如何学习

经常会有人来问我一些关于学习方面的困惑，概括起来基本就那么几个问题：

1. 感觉自己很迷茫什么都学什么都不会，像个无头苍蝇一样
2. 学习xxx也很久了，但感觉还是很菜也没什么产出
3. 安全搞来搞去也就那样，xxx这块太卷了感觉搞不出什么东西来了

确实，这些问题我在年轻的时候也是经常拷问自己，直到我三十了，ED了，我才慢慢的走出迷茫。想了想，也确实可以给大家写一些建议，希望帮助大家摆脱无端的迷茫投入到真实的进步当中。

先排除初学者

如果你是初学者，你应该先学基础，可以按照下面的步骤学习：

1. 给自己一个月时间学习基础性知识，比如tcp/ip网络、win/linux操作系统、一门脚本语言比如python，多做简单的实验，不用完全掌握，看书看半本就行了后面的选学。
2. 买几本书比如《白帽子讲安全》、《java代码审计》、《内网安全攻防》等，分别对应的是web安全基础、java审计基础、内网基础。当然不一定要都学，可以选其中一个感兴趣的仔细读完一本，其他的大概了解一下就行了，如果你对其他领域比如iot之类的感兴趣也可以自己去找对应的书籍看。
3. 装个kali，玩一玩常见工具比如nmap、sqlmap、burpsuite、ida让自己对简单的脚本小子有一定理解先。

上面这些不一定要几个月，也不是要串行的学习，可以并行的穿插着一起学。在学习的时候我建议多看书多做小实验打打靶机，不建议报班和看视频。快的话一个月能渡过初学期，有一定功底后就进入到无止尽的学习路了。
一定要多用搜索引擎，群聊问问题是最低效的，迭代搜索法才是解决实际问题最有效最快捷的方式。

好了开始进入正题

这里我建议以实际项目驱动进行学习，过程如下：
自我定位->设立项目->解构项目->完成第一个子项目->阶段性复盘->反思性学习->进行下一个子项目->循环直到完成目标项目->整体复盘和反思性学习->重新定位->设立新项目->循环

自我定位

首先我们要对自己的职业定位有一定的认知和规划。这里我用游戏的机制来比喻一下，我们玩mmorpg的时候都需要对人物进行加点和转职，在现实社会中你可以理解为人类的时间精力总量大致相同，对应到游戏里就是技能点数大致相同，那么技能那么多我们就需要去合理分配点数（时间精力）加到必要的技能上去。
我们度过了初学者期后就进入到了初级职业转职的时候了，一转的时候我们得先选择大方向而不是纠结小方向，大方向比如我是做web还是做二进制，是做app还是做pwn等，选择一个自己喜欢的大方向后就开始做具体项目了。
后续随着经验的积累，这种转职会越来越明细，比如web里的二转可以转代码审计或者黑盒src等，再比如代码审计的三转可以转php或者java等
安全是一个越来越细分的领域，职业定位会随着你的学习而进入不得不选择一个方向的时候，这时候对自己定位很重要，如果你定位不清晰很容易浪费你的精力。
当然，在你没有到达下个转职阶段的时候，你可以根据自己的实际情况随意分配你的技能点数，即使你一个web分配到域内攻防也是没关系的，只要你的大方向对就可以了。不用太纠结自己是不是乱加点了，人生就是瞎几把加点的。

项目驱动学习

那么好，我们开始进入到真正的学习长征。我建议围绕**项目**来进行自我驱动学习。这里说的项目可以是任何东西，并不是说要进入公司做实际公司的渗透项目，而是指你要给自己定一个实际的目标，这个目标是具备在一定时间内可以完成的。比如我在之前给自己定的目标是挖掘sxf的vpn漏洞，那么我就会去围绕这个具体目标进行学习，大致上分为下面几步：

1. 指定一个具体目标，比如挖掘sxf vpn
2. 针对该目标进行信息搜集，比如获取目标的镜像，了解镜像里的各种服务和配置，后台大致功能，vpn操作步骤等
3. 基于前期的信息收集我们开始做项目初期评估，比如可能要花费的时间，涉及到的技能树有哪些，阶段性产出是什么
4. 如果项目比较大，那就进行解构，解构成几个具体的部分，比如vpn里有php的后台、apache的模块、nodejs等，那么每一个都可以是一

个**子项目**，针对子项目进行进一步评估并排序
5. 针对排序完的优先级第一的子项目涉及到的技能树进行学习，先学到该技能的最低要求，然后停止学习，进入到项目里进行尝试性使用，在一轮几天的使用后进行反思，然后回到技能的学习上，如此反复直到达到阶段性目标比如挖到一个简单的漏洞
6. 多做笔记，将自己达到目标的整个过程都用文档来记录下来，记录时注意不要只记录正确的步骤，也要记录你失败的过程和你针对失败的思考，失败的尝试才叫经验，成功的过程叫做流水账

这样一套下来你就会有项目经验了，也会因为有实际产出而获得激励从而促使你进行下一个项目的学习。同样的你在项目实践中也会遇到各种困难，这些困难会促使你逐步反思打磨你的认知。

复盘

在完成一个项目时（包括一个子项目），我们应该进行复盘，复盘时应该写复盘笔记，一个复盘里至少要包含以下内容：

1. 项目整个完成过程的记录，包括失败的尝试和成功的尝试，以及思考的过程
2. 有没有副产物和存疑的地方，比如过程中学到一些新的技巧点，或者是某一块代码看起来有点问题以后可能用得到，这些都记录下来
3. 技能树是否存在不足，哪些地方不足，这些不足强化的优先级如何，对于优先级高的强化点放入后续的学习计划之中
4. 对成功的场景进行抽象总结，对抽象出来的场景进行泛化成为一种漏洞思维模型，后续的遇到类似的模式直接套用即可
5. 对涉及到的项目文档进行细节整理和补充，因为我们在做项目时通常是边做边写会写的比较乱，复盘整理的时候需要把他们重新整理，文档结构越规范越清晰越好

反思性学习

在复盘完成后，我们会有很多新的体会和认知，尤其是对自身技能树的不足有一定的认知，那么我们应该进行反思性的学习，针对不足的地方进行针对性加固学习，不过学习的时候一定要遵守以下几个原则：

1. 不要焦虑，你在经历过一个项目后你肯定会发现自己好菜啥都不会，很正常，你本来就很菜，因此不要焦虑，你能完成项目就说明你有产出，这个产出就是你进步的证明
2. 对技能树加固要有取舍，你发现一个综合的项目涉及到方方面面，你各个方面可能都不太会，这时候你要对技能树进行梳理，哪些是需要舍去的，哪些是需要加固到最低要求的，哪些是自己主要方向需要不断强化的
3. 设置学习的时长，不能一直陷入学习中，学习是学不完的，反思性学习可以认为是进行下一个项目前的准备期，这个时间不宜过长，一般建议两星期左右。

其他建设性意见

1. 早睡早起，少喝咖啡多喝牛奶多锻炼，有点不舒服就去医院看，保持良好的身心健康才能持久的学习
2. 不要骄傲和自卑，完成了某某项目获得某个荣誉，这时候你要提醒自己不能骄傲，开心就分享一下吹个牛就完了，居功自傲要不得。另外也不能自卑，谁都是个彩笔，不懂很正常，知识是学不完的，你要是觉得自己是大牛那一定是因为你处于无知的高峰
3. 不要想着一口吃成胖子，所谓欲速则不达，大器晚成，按照计划一步一个脚印走才是正常的
4. 保持分享，交流分享有助于激发新的思想，经常能看到某人分享了一个技巧后群友一顿讨论后得出一些新的情况和玩意
5. 混圈不等于技术等级，你混什么圈和你自己的技术无关，你和p🐂一个群你也是个学习p🐂十年前技术的彩笔
6. 提问不等于交流，整天问问题不是交流，是白嫖知识，适当的问题可以促使思想风暴，但不代表你可以一天到晚白嫖，你要想着去回馈帮助你的人，而不是一天到晚浪费别人时间
7. 知识体系可以参考，但不要纠结，项目才是一切，选择与你职业定位相关的项目就可以保证你的发展不会走歪
8. 碎片知识很多每天保持跟进但不要全学，建议只学习与你强相关的文章非强相关的文章推送可以大致过一下脑子知道有这么回事以便哪天遇到时候可以快速索引
9. 知识没有高低贵贱之分，尽量避免带有偏见去看待事物，比如鄙视等保合规、鄙视扫描器、看不起吹概念不落地的等，抛开吹逼和人情世故部分，这些事物本身都有我们值得学习的内在
10. 文章也是产出，如果你做项目比如审计cms却没有找到漏洞，那么你可以把过程记录下来成为文章，文章也是产出不要认为自己一点产出都没有，这就是你的产出

赛博回忆录

收录所有的学习记录，过往总将成为过去，记录下学习的历程成为回忆录，以后老了这就是曾经努力存在过的见证。安全所有领域最后必将殊途同归，希望我们能在技术尽头的烧烤摊相遇，到时候一起撸串吹牛逼