【渗透技巧】搜集SRC信息中的"技术活儿"

aerfa / 2017-12-21 15:00:00 / 浏览数 3932 安全技术 技术讨论 顶(0) 踩(0)

生活的艺术，就是艺术的生活；
挖洞的思路，就是思考着挖洞。

各路SRC的迅速崛起，无疑给广大白帽子带来了福音与福利。展露拳脚，占据排行，赚零花钱，获得认可，节日礼物，与小姐姐聊天.....可谓干劲十足，即使拖着疲倦的身躯

信息收集是伊始，个人觉得也是重中之重。

0x01 常规操作--官方域名

基本上SRC都会提供相关域名，常以 *.xx.oo 形式告诉一级域名。

0x02 常规操作--域名加工

根据主域名，可以获取二级域名、三级域名、.....主要姿势可以有：

其中不得不称赞：
【1】DNS域传送漏洞
如果存在，不仅能搜集子域名，还能轻松找到一枚洞，这样子的好事百试不厌。如果SRC一级域名不多，直接在kali下 dnsenum xx.oo
，如果一级域名很多，写个py调用dnseum或dig也是轻松+愉快。

【2】备案号查询
这算是奇招吧，通过查询系统域名备案号，再反查备案号相关的域名，收获颇丰。

【3】SSL证书
通过查询SSL证书，获取的域名存活率很高，这应该也是不错的思路。

【4】google搜索C段
这招用的比较少，国内没条件的就用bing或百度吧（国内站点足矣），在没什么进展的时候或许会有意外惊喜。

【5】APP提取
根据SRC的APP，进行提取（相关工具可以看看Seay的博客），此外在APP上挖洞的时候，可以发现前面招式找不到的域名。

【6】微信公众号
企业的另一通道，渗透相关公众号，绝对会有意外收获：不少漏洞+域名，这里面有不少技巧，打算在后续写公众号分享。

【7】其他的比较普遍，就不再介绍。

0x03 常规操作--IP网段

有了庞大的域名，接下来就是帮助SRC梳理资产了。
域名可以先判断存活，活着的继续进行确定IP环节。根据IP的分布，确定企业的公网网段。这其实是一项不小的工程，精准度比较难以拿捏。不过通过不断实战，肯定可以琢
东西，所以有人称白帽子可能会比企业的运维更了解资产信息。

0x04 常规操作--指纹识别

在这个过程中，可以加入端口扫描、敏感文件扫描之类的操作。
具体的"神器"，我也没有自己习惯哪一款就用哪一款，没有喜欢的就自学自造，只要保证用起来不习惯或者想偷懒又或者不顺手了，就主动一点吧。如果把上一篇公众号文章

0x05 常规操作？--历史漏洞

现在可以从wooyun镜像站点搜索相关漏洞。
仔细分析，大胆验证，发散思维，对企业的运维、开发习惯了解绝对是有很大的帮助。可以把漏洞保存下来，进行统计，甚至炫一点可以做成词云展示给自己看，看着看着或

0x06 常规操作？--敏感信息

之前在归纳梳理漏洞的时候，稍微根据自己的习惯总结了信息泄露类，涉及的很不全，这里想偷懒一下贴出之前的图：

最想强调的是github信息泄露了，直接去github上搜索，收获往往是大于付出。可能有人不自信认为没能力去SRC挖洞，可是肯定不敢说不会上网不会搜索。github相关的
github.com、rubygems.org...
pan.baidu.com...
QQ群备注或介绍....甚至混入企业qq工作群...

【渗透技巧】搜集SRC信息中的"技术活儿".rar (1.436 MB) 下载附件

上一篇：Java序列化和反序列化 下一篇：【JSP代码审计】某商城几处漏洞审计分析

1. 8 条回复

 hades 2017-12-21 15:01:12

@aerfa 我能说是你不会用么 哇哈哈 我来 (□•□□•□)□□

0 回复Ta

 aerfa 2017-12-21 15:15:37

@hades 尴尬.jpg

0 回复Ta

 AAAAAAAAAA 2017-12-25 10:43:52

【2】备案号查询
这算是奇招吧，通过查询系统域名备案号，再反查备案号相关的域名，收获颇丰。

【3】SSL证书
通过查询SSL证书，获取的域名存活率很高，这应该也是不错的思路。

这两招学习了。

0 回复Ta


bywalks 2017-12-25 20:58:24

点赞.jpg

0 回复Ta


独自等待 2017-12-26 20:06:47

写的很不错。

0 回复Ta


xman21 2017-12-27 20:33:19

good

0 回复Ta


hack**** 2017-12-28 13:33:38

可以 一看就是个src老手啊

0 回复Ta


aerfa 2018-01-08 11:12:05

@hack** 在线小菜，不值一提

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