17总结碎碎念

原创

Neil-Yale 于 2018-02-16 11:25:38 发布

今天是正月初一，本来这篇总结是想除夕写的，结果昨天晚上看春晚去了。

大概是16年6月份左右开始接触安全的，那时候学校也是第一次组织信息安全类的比赛，组队参加全国大学生信息安全竞赛，那时候我才大一，由于班主任的原因，得以和大佬们一起划划水。也是那时候开始认识drop,hook,老锥三位大佬的，还有晓生学长，不过很少接触。虽然身边有大佬，碰到问题基本上也都靠google，怕问大佬们太丢脸了。在精灵师傅的群里，不对，现在是pcat师傅的群了，也见识了其他师傅的厉害，基本上都是同辈吧，也就差个两三岁的样子，真是厉害，印象比较深刻的有pcat,精灵,phith0n,muhe,柠檬，苹果，swing等师傅，看了他们写的很多东西，真的觉得自己实在弱。对了，还有厦大的一位大佬，chybeta，整理了两个repo，分别是软件安全、web安全方向的，都是精华，在github上。最近在逛看雪的时候还看到了muhe师傅16年入门时候的足迹呢，好像在问看得懂每一句汇编，但是合在一起就看不懂怎么办的问题。。现在muhe师傅都在写fuzzer,调试内核了，真的强。在bilibilli上，也看到muhe师傅了，在学编译原理。感觉真的厉害。

身边的大佬们的去向，晓生学长好像去了不可描述的地方，drop去了四叶草，hook去了万网，老锥保了西电网信院的院长的研究生。都很厉害，在回到我自己，实在是太水了。很羡慕前面提到的三位师傅，可以一起分工配合打比赛，到了我这届，就我一个人了，本来还有一个的，结果跑去创业了。学弟们也实在对安全不上心，技术也没怎么样。没有队友，要想能够打比赛拿到好名次，所以当初心太大了，想着能够成为全栈，Mobile sec,pwn,web,misc,crypto,reverse全精通，然后一个人吊打全队，就像偶像汪神一样，汪神当年在国赛初赛上一人吊打几百只队伍，实在是佩服。在ichunqiu上看了他给xman做的培训，感觉他的理论非常扎实，实在是大神。不像现在圈子里很多浮躁的人，只是script kiddo，还有好多工具都不会用的。。。sqlmap里tamper都不会，，，提交的漏洞全是php id=1'跑个sqlmap出来的，，，没针对谁，举个例子而已。

我目前为止自认为学习安全最执着的时候是在我大二下学期，那时候我一直在实验吧刷题，还看了linux内核源码剖析，实在是不知天高地厚，哈哈，确实是看不懂，但还是硬着头皮读完了。那时候安全也是风口上的猪，当然现在应该也还是，我也很肤浅、浮躁，甚至想着退学，就专门搞安全了，因为那时候觉得我安全完全靠自学，专业课教的我以后都用不到，而且老师也差劲，干嘛用花费时间在课堂上。然后我就把这样的想法和好几位任课老师说了，他们也允许我不去上课。那个学期我java,算法与数据结构，英语，计算机网络都没去上，当时我自学得都挺好的呀，结果期末给成绩的时候，给的都是60，70.。。。。。把我保研的理想给打破了。。本来我还是有希望保研的，结果这么一来，，，委屈。

所以，后来就陷入了考研还是工作的焦虑困境中，到现在，我还是决定考研了。考哪？这种立flag的事情当然不能公开说了啦~~所以呢，今年（18）基本上是不会在安全方面有太多投入了。

目标院校的一门业务科考的是密码学，，我的天，大部分院校考的都是计算机综合的，这不按常理出牌啊，本来还行借助考研复习的时候，重新梳理一遍计算机专业的全部框架、体系结构，现在看来，得去搞密码学了。

做安全一入门就会知道了，实在是计算机行业的集大成者，搞web人家给你个拓扑，你不会计算机网络能行吗，有个sql你不会数据库能行？搞逆向，不会C，不会汇编，不会算法，不会数据结构？

搞安全的就是互联网的保安，你见过哪个保安懂这么多活这么累的，没出事觉得你没用，出事了就得背锅。

我是从CTF入门安全的，以后有准备从事安全这一方面的工作。一年半的时间里算是把CTF里基本是全部的方向都给玩了个遍，全都入门了，全都不精通，，，惭愧。

本科剩下一年半，一年要用来准备考研，还有半年去尝试新的方向，或者在入门过的领域里找一个深入进去。

可能我就比较贪婪吧，什么都想学都想掌握。就是这个原因，当初选了物联网这个专业，因为物联网工程这专业学的多呀，大一一门物联网导论的时候，老师说，软件工程、自动化、通信、计算机的课我们都得学，那时候一听真的是好高兴，哇塞，可以学这么多东西诶，现在，，，计算机的我研究学习的了。

不过学的多，知识面广点也是有好处的。主要是前乌云大佬猪猪侠一次演讲上的话启发了我，他说，知识链决定发动的攻击有多深，知识面决定发动的攻击有多广。从此我就在每个方向的门口划个水留下个到此一游就浅尝辄止了。我当然知道要先精通一个方向在横向发展的道理，但是还是抑制不住内心对新方向新知识的渴望，所以前一秒还是数据库里select呢，后一秒就跑去寄存器了。

CTF里面我主要玩的还是misc，毕竟不像pwn需要深厚的理论功底，不像web各种花式绕狗、WAF，脑洞打开，misc还是很好玩的，尤其是取证那一块，主要考察的就是对新知识理解、运用的能力，以及平时接触积累的知识。玩misc实在是轻松加愉快。

我觉得学习任何领域的任何知识，主要学的还是思想。想特斯拉、spaceX的Mask在15年在清华的演讲上回答清华经管院的提问，他总是会以物理101的思想来回答（101好像是国外的基础课程的编号，我在网上也看过web hacking101，linux101，crypto101）

以我自己学习中的一个例子来说吧，cookie,在web中的应用就不用多说了吧，在典型的场景里，XSS拿到cookie，配合CSRF去做羞羞的事。

在pwn中，也有个cookie，在开启canary的时候，会在指令中加入cookie，如果指令被植入shellcode或者其他方式篡改了，可以通过cookie检测出被篡改了，然后程序就会终止或者报错。

这两个场景里，cookie都是起到凭证的作用，web中cookie正确才能执行用户的请求，pwn中cookie正确程序才会继续执行指令流。

做安全是有一个圈子的，比如现在很流行的威胁情报，大佬们就有一个共享情报的微信群，，比如在weibo上就可以看到，tk，yuange、0x557,heige、瘦蛟舞大佬们的互动，前几届蓝莲花大佬的互动，还有新生代的北航、北邮、西电、成信大佬们的互动。还有xxx的，花无涯、黑色镰刀、helen他们也有一个是吧。。。

好像黑哥在很多团队里，n0troot,好像90sec里也见过黑哥写的东西，泉哥也是，当年pkav还是安全焦点里好像见到过泉哥，还有看雪里，。

我也想加入个队伍、圈子，，无奈自身水平还会太差，对水平够了再说吧，也或许哪位大佬看到这儿之后原意收留我呢。

从来没有一个完美的学习环境，现在学习的资料多了，但是网站的安全意识都上升了，还有网络安全法，提高了实战的门槛，自己搭环境其实有时候还是很麻烦的，在web方向我一直徘徊在内网门口，从来没有接触过内网，或许碰到了我不知道，AWD也没有打过，之前看lemon的github有教学，看到搭建环境就头大了。。。也玩过docker，vargant，其实在国内都不方便，不过买台vps玩还是很不错的。而以前呢，只有一些杂志，很少的资料，我记得看哪位大佬的采访来着，他说当年都是把txt的资料放在诺基亚那小的可怜的屏幕里一点点看一点点学习的，但是当年的网站就是一片蓝海呀，，看完了看心情随意渗透。

现在看到那些漏洞分析就头大，尤其是软件安全那一块，IDA Pro的图片一出来马上开始慌了，，，还有web的代码审计，跟着一个变量跑来跑去，，这应该就是做安全研究、漏洞挖掘的人做的事情吧。

有时候会怀疑自己是否真的喜欢安全，我当然喜欢安全，但是可能不喜欢漏洞挖掘这一块。

做漏洞挖掘当然有其自身的意义，我觉得最大的一点就是再和骇客们赛跑，比谁先找到0day，白帽子们报给公司修复，骇客们集成0day到工具中日后发动攻击，这是真正意义上的攻防博弈。

但是我觉得这是做安全做到最后该做的事情，以前有个典故是说扁鹊三兄弟的，里面有一句话，*上医*医无病,*中医医*欲病,下医医已病

一个医生当然应该是碰到无病治无病，碰到欲病治欲病，碰到已病治已病，一个安全人员也应该是这样的。

治无病，在安全里面，指的就是安全开发，尽管从来没有安全的系统，但是还是尽力保证安全吧。治欲病，指的就是漏洞挖掘，安全研究，在被骇客打破之前，自己人先把它修复。治已病，指的就是应急响应。

以后我做安全，应该是会从事安全研发的吧。

突然意识到学习安全到现在，还没有一点产出。。。到时候不管是工作面试还是考研复试的时候怎么办呢，所以最近有个想法，造轮子，拿python重写个工具，比如metasploit，哈哈哈，开玩笑的啦，那么大的工程量，，，

我觉得大部分src实在是精明，几百几千的礼品就可以吸引大量白帽子帮你安全测试，要是不高兴了再和世纪佳缘一样打个110，主动权在自己手上，又花不了多少钱。当我意识到这一点之后，我就不挖洞了，以前我还在补天、cnvd、edusrc交过。

本科学的是物联网，有大佬提到过，现在的物联网安全就和2000到2005年那时候的互联网安全一样，毫无安全可言，这话说得也有些道理。我就不按学术意义上的把物联网分成几层模型来分析了。

随便看看，到处都是攻击面。从底层采集数据开始，那些传感器本身就要求低功耗，自身的设计就不会复杂，安全协议、算法更是几乎没有涉及，这一块就很容易被攻击了。王小云教授MD5都能碰撞出来，谷歌SHA-1也能破解出来，一般的算法算的了什么。。这一块还涉及到智能硬件的固件那一块，我在ctf中玩取证时用到的binwalk之类的就是在分析固件时很常见的工具，纯玩硬件太烧钱，我接触的基本上都是软件层面的。到了数据传输阶段了，mqtt,蓝牙，zigbee,wifi五无一不存在漏洞，在局域网里面，中间人欺骗什么的更是被玩到烂了。云平台那儿，要是爆出一个系统漏洞，全部的云平台都得遭殃。这还取决于云产商的实力，之前好像某厂隔离环境就没有做好，然后就被嘿嘿嘿了。就我接触到的工控安全来看，其实和云平台也是一样的，本来大部分情况下在局域网里面随便做做是好的，结果被挂到了公网上，小白都能配合着zoomeye,shodan来一波流，能怪谁呢。现在的智慧家居离不开一个中枢，那就是手机。因此最近几年移动安全也是大火，很多师傅都说过，去面试什么人家都会顺便问一句接触过移动安全没有，，主要就说说安卓吧，没有加固之类的apk那简直就是乱来了，被反编译以下，说不定硬编码的密钥之类都泄露了，怎么保证安全。

所有的一切，都根本于开发人员没有安全意识。黑客常会提到的社会工程学，指的就是针对人性的攻击。实在是可怕。万物皆变，人是安全的尺度。

以后想从事物联网安全的工作，上能分析系统逆向应用调试内核，中能破解无线通信，下能拆硬件找引脚玩示波器调戏固件。。。也恐怕也就是一个全栈的安全研究人员的技能了吧。

新的一年里，暂时不打算尝试新的方向了，准备从移动安全入手，开始精通一个领域了。不想划水了~~~

真正厉害的人呢，是做别人没有做过的事情。我还在跟随别人的脚步，实践别人做过的事的阶段，这也是应该做的基础吧。念念不忘，必有回响，总有一天会成为厉害的人的。共勉。