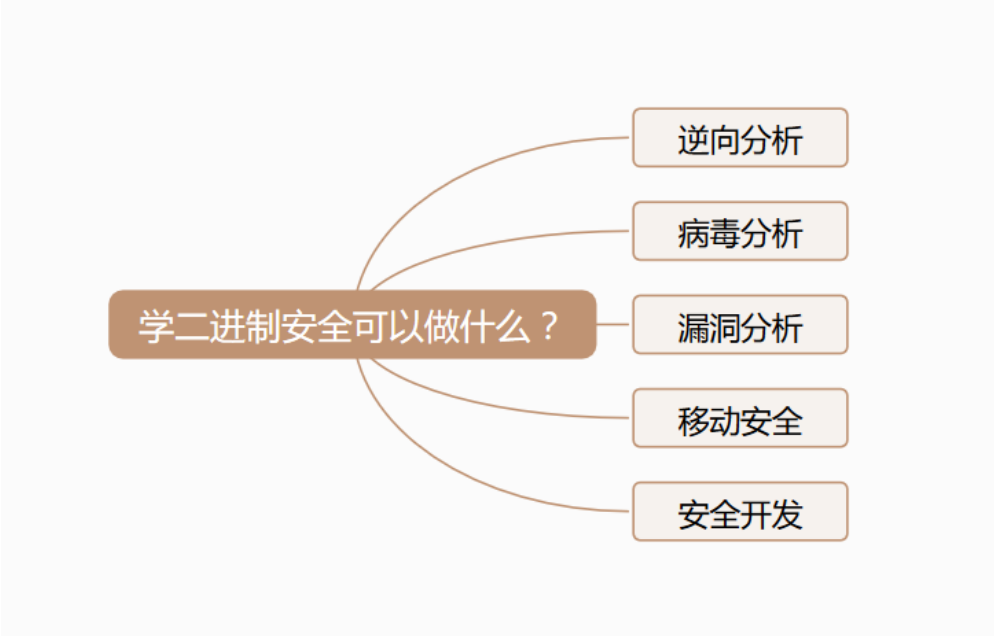
关于二进制安全如何入门

在谈论如何入门之前，我们先来看一下入的到底是什么门。很多人都有疑问，二进制安全是什么？学了二进制安全之后能做什么？我曾经也有过这个疑问，所以首先来说二进制安全到底“能干什么”。



我简单的解释一下这些职位是什么意思：

1.逆向分析：负责分析成品软件的技术原理。比如分析竞品软件，来吸取技术上的优点，进行技术难点公关。需求公司比较广。

2.病毒分析：负责分析病毒样本，研究恶意代码的技术手段等工作。主要是安全公司尤其是杀毒软件公司需求较多。如360、金山、腾讯电脑管家等公司。现有学长在奇虎360任病毒分析职位。

3.漏洞分析：负责分析漏洞样本，对已有漏洞编写利用程序以及漏洞挖掘。主要是安全公司需求较多。现有小组的学长在PKAV、腾讯、360等公司就职。

4.移动安全：负责安卓平台的安全(IOS较少)，也有安卓平台的漏洞挖掘。现有小组的学长在阿里巴巴负责移动安全。

5.安全开发：包含较广，比如硬件平台、内核安全等等。一般都是安全公司需求较多。如防火墙、主动防御系统、反外挂等。比如我面过的腾讯的游戏安全TP团队。

Q&A

1.怎么学习二进制安全?

答：我推荐先去看《逆向工程核心原理》（资料里有）这本书，很多人说要先去学C语言要去学汇编这些是基础blabla……

这些是基础不假，但是你抱着一本C语言（就拿CPP来说）600多页，两个月

也看不完，再加一本汇编半个学期就过去了。而且这些东西真的有用吗？等你真的用的上的时候你自然会去想办法去学。我的建议是你看这些东西就是掌握一个大体的结构就够了，然后就拿着调试器比如OD（工具里有）跟着《逆向工程核心原理》去调试。比如你在OD里面看到了一个不认识的指令，你再去百度再去翻书查是什么意思，不要不动手整天抱着一本书“学基础”。

如果你曾经学习过C语言，看汇编和使用调试器又难不倒你，那么我推荐你去学习一下Windows API的使用，尤其学习一下Windows的数据类型和编程风格。至于学习Windows API，注意不要去看《Windows程序设计》这本书，可能有很多人会推荐这本书，这本书也的确很好很经典，但是它是一本字典，可能没有谁会把汉语字典从头翻到尾来学习语文的吧。我推荐你去找一本WINDOWS API大全一样的书，跟着例子敲一敲，没有书就去MSDN，找不到MSDN的可以去百度百科，比如你想查CreateProcess就可以在百度百科里查到用法。等你已经熟悉了Windows API是个什么东西之后再去“查字典”。编译器我推荐使用VS2015，MSDN就可下到，注册一个微软账号可以永久免费使用。VS2015可能对你来说很复杂，但是值得花一个星期来研究一下是怎么使用的。

tombkeeper ，尔曹身与名俱灭，不废江河万古流

余弦、 慵懒吉他、 猫流、 o0xmuhe、 黄玮 等 137 人赞同

我是先看漏洞公告，2002年之前绿盟漏洞库中的每一条我都看过，在看的过程中理解漏洞。然后看别人的漏洞分析文档，在看的过程中学习调试和汇编指令。最后学编程。

就像TK教主说的一样，我也没有专门的从头到尾的看过汇编语言的书，但是每次遇到不认识的指令我都会去查书，这样那本汇编书反倒被我在实践中看完了。（我不是说编程不重要，我的意思是动手最重要，让需求驱动你学习，而不是书的目录驱动你学习）

2.我现在什么都不会怎么办？&我一点基础都没有，能加入三叶草吗?

答：一年前的这个时候我什么都不会，完全的0基础。连mov指令是干啥的都不知道，都得去百度现查。有很多很叼的学长刚入学的时候也是完全没有接触过安全，但这并不影响他们日后成为大牛。事实上一年时间完全能够学到很多东西，只要你选好方向，付出努力就可以。引用黑哥一句话：整就牛！之前有个学弟跟我说，觉得自己水平不够打算慢慢学等大二再来小组面试。我想说如果真的打算做技术那么就从现在抓起，不要想什么大二再来。等大二就已经晚了，各种比赛机会实习机会已经与你无缘了，既然已经下定决心做技术为什么不抓紧现在呢。当然，在大学里的选择是有无穷多种的，如果你对技术不感兴趣完全可以选择适合自己的道路。

什么都可以不会，但不能学不会。

> **tombkeeper** ，尔曹身与名俱灭，不废江河万古流
>
> 收录于 编辑推荐 • evilddog、 云舒、 o0xmuhe、 慵懒吉他 等 271 人赞同
>
> 给你个建议：别想那么多，先干起来再说。

我找到第一个漏洞的时候，还在医院实习，只会写几行批处理。为了写 PoC 需要学编程语言，看电脑报介绍过 Perl，就去买了本《Perl 编程 24 学时教程》。后来为了写更好的 Exploit 学了 C 语言。再后来，为了各种研究读各种 RFC、调各种程序、读各种代码、试各种工具，等等。干这行，你永远不知道未来需要会什么。所以什么都可以不会，但不能学不会。

3.能不能推荐一下学习资料呢?

答：推荐去看雪论坛：http://bbs.pediy.com/

比论坛本身更有价值的是他的精华合集KSSD:http://www.pediy.com/kssd/

如果你对某一方面感兴趣，推荐把这一子目录下的文章撸完一遍。

4.上面那些东西已经不能满足我了，我该怎么进阶呢?

答：首先可以关注下安全圈内的动态，来获取下新鲜的资讯。

微博就是一个很好的途径：

乌云知识库
http://weibo.com/wooyundrops?from=myfollow_group

玄武实验室
http://weibo.com/xuanwulab?from=myfollow_group

云舒
http://weibo.com/pstyunshu?refer_flag=0000015012_&from=feed&loc=avatar

FreeBuf
http://weibo.com/freebuf?refer_flag=0000015012_&from=feed&loc=avatar

TK
http://weibo.com/101174?refer_flag=0000015012_&from=feed&loc=avatar&is_all=1

Phithon
http://weibo.com/101yx?refer_flag=0000015012_&from=feed&loc=avatar&is_all=1

黑哥
http://weibo.com/u/2783938821?refer_flag=0000015012_&from=feed&loc=nickname

猪猪侠
http://weibo.com/ringzero?from=myfollow_group&is_all=1

然后就是乌云知识库、也可以看下FreeBuf。其实我认为看网上的文章远不如看书，书上的知识是成系统的，往往能够讲清楚前因后果。当然，如果是比较新的内容那么书就不管用了，但是对于初学者来说书是完全足

够解答疑问的。

重要的是学习能力和动手能力，如果是做漏洞方面的话可以多调调POC，我最近也在调一些漏洞，如果有对漏洞感兴趣的小伙伴欢迎联系我，我们可以一起技(P)术(Y)交(Jiao)流(yi) :)