接针对网站本身进行攻击和渗透，很少有人重视信息收集这块。

0 回复Ta


hades 2017-06-21 13:41:02

看来信息收集的那个图我要上传上来了

0 回复Ta


ze7o 2017-06-22 04:25:28

快传

0 回复Ta


asdpppp 2017-06-26 08:26:04

期待后面的文章

0 回复Ta


菲哥哥 2017-08-02 12:50:07

就但说as号获取 ip段这个 我觉得很少有人去深入研究，，现在的白帽子都被src搞晕了头脑，净是挖些逻辑漏洞 你让他全面的搞个大目标 绝对歇菜

0 回复Ta


超神哥123 2017-08-07 01:16:20

get收藏了

0 回复Ta


超神哥123 2017-08-08 02:20:23

复现了一遍这信息收集真累

0 回复Ta


超神哥123 2017-08-08 02:20:45

说的没错

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板