> 最近发现很多小伙伴都在问我想要学习渗透测试，但是不知道怎么开始，也不知道要学习什么？所以在这里我打算分享一下我的渗透学习之路以及给初学者的一些建议。首先做个自我介绍：
>
> **常用ID：** myh0st
>
> **个人博客：** http://www.myh0st.cn
>
> **学习工作经历：** 90sec论坛元老（曾经的管理员）、微信公众号【信安之路】创始人、CISP-PTE（注册渗透测试工程师认证）考试命题专家组成员
>
> **我能回答的问题：** 渗透测试相关问题（当然回答的不一定好，肯定比不上弦哥）、关于CISP-PTE认证的相关问题等
>
> **兴趣爱好：** 热爱技术学习、分享、交流，喜欢交朋友，感谢弦哥的新人邀请我做嘉宾，我会尽我所能帮助圈子里的小伙伴提升自己的技术实力，在信安之路上前行不在孤单。

我的学习之路

转眼间，我从学习渗透测试到工作也快六年了，记得刚开始接触安全是在 2012 年初，刚进入实验班的时候，在之前曾经在图书馆借了一本《黑客笔记》来看，回到寝室看了两页，完全一脸懵逼，一点看不懂，然后就原封不懂的还回去了。我考入大学时的专业是网络工程，跟安全并不沾边，身边也没有做安全的同学，由于学校全校选拔实验班，所以才有了接触安全的机会，进入实验班后就开始了我的安全之路。

回想当时学习安全时的场景，由于之前学过数据库、数据结构、c 语言等专业课，但是对于安全来说帮助并不是很大，所以也算是从零开始学安全。希望我的这些经历能对大家的安全学习之路有所启发。

当时我看的第一本安全资料是 txt 版的《黑客笔记》，还是我们班学习委员分享给我的，在当时一点基础都没有的时候，看起来是非常费劲的跟我大一的时候看是一个效果，但是，既然已经进入了实验班，以后要走这条路就不能像大一的时候那样放弃，所以就硬着头皮一点一点的看，即使当时看不明白，没关系，能够在自己的脑海中留下一点印象就足够了。再后来，我们的网络攻防课给我们发了一本黑客书籍《黑客攻防技术宝典- web 实战篇》，同样硬着头皮把它看完一遍，在看书方面基本也就完整看了这两本书。

如果只是看书的话是非常无聊的，大家都深有感触，尤其是在看不懂的情况下。如何解决这个枯燥的问题呢？我当时的解决办法是：

1.保持足够的兴趣才能坚持下去

2.寻找志同道合的朋友或者组织一起学习一起交流
3.参加CTF比赛，在比赛时会遇到很多有趣的知识点，针对自己的不会的知识点进行逐一理解
4.在学习技术的同时，整理自己学到的东西，然后分享在自己混迹的组织之间
5.在网上寻找有漏洞的网站，进行实战，在获取到权限之后也会提升自己的成就感（目前大家可以拿国外的站点练手，不要选择敏感目标，切记）
我第一个参与的组织是**AG 安全团队**，当时还在玩 YY ，一起玩耍一起学习，后来就在老K的引导下加入了 90sec ，然后每天看看论坛的文章，基本上把论坛之前发过的所有文章都看了一遍，然后把自己在学习中总结的所有知识发到论坛，这样在大家的鼓励下，学习的激情会逐步提升，在体现自己能力同时学习技术，这就是在学生时代的成就感。
在毕业之前学习的安全知识基本上是以 web 为主，毕竟在安全领域，web 安全占据了主导地位，涉及面非常广，有关内网安全、外围服务安全等知识都是在工作后才接触的，这里就不多说了。

如何做一个脚本小子

针对没有一点基础想要入行的同学，一个初级渗透测试工程师所要做到的目标是，在拿到一个目标之后，可以利用自己掌握的所有安全工具，对网站进行全面的检测与利用，刚开始就去学原理会有点乏力，所以切入点可以先从一个脚本小子做起。
对于 web 安全工具，我当年玩的啊D、明小子、穿山甲、萝卜等注入工具，现在都很少有见了，都基本可以用 sqlmap 来代替，所以玩注入一定要把 sqlmap 用熟练，在学会编写 sqlmap 支持的 tamper ，那么你就可以解决大部分的注入问题的利用。
当年玩上传截断是用的 WSockExpert 抓包然后用 winhex 添加截断符最后用 nc 提交，多麻烦，在现在的神器 burp 面前简直弱爆了，所以 burp 也是初学者一定要掌握的工具。burp 不只是用在这里，还可以爆破一切 web 应用，如：后台、wenshell 密码、目录枚举等，还自带编码解码功能，还支持很多的自定义插件，所以学习 burp 也是非常重要的。
当年玩扫描，一般用 s扫描器、superscan、x-scan 等，如今的 nmap 可以做所有的扫描操作，也能自定义扫描脚本，功能强大是公认的，所以学习这个工具的使用也是非常必要的。

作为一个脚本小子，不需要知道很多的漏洞原理以及如何防护，只需要做到熟悉网络上存在的所有安全工具的使用方法，以及这个工具有什么用，针对什么样的漏洞使用，在什么样的情况下使用。在做到这一点的时候，你已经拥有了初级渗透测试工程师的能力，你可以自己完成一定的渗透测试工作了。

如何提升自己段位

在你成为一个脚本小子之后，虽然可以做一定的渗透测试工作，在别人对漏洞做了一定的防护的时候，工具的智能化并不能及时满足需求，所以这个时候，脚本小子就无能为力了，所以就要提升我们自身的能力才能完成我们的渗透测试的功能。
由于业务的驱动，我们不得不提升我们的段位，否则将会被淘汰。要想成为一个中级渗透测试工程师需要做的，就是把我们之前所有会用工具以及知道的漏洞这些原理弄明白，这样即使网站做了一定的防护，在我们的测试下，了解其防护措施然后有针对性的绕过，在这个过程中，你的实力就会不由自主的提升，不过到达这一步的时候你也就不用我建议，你也可以自主完成学习并且进步。
平时养成以下的习惯：
1.能够把自己的学习成果记录下来，在下次遇到的时候可以快速拿出来并且使用
2.多关注一些好的技术博客，像 sec-wiki、长亭的wiki、安全客、freebuf等
3.可以关注一下国外的安全 wiki，如：reddit

渗透测试流程

每一个渗透测试者都有自己的渗透测试流程，这都是自己在实战中总结的方式方法，在这里我说一下基本的流程。
在实战中，越是小的公司企业越难以渗透成功，为什么呢？因为，公司的业务少，只有那么几个暴露在外网的服务，服务越少越容易管理，越不容易出现漏洞，所以攻击面越大我们的成功率就越大，但是如何扩大攻击面呢？
1.收集尽量全的企业域名（包括各种子域名以及子公司的域名，越全越好）
2.收集尽量全的企业申请的公网 IP
3.对所有收集到的域名以及 IP 地址进行端口扫描（由于时间可能比较久，所以可以选择利用 zoomeye、shodan、censys 等平台）
4.针对不同的服务进行对应的渗透测试（尤其是可能存在漏洞的中间件）

经过这几个步骤，你会收集到很多的资料，你的成功率跟你收集的资料的质量息息相关。这几个步骤看起来并不复杂，但是其中涉及的安全知识方方面面非常多，如何收集的够全，如何测试的更准确都是我们需要关注的。

针对web的渗透测试

拿到一个 web 网站，我们首先需要知道，这个网站用的什么服务器、用的什么脚本，可以使用一些抓包软件如：burp 等，根据服务器的 banner 来猜测。
如果不怕服务器拒绝服务，也可以直接拿大型扫描器进行扫描，如 awvs、netspeaker、w3af 等。
也可以用一些开源的爬虫软件爬取所有的动态页面，了解网站的所有功能，只要是我们用户可以控制的内容，都是我们需要测试的地方，一切用户可以访问到的功能都是不安全的，不局限于 web 功能、也包括隐藏的 http header 中的一些字段，如：cookie、x-forward-by、referer等。
有些爬虫爬不到的页面可以通过查看，robots.txt 发现一些隐藏的目录，或者使用搜索引擎寻找以前收录过的测试页面或者使用目录扫描器枚举存在的目录，工具如：wwwscan、burp 等，重要的是字典。
还可以使用一些寻找信息泄露的工具，如猪猪侠的那个敏感信息泄露的工具，寻找一些备份文件，从中寻找可以利用的点。
针对那些开源的项目，大家可以在网络上寻找对应版本的已知漏洞进行测试，如果没有的话，自己有实力可以去挖。
总之，方式方法多种多样，需要时间的积累，只要能够坚持下去，相信在不久的将来你一定会成长为你想成为的人，大家共勉。