登录

【独家】我的企业安全推动

泳少 / 2017-03-09 06:07:00 / 浏览数 8180 安全技术 技术讨论 顶(0) 踩(0)

0x00前言

先简单说说吧，来了某公司一段时间了，做了很多事也让我成长的很快。但是在公司安全似乎不太被重视，却又不知道如何慢慢建立起来。本文主要阐述的是把小事情做好了

0x01借鉴

之前ysrc在github上发布过"巡风"这么一套系统：https://github.com/ysrc/xunfeng
里面有详细讲解了搭建的方法，大家可以去看一下。然后这段时间一直忙于搭建，调试等，现在算是搭建好可以使用了

首先使用这套系统的目的是想更清晰的对内部办公网络、及内部服务器的资产管理，想先从内部出发再慢慢延伸到线上(当然了。线上现在采用了第三方厂商的一套系统所以

一些没有密码就能访问到的服务

当然了还有很多，这里就不一一列举了

巡风这套系统确实很实用，闲了的时候可以自己写写PoC然后让它定期去进行检测，后期如果时间允许的情况下可能会把UI这一块修改，为了让自己看的更舒服(zhuangbilit

其实不仅限于巡风这一套系统，在github上寻找一些有关资产管理的系统，从中学习该系统的优点，把它们完善与结合在一起。比如https://github.com/Cryin/AssetsView

[redacted](Echarts[redacted]

它的好处就是覆盖了网路拓扑图一目了然，也可以看到ip、主机名、操作系统、mac地址等

前段时间在FreeBuf上有大牛发布过：一个人的"安全部文章，http://www.freebuf.com/articles/security-management/126254.html

对于他做的一个总结在这里想引用一下

1. [redacted]
2. [redacted]
3. [redacted]/[redacted]
4. [redacted]IP,[redacted]XX[redacted]
5. [redacted]
6. [redacted]

其实就我目前而言，公司上的程序猿上报bug还是很乐意修复它的，当然我的leader对安全也比较关注，只是她不太懂，现在全靠一个人支撑着内部的安全测试，测试通过了

隐隐约约记得webqq上是可以实施监控的，由于码代码还不是我擅长的一块。只能每天人工打开qq去阅览一遍，看下存在什么样的风险及时上报于公司

最近也在看一些关于企业内部安全的事情，看到了专业种田大牛在公众号上写的这么一文：

我觉得即使公司不注重安全但是他既然让你来上班，自己就应该做好分内事，没有时间或者说不会码代码可以善用开源，然后自己再删删改改就可以了

0x03 推动

内部安全要如何推动？这相信难倒很多人，其实啊，技术很难做到位的，但可以给他们定制一份安全策略，比如"web安全验收参考文档"

让开发人员按照这个标准去进行开发，如果再检测安全时候发现上述安全问题那么就让他进行一些小惩罚，既可以减少彼此之间的工作量，又可以让自己舒心，何乐而不为~

还有的就是定期进行内部的安全培训，小到信息泄露讲解，大到对企业模拟一两次大规模的黑客攻击(包括但不限于钓鱼、APT等)当然了这种做好最好先给自己领导报备了让

另外，一律禁止员工在办公网络分享WiFi网络，以免被外界进行物理渗透从而进入内网。

目前所做的一些事情：保垒机(作用于员工操作服务器的时候监控操作命令以及各种应用和服务器的视频录制，不通过堡垒机跳板无法连接服务器)、上线前的安全测试、安全

打算日后等新人员到岗后可能做的事情就是要做扫描器的开发功能点包括但不限于（服务弱口令、SQL注入、域名暴破与监控、XSS漏洞扫描、url爬虫、开源CMS漏洞扫描、

0x04 总结

其实我更应该感谢现公司能让我一个人做那么多事情，以前总觉得挖漏洞是一件让人兴奋的事情，而到了现在更希望维护好企业的安全。懂攻击不懂防御万一哪天把自己公司

在攻防两端对立之间，在甲方做过后，就知道了乙方所谓有多屌多屌的技术和产品，也只是解决某些问题。有些时候是需要外力帮忙的，甲方自身安全人员也不一定能推得动

另外大家也可以参考一些文章及书籍：

http://www.freebuf.com/articles/security-management/126643.html

http://www.freebuf.com/special/127172.html

http://www.freebuf.com/special/127264.html

http://www.freebuf.com/articles/neopoints/127508.html

书籍：《互联网企业安全高级指南》

相信以上这些可以帮助你点什么，一起加油吧~

上一篇：NTFS 3g本地提权漏洞—【CV... 下一篇：如何优雅的把LFI转化为RCE（2...

1. 12 条回复


xiaopigfly 2017-03-09 06:35:23

顶一个。希望日后做出成果了可以写的更加细腻。lz加油

0 回复Ta


沦沦 2017-03-09 06:38:41

666666

0 回复Ta


hades 2017-03-09 06:52:25

互联网企业安全高级指南 有点偏方法框架 ，有人已经在整理落地的东西

0 回复Ta

 紫霞仙子 2017-03-09 10:00:09

还是很支持我泳！

0 回复Ta

 泳少 2017-03-10 01:23:19

谢谢我霞

0 回复Ta

 泳少 2017-03-27 10:00:42

..

0 回复Ta

cryin 2017-03-29 09:49:37

支持 ~~，尽然看到我的项目AssetsView了。。惭愧，当初的想法是写一个资产发现 管理
集成系统、web漏洞扫描一体的东西，，但是太庞，需要投入的时间也很多，所以都好久没再继续开发了。。不得不说巡风真的很不错，而且已经相对成熟的东西。这种

0 回复Ta

cryin 2017-03-29 09:59:45

引用第7楼cryin于2017-03-29 17:49发表的 ：
支持 ~~，尽然看到我的项目AssetsView了。。惭愧，当初的想法是写一个资产发现 管理
集成系统、web漏洞扫描一体的东西，，但是太庞，需要投入的时间也很多，所以都好久没再继续开发了。。不得不说巡风真的很不错，而且已经相对成熟的东西。这种
[url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=793&pid=1850][/url]

这个想法源自国外安全公司qualys.com的Qualys AssetView
https://www.qualys.com/suite/assetview/

如果有机会可以看下，很不错的资产管理系统

0 回复Ta


mefortune 2017-03-31 03:27:39

膜拜表哥，我搭建了好几次都没成功，问一下assetsview运行的环境是什么，我的是apache2.4.9,mysql5.6,php5.5

0 回复Ta


冰点 2017-04-01 07:33:07

表哥，好几个图都看不了，不知道是不是我的问题

0 回复Ta


hades 2017-04-01 15:58:14

图是挂了 ，最近他太忙了，回家补工作在，晚点更新图

0 回复Ta

泳少 2017-04-05 01:56:33

已知晓。。。先知的图不知道为啥丢失了~~

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