# 渗透测试入门手册

**本手册将持续更新！这是20190607版**
**如果觉得本文有用，请高抬贵手分享给你的朋友。**

## 渗透测试是什么？

- 维基百科的释义：https://zh.wikipedia.org/wiki/渗透测试
- 百度百科的释义：https://baike.baidu.com/item/渗透测试
- 5号黯区的释义：我们理解的渗透测试是通过各种手段对目标进行一次渗透（攻击），通过渗透来测试目标的安全防护能力和安全防护意识。
    - 打个比方：比如电视剧《我是特种兵》里面的演习，特种部队（进攻方）渗透到蓝军（防守方）的指挥部进行斩首，如果斩首成功，那么就可以知道蓝方的防守能力不够好，需要改进，反之就是特种部队的特种作战能力不足，需要提升。那么渗透测试工程师就相当于特种部队里面的特战队员，我们需要对我们的目标做一次渗透，以测试目标的防护能力。渗透测试工程师就相当于矛，目标就相当于盾。

## 学习渗透测试的战略方针是什么？

其实这个方针很简单，但是很多人就是无法严格贯彻执行。简单来说就是：多学，逮住几套视频，使劲看，使劲学，使劲啃透。

所谓技术大神是怎么样的呢？技术好？说技术好是很宽泛的，很表面的。我们把技术好剖析开来就是：懂得多，解决问题能力强。其中，想要懂得多比较容易实现，多学习知识就行了，但是否能把知识用于工作，这就是解决问题的能力了，这个能力需要培养，也有的人解决问题的能力天生就比别人好，这也就是为什么有些学历低的人，却比很多学历高的人混的还要好的一个很重要的原因了。

### 知识的积累

想要懂得多，就要话大量时间去看，去记，去实践，去总结。大家可以看到，无论是电视上还是现实中，绝大多数满腹诗论的人都较为低调，因为他们把自己一天中大量的时间花在了学习和研究上面。那么我们学习渗透测试，到底该如何去学呢？找到一个有足够多技术总结的文章或者是视频教程来学习，一定要静心学习，学习从来都不是浮躁的人能做好的事情，无论是学语文数学还是渗透测试。学完一套就学第二套，起码得看三套视频，这三套有很多知识点是重叠的，但是因为讲解人的讲解方法不同，你也就会有不一样的理解，更能帮助你消化吸收知识。三套视频总课时加起来得有250课，如果每课约为20分钟，那就是5000分钟，大约就是连续学习84个小时，如果这84个小时的知识你都懂了，那么恭喜你，你入门了，你能对小型网站发起渗透测试了。

### 解决问题的能力

解决问题之前要找到问题出现的根本原因。比如你觉得你跟你的女（男）朋友分手是因为某一件事出现了分歧的争吵，但事实上是因为你们的观念不同，因为你们不够相爱，争吵只是你们分手的导火索，并不是根本原因。所以，透过现象看本质非常重要，这关乎我们能否彻底的把问题解决。那时候有个人跟我说，他看了很多教程，也懂很多知识，但就是无法实战，所以他实习的时候不敢去面试安全公司。*他表达得有点粗俗：“我看过很多视频，也懂得怎么利用某个漏洞，但是当面对一个网站的时候，我就是不懂的怎么下手，就比如有个美女躺在我身下，我都不知道怎么下手。”*我特别纳闷，既然美女都躺下了，你为何不替她宽衣解带？不会宽衣解带？那你也不懂去看看岛国的爱情动作教育片？那其实说到底就是你看不到自己的知识储备量不够。既然知识不够，那就胆子来凑啊，不会宽衣解带，就撕开啊！还是不会撕开，那你就脸皮厚一点，让人家女生自己来啊。这种事情的最终目的是达到双方都愉悦的目的，谁主动都可以的啊。回到渗透测试上来，他不知道如何对一个网站下手，我问他为什么？他说不知道，这就是我们开头说到的，不知道如何对一个网站下手是他不敢去面试安全公司的一个原因，但是根本原因是他不会变换方法，没有舍我其谁的勇气。

## 学习渗透测试的具体方法是什么？

1. 关注一些安全站点：这样可以了解最新的东西，提高对安全的亲切度，这样你不惧怕它，才能靠近它，占有它。

```
www.freebuf.com
www.anquanke.com
xianzhi.aliyun.com/forum
www.52stu.org
```

2. 找几部高质量的视频教程，坚持学完，并做好每个视频的笔记。*我以前学习是别人每讲完一个知识点我就把视频暂停，然后把笔记做好再继续看的，甚至把视频里面的代码抄下来，自己读再一遍那个代码（虽然读不懂，但是混个脸熟也挺好）。*
3. 制定一个小阶段的学习计划及目标。
4. 建立一个自己的博客，把自己的所学、自己的笔记记录下来。这个很重要，因为这样你可以以一个第三者的视角看待自己的东西，就会找出不足，你就可以改进。
5. 每天看几篇漏洞文章，以增加自己的漏洞只是储备量。http://wooyun.2xss.cc/
6. 每天遇到新的问题，我们不妨用笔记录下来，一个一个的解决，不要着急，古人云：欲速则不达，慢慢的，你的只是储备量就会多起来的。
7. 买两本纸质书籍当作理论支撑，因为视频里面讲的理论没有以文字呈现，大家理解起来也是有困难的。这里推荐几本：入门级别的《Web安全渗透剖析》，进阶级别的《白帽子讲web安全》、《网络攻防实战研究：漏洞利用与提权》。
8. 找一些跟自己志同道合的朋友一起学习。比如加一些讨论氛围好的QQ群，一些小密圈，一些论坛。那些论坛搞得花里胡哨的就肯定不是静心钻研技术的。这里我稍微推荐一下我们论坛www.52stu.org，*要用电脑浏览器才能访问哦！*我们论坛是坚决抵制花里胡哨的，一看到就直接删掉。

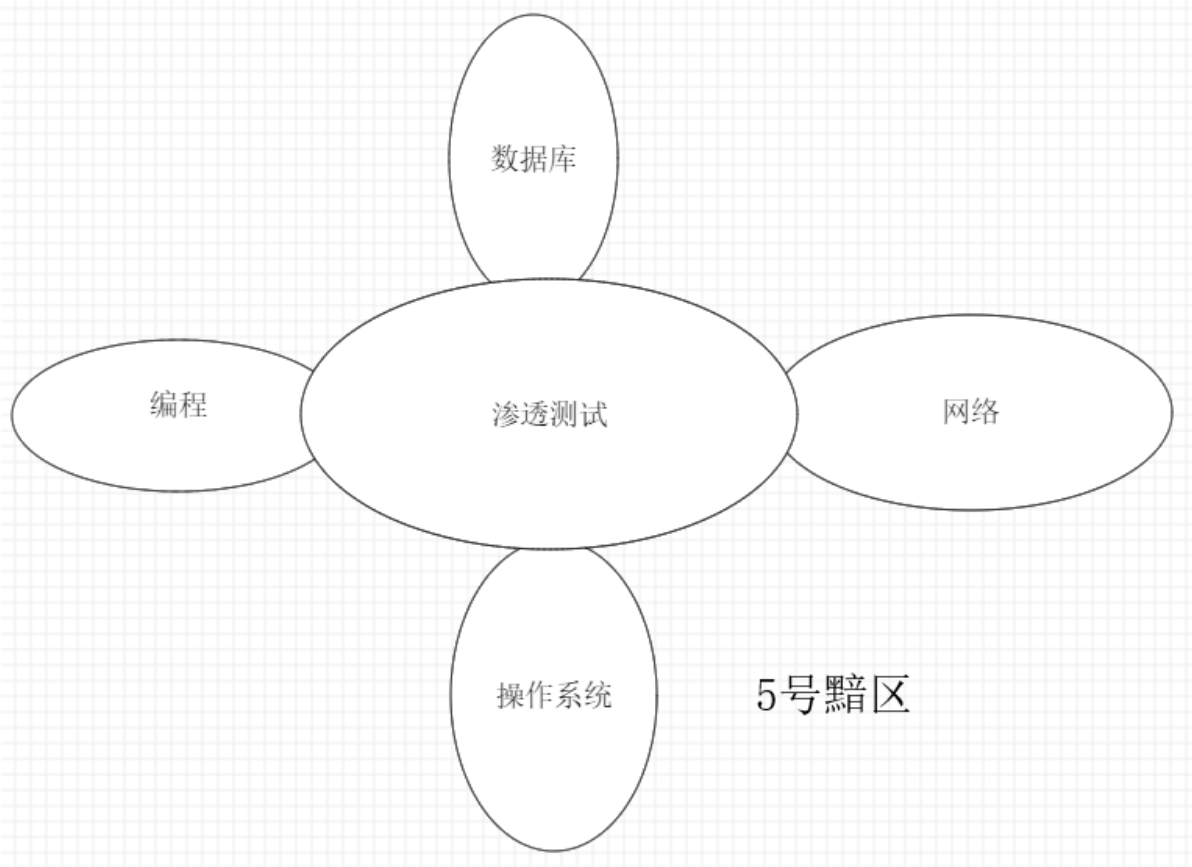
# 学习过程中遇到的各种疑难杂症怎么解决?

## 渗透要不要学编程?

*相信人都会有这个疑虑，那么作为职业的渗透测试的我，可以跟大家说一下我的看法。*

学习渗透测试之前要明白渗透测试这个领域包含什么东西，渗透测试是集合计算机各领域的知识于一体衍生出来的计算机新领域。

请看下图：




从上图就可以清晰的看到，渗透测试会涉及包括但不限于数据库的知识、网络技术的知识、操作系统的知识、编程的知

识。所以你觉得你要不要学习编程呢?

**计算机各领域的知识水平决定你渗透水平的上限** 比如你编程水平高，那你在代码审计的时候就会比别人强，写出的漏洞利用工具就会比别人的好用；比如你数据库知识水平高，那你在进行SQL注入攻击的时候，你就可以写出更多更好的SQL注入语句，能绕过别人绕不过的WAF；比如你网络水平高，那你在内网渗透的时候就可以比别人更容易了解目标的网络架构，拿到一张网络拓扑就能自己在哪个部位，拿到以一个路由器的配置文件，就知道人家做了哪些路由；再比如你操作系统玩的好，你提权就更加强，你的信息收集效率就会更加高，你就可以高效筛选出想要得到的信息。

## 计算机各领域的知识水平，我们该学到什么程度呢?

我说了，**计算机各领域的知识水平决定你渗透水平的上限** 那咱们零基础是不是要把上面的都学的很好了再搞渗透呢?并不是的，作为初学者，可以先学习那些基础，比如你先学一个编程语言的基础，用PHP做例子，你起码要懂if else这些、连接数据库；比如学数据库，用MySQL做例子，那至少也是要会增删改查、子查询这几个操作；网络的话比较难，也是很抽象的，你做外网的渗透，至少要懂基础的http协议，知道端口是什么，知道网站是怎么架设起来的；操作系统的基础相对比较好学，主要是各种命令的作用，各种软件的安装和使用，*你非要使用那个对你们没啥卵用的kali-linux就得先学习Linux的操作*

## 渗透测试的思维是怎么样的?

- 我们所谓的猥琐的思维就是渗透要的思维，也就是大家常说的鬼点子多，鬼主意多。这意味着我们要从不同角度去思考同一件事情，但我们在渗透的时候要始终贯彻一个方针：换位思考。比如管理员会怎么设置网站，管理员会怎么设置密码，管理员会… …
- 渗透就跟泡妹纸一样样的，认识妹纸--了解妹纸（信息收集）--逗妹纸开心（扫描）-- 得到妹纸的肯定之后就开始寻找时机表白（漏洞利用） -- 表白失败（漏洞被修补或有WAF）要么死缠烂打要么就Next one，要么就用其他的方法来搞定妹纸（有WAF就是心存芥蒂，我们就要得到真心，就是要用真情感化），比如搞定她姐妹，帮她搞定她的难题，要浪漫~!

## 学习渗透的过程中遇到问题问谁?怎么问?

- I、学会利用搜索引擎
  渗透测试主定是一个非常有破坏性的技术，所以很多问题都没办法直接搜索到答案，这就考验各位的学习能力了。比如用Google、Baidu变换关键字来搜索。
- II、到论坛提问
  去问别人，一定要把问题描述清楚，最后是把出现问题的地方截图一起发出来，方便好心人回答，比如我们5号黯区论坛的提问和回答，请看下图：

查看: 37 | 回复: 2

**上传一句话木马连接上过一段时间就被踢出来怎么搞** [复制链接]

发表于 2019-5-28 08:07:26 | 只看该作者 楼主 电梯直达

**hycc**

3 主题 | 10 帖子 | 43 积分

新手上路

积分 43

发消息

IP 编辑 禁止 帖子 清理

本菜在进行一次测试的时候，成功上传了一句话，并连接，但是过了一会就会被踢出，网站也无法访问，过一段时间网站又能访问，菜刀马也能连接，有什么思路解决下这个问题?求大神解惑

收藏

回复 编辑 推送 举报

发表于 2019-5-28 10:33:58 | 只看该作者 沙发

**IversOn5**

9 主题 | 22 帖子 | 106 积分

超级版主

积分 106

发消息

IP 编辑 禁止 帖子 清理

我们通常说的被踢出来，是说马被删除了，也就是权限丢了。

但是你这个是没有被删除的，也就是管理员是没有发现的。
1.出现暂时性不能连接的问题，考虑是网站服务器有某些防护机制。这种机制可能是你执行了某些特定的命令就会被触发。
2.还可能是目标网站服务器的网络有问题。

解决办法:
1.针对第一种，就需要你细心看看是不是执行了什么命令就连接不上。
2.第二种的话，一旦出现访问不到的情况，那就可以用你的vps机器去访问试试了，看看是不是别的IP可以访问的到，就你的不行。如果是的话，那就是有某种WAF了。
3.尝试用一些TCP的马去操作，比如MSF、远控。

enter description here

查看: 105 | 回复: 10

**对内网知识的一些不解** [复制链接]

发表于 2019-5-13 22:34:03 | 只看该作者 楼主 电梯直达

**白云**

1 主题 | 10 帖子 | 84 积分

注册会员

积分 84

发消息

IP 编辑 禁止 帖子 清理

问题一：内网具体是如何组成的呢?
问题二：如何才能了解清楚学校或者小区的内网结构?
问题三：在内网中，如何查看哪些IP地址被占用?

收藏

回复 编辑 推送 举报

发表于 2019-5-13 23:09:32 | 只看该作者 沙发

**IversOn5**

enter description here


- Ⅲ、加入一些培训
  培训都是有答疑解惑的服务的，但是回答的好不好就看讲师的水平了，我知道的网上的很多讲师都是半吊子，语言表达能力也是很有欠缺的。大家选择的时候一定要擦亮眼睛，我就不给大家推荐了。

## 渗透工具的问题

我一开始就是用的Baidu找的工具来用的，当然，现在也差不多，只是多了朋友间的相互传递。你 **不要怕有后门**，因为都是要放在虚拟机里面运行的，只要还原一下VM的快照就完事了。而且随着学习的深入，你就会发现，其实平常用的工具就几个：Burp suite、AWVS、App scan、SQLmap、浏览器。至于其他的扫描器的话，很多都是脚本语言来写的，比如Python，只要是个正常人都不会往Python脚本里面加入后门。亦或者是Java。这些东西在官网下载，或者一些可信度高的网站下载就可以了，就比如上面的网址提供的下载。

## 关于渗透测试实战的问题

网络安全法规愈发完善，我们不小心可能就做了违法乱纪的事情，所以请大家切勿瞎搞。我们可以去一些在线靶场去测试我们的所学，比如墨者靶场；还可以在本地搭建一些本地靶场，比如Dvwa；我们5号黯区未来也是要花大力气去搭建比这些都要逼真的靶场的，包括owasp top 10的漏洞，还有内网的工作组渗透、域渗透，包括流量监控和键盘记录，更甚者是邮件规则滥用getshell，一切都模拟真实的大型网络环境。当然这个靶场搭建下来估计要不少钱，所以也是要付费才能使用了的。

## 关于学到什么程度才能去工作?

如果是在校生的话，人家企业是会放宽条件的。安全方面的也有很多个方向的，比如有渗透、安服、审计，这个就要看你往哪个方向走了，360行，行行出状元，不要问我哪一行吃香，没有产出，你连呼吸都是错的！至于学到什么程度，你可以去看人家招聘信息啊，然后去应聘啊，不要怕应聘，主要是测试自己是否达到人家的要求，如果达不到就继续学习呗，反正你还在读书。如果不是学生又要转行，最快的就是找培训机构培训，比如我们5号黯区的培训。

比如甲方的安服方向

职位描述

**岗位职责**

1、负责对客户业务系统、APP进行安全检查和渗透测试，并协助客户做好漏洞修补和安全加固工作；
2、协助客户对突发安全事件进行应急响应，分析取证并提出有效应对措施；
3、跟踪国际/国内安全社区的安全动态，进行安全漏洞分析、研究与挖掘；
4、参与安全评测技术研究、工具开发及实验环境搭建，参与相关国家科研项目申请和研究工作；

**岗位要求**

1. 有相关实习经验
2. 熟悉Web攻击方法, sql注入、Xss攻击、命令注入、CSRF攻击、上传漏洞、解析漏洞等；
3、会使用主流渗透测试工具，Burpsuite、sqlmap、appscan、AWVS、nmap等；
4. 至少熟悉一门编程语言C/C++/Perl/Python/PHP/Go/Java等，能够进行WEB渗透测试，恶意代码检测和分析；
5. 思想端正，具有较强的责任感和良好的团队协作精神；
6. 加分项：（1）在安全杂志或者社区发表过文章；（2）参与过CTF比赛、安全攻防竞赛。

注：能力突出的应届生不受此薪酬限制。

比如乙方的安服方向

- 渗透测试工程师(J10336) (未申请)

**招聘类别：** 实习生招聘 **工作性质：** 实习 **薪资范围：** 面议 **招聘人数：** 40

**发布时间：** 2019-02-01 **截止时间：**

**工作地点：** 全国

工作职责：

1.负责公司承接的渗透测试项目；
2.跟踪国际/国内安全社区的安全动态，进行安全漏洞分析、研究与挖掘，并进行预警；
3.协助做好信息安全风险应急响应工作。

任职资格：

1.熟悉渗透测试步骤、方法、流程，熟练使用一定量的渗透测试工具；
2.熟悉攻击的各类技术及方法，对各类操作系统、应用平台的弱点有较深入的理解；
3.熟悉常见脚本语言，能够进行WEB渗透测试、恶意代码检测和分析；
4.有一定代码编写能力，至少掌握两种以上常见编程语言；
5.主动性强，具有良好的沟通、协调和组织能力和文档编写能力，逻辑性强，具有较强的责任感、具备能够独立的开展工作的能力；能熟练阅读英文文档。

比如乙方的渗透方向

任职资格：

1.精通多种安全技术，掌握或熟悉各种攻击与防护技术；

2.具有一定的脚本编程能力，可以自己编写简单的攻击和检测程序；

3.有Unix、Windows系统知识经验，能熟练使用Unix、Windows系统平台下各种应用系统，如：MSSQL, Oracle, Exch

ange等；

4.熟练掌握某一类开发语言，如Java/PHP/.NET等；

5.具备较强的动手能力，熟悉常见渗透测试技术和工具；

6.掌握逆向的相关技能，有一定的逆向分析实践经验优先；

7.有安全和网络相关证书，如CISSP、CISA、CISP 、CCNP、CCIE等认证者优先。

§

**本手册将持续更新！这是20190607版**
**如果觉得本文有用，请高抬贵手分享给你的朋友。**

# 关于我们

**致力于培养出更多实战型网络安全人才。**

# 关注公众号

关注公众号

# 随意捐赠

随意捐赠

## 加入小密圈

加入小密圈

## 加入QQ群

加入QQ群