安全小课堂第四十五期【域名爆破的原理与工具】

京东安全应急响应应中心 2017-02-17

域名爆破的原理与工具

对网站进行安全检测的过程中域名爆破不仅能帮助发现无法搜索到的域名，还能收集到通过探测目录是不能够探测到后台，能大大提高渗透的成功率。 本期安全小课堂JSRC邀请到了讲师Chora师傅的分享关于域名爆破的专业知识。感谢Chora师傅的分享，以及 JSRC 白帽子iDear ， 王松_Striker ， 苦逼司马，恋锋，齐迹，胖猴粉、Stu、沦沦的讨论。

Chora：JSRC核心白帽子，MS509团队核心成员，跨平台版中国菜刀Cknife作者；
8年网络安全研究经验，擅长渗透测试、代码审计以及安全开发；
仅用一周时间进入2016年JSRC年度白帽子排名前十，曾获得JSRC月度第一白帽子。

京安小妹

Chora师傅能讲一讲对网站进行安全检测前一般需要收集什么信息吗?

Chora 

要收集的信息有很多，只要与之相关的我都会进行保存，比如域名、IP地址、邮箱等等。

主要会获取一些Banner比如状态码，Server头，标题，以及开放的端口等。

今天小课堂的主题域名爆破就是收集域名的一种方式。

京安小妹

Chora师傅能讲一讲域名爆破的重要性吗?

Chora 

1、域名爆破能够发现一些在公开信息里搜索不到的域名

1、域名爆破能够发现一些在公开信息里搜索不到的域名；

2、有的域名可能直接绑定的内网地址，有利于黑盒模拟内网环境。

3、还有一点就是很多大型网站的后台都是使用二级、三级域名，不会在目录下，

比如某小型网站http://www.xx.com/，的后台是www.xx.dom/aa/houtai，后台被映射到一个二级或者三级域名下，通过探测目录是不能够探测到后台的，就需要域名爆破来发现。

所以通过爆破获取到的域名更能够找到一些后台，也就是说更容易渗透成功

京安小妹

域名爆破的原理是什么呢?

Chora 

爆破的原理其实是通过**枚举**的方式来实现的（爆破域名顾名思义就是枚举的意思）枚举域名的A记录.

比如要爆破xx.com的子域名，

首先的访问一个随机并不存在的域chorashuai.xx.com，

取得A记录后保存，

然后开始枚举a-z0-9，比如1.xx.com、 2.xx.com 、3.xx.com之类的。接下来的步骤就分为两种方式了。

其中一种：直接获取1.xx.com 2.xx.com 3.xx.com的A记录，有A记录则表示存在也是可行的，但是如果遇到泛解析则该方法失效。

另一种，在泛解析的下也可以使用，把这些枚举的域名A记录与之前chorashishuaige.xx.com的A记录做对比，不同的则是存在A记录的域名，也就是在用的域名。

京安小妹

关于域名爆破Chora师傅有什么工具推荐么?

Chora 

推荐两款工具，估计大家都使用过：

- subDomainsBrute
- layer子域名挖掘

京安小妹

这两款工具各有什么优缺点

Chora 

以前我对这两个工具也有做过简单的对比，就是个人在使用上的一些对比吧，优点有很多，不能说有缺点，我只能说对我个人而言有一些麻烦的问题，或者说不足，都是个人的观点不代表对这两个作者本身的不敬。

subDomainsBrute

优点：跨平台，循环遍历，支持自定义规则

以前有对比过subDomainsBrute以及layer发现前者比后者会少几个结果，但是不知道现在情况如何。

少几个结果是指同样的线程，同样的字典，结果会有少几个，不知道现在有没有完善在。

layer子域名挖掘

优点：结果比较准确

但是不是跨平台的，有时候只有mac环境或者kali环境下就不能使用，也不能循环遍历。

另外这两个工具都有一个使用问题，个人使用问题

大家都知道枚举的时候，可能会造成网络不畅通，打开缓慢甚至打不开的情况。

我以前在做众测的时候，发现了某一个域名可能有问题就想先看一看，但是要打开需要先关掉爆破工具，但是关闭爆破工具后又得重新爆破了。如果不关闭呢，要等爆破完，奶粉钱已经被抢光。

并且再好的网络大量枚举会造成网络卡顿的，这个后面我会说到为什么会有长时间的大量循环枚举。

于是后来我自己写了一个工具，跨平台，可指定层次循环爆破，速度快，可暂停（暂停只是一个小功能，循环爆破才是最重要的。）

京安小妹

循环爆破是什么意思呢？能讲得详细一些么？

Chora

先爆破xx.com，发现了a.xx.com，出来的结果，再进行一次爆破，继续爆破

b.a.xx.com，然后c.b.xx.com，一直循环到没有域名位置，这样能爆破出深度的域名。

比如一个6级域名，

先爆破出了house.xx.com；

然后爆破出了db.house.xx.com；

然后爆破出了esf.db.house.xx.com以此类推到第6级。

不过当到爆破达一定量过后就会卡顿，所以暂停功能也是必须的。

京安小妹

对于互联网企业，有什么措施可以防止域名被爆破么？

Chora

这个问题我不能说有绝对的防御，通过使用DNS轮询+泛解析给探测域名的黑客们制造一些小的麻烦还是可以的。

昨天群里的齐迹（猪八戒网安全负责人）说到了泛解析，但其实也不能解决域名爆破的问题的，第三个问题讲到的通过对比就能排出掉了，

DNS轮询+泛解析应该能防住layer跟subdomainbrute，

但是改一下程序就可以绕过了，其实作用不太大的。

京安小妹

Chora师傅还有其他什么需要补充么？

Chora

有两个小技巧想跟大家分享下，不知道大家有没有发现过或者正在使用：

第一个，大家有可能已经正在使用了，就是爆破4位。一般都是1-3位，很多朋友遗漏了4位，5位由于数量太大基本不可能实现；

第二个是已经集成到我工具里的一个小技巧，比如有些大型厂商喜欢mxxx.bb.com、adxxx.bb.com会有前缀或者后缀bb-o2o.bb.com这个时候就可以自己写一个工具替换xxx来进行爆破。

我工具的格式如下m{fuzz}.XX.com，就是要在哪个位置爆破就插入{fuzz}，这样也能发现一个隐藏的域名。

白帽子提问：暴力破解的破解量是不是太大了？

Chora师傅：会很大，但爆破可以通过枚举0-9a-z，也可以枚举字典里的常用单词，一般我会结合起来。

白帽子观点：关于枚举造成网络卡顿的问题，在服务器上进行爆破可以解决。

Chora师傅：如果一直爆破就算服务器再好也会断网。

白帽子提问：关于枚举造成网络卡顿的问题，在路由上给爆破的IP限速能？

Chora师傅：枚举不是网速，他是大量的dns请求会造成路由器问题，所以限速没用。

白帽子提问：收集域名有啥姿势分享不，某些公司多个主域这样的情况。

Chora师傅：多个主域也还是得一个域一个域的收集，最多能够自动化一下节约时间。

白帽子提问：域名搞到IP咋搞比较好，有些CDN或者反向代理，把真实IP都藏起来了。

Chora师傅：这些其实网上都有方法，我也是使用那些公布的方法没有什么特殊的，唯一特殊的就是我把方法总结成工具，方便解决时间，不遗漏目标

最后，**小课堂持续征集讲师**，只要你在网络安全领域对有所擅长、有自己的见解、或者只是纯粹想跟大家分享个0day，都欢迎自荐成为安全小课堂讲师。

作为安全小课堂的讲师，不仅能享受分享知识的成就感与荣誉，而且通过与大家的讨论也有利于自己对知识进行梳理，完善自己的知识体系。当然，JSRC的日常福利是少不了

的。

如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，查阅请直接回复“安全小课堂”或点击阅读原文查看查询方式。

微信公众号：jsrc_team
新浪官方微博：京东安全应急响应中心

阅读原文