本课时，是无相关技术介绍，但笔者认为本课便是整个系列的点睛，故此时选择主谈一课时“关于渗透的沉思”。

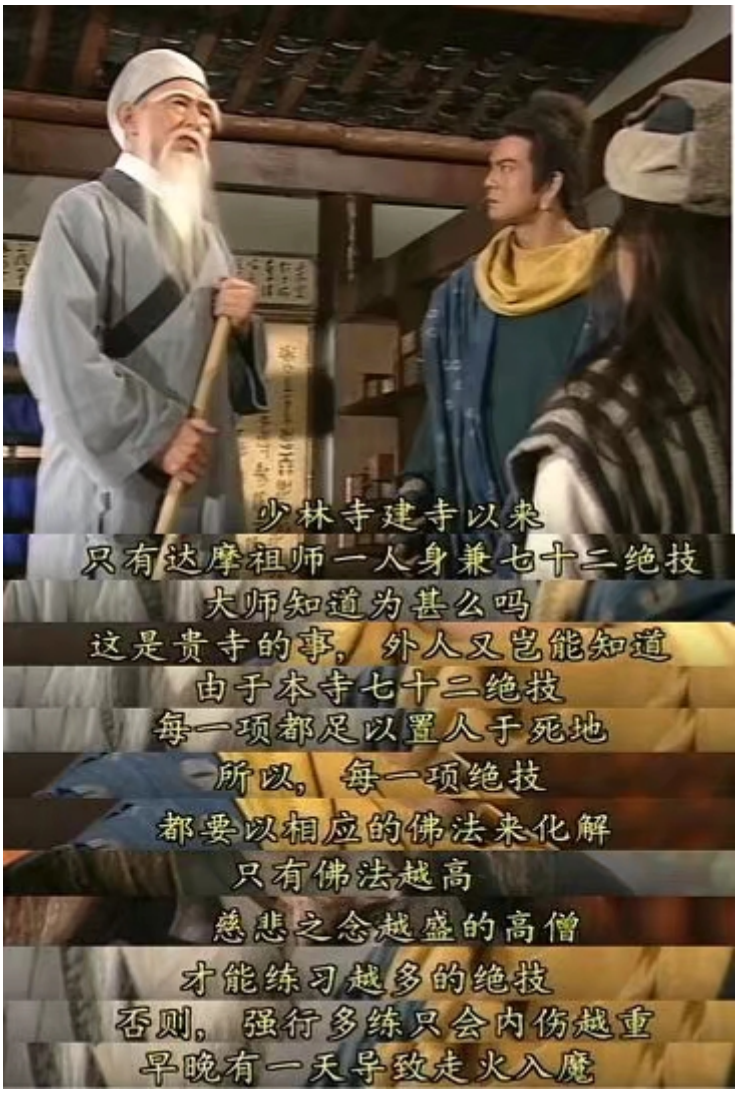
在谈"渗透的沉思"之前，先来解决几个问题。也是这几天邮件以及留言的主要问题之一。

- 刚入门应该学习那一块知识？/安全从业者工作多年感觉心累，知识更新太快，跟不上了，怎么办？
- 是不是应该选择并新学习一个大型渗透框架来做渗透？
- 某项目/某目标渗透没有任何思路了，怎么办？

这三个问题应该是每一个安全从业者在不同的阶段一定会遇到的三个问题。同时笔者曾遇到过4四次瓶颈，也分别与以上大致相同，只是第四次迷茫瓶颈，会在未来的课时中更新。

网络安全是一个特殊的行业，亦正亦邪。亦又一新兴行业，虽前景可期，但是大多数人都在”摸石头过河“虽前岸可期，却对河水深浅无所知。无论是入门还是工作多年都会遇到特别迷茫期，选择哪个方向，亦或者知识无心更新，网络安全应该选择一个可以“沉淀”下来的方向便是最好的方向，让多年的知识或者技能沉淀下来，形成知识化，体系化，与传递化。最简单的一个例子，笔者应该在2009年写过“针对一流信息拦截系统”的技巧与归纳，回过头看来，这个技术在今天还能用吗？甚至“一流拦截”这个软件都没了。但是能留下来至今依然有用的便是：知识化（对一流拦截的研究总结），体系化（对当时waf等的系统归纳），传递化（文章分享）。我把它简称渗透"三板斧"，更像是：学习，归纳，总结，分享的一个完整流程。并非知识太快，并非哪一安全方向领域就一定更有前景，而是这“三板斧”是否完整连接。

渗透测试发展到如今，工具五彩缤纷，框架五颜六色，姿势日益骚奇。知识来源手段源源不断，一会推特，一会小密圈，眼花缭乱，应该怎么去看待？这里笔者先把这个问题放下来，不知大家看没看过《天龙八部》，也借此缅怀金庸先生，在天龙八部中，原著用一百万字在讲述一个非常悲剧的故事，想复仇的得不到复仇，想复国的得不到复国，想复婚的得不到复婚。虚竹呢？又是不忘初心，虽内功与美人竟得，但却再也回不去少林了。刚认父母，便生死相离。8个字概括整个著作便是人生八苦：生苦，老苦，病苦，死苦，怨憎会苦，爱别离苦，求不得苦，五阴炽盛苦。也正是Micro8系列的主旨8章标题，在扫地僧一集中是这样说道：



同样渗透也一样，并不是强制个人追求工具，框架，姿势来强制推演表面的功力，正如鸠摩智一样，靠小无相功来驱动少林72绝技，最终走火入魔，人走向最后的迷茫。反观乔峰，主要就会那么几招，便震出扫地僧口吐少许鲜血。获取工具/框架/姿势等越多并非是一件好事，当没有自己的知识体系的时候，反而导致知识混乱，体系复杂。当遇上实战场景，不知用哪一招来制胜。混乱一通，权限丢失，踪迹露出。最终一场空。渗透的沉思非常重要，尤其是在后渗透阶段，需要有着一套非常完整周期计划，思考可能遇到的问题，或者通过已知的信息搜集，来推导可能面临的问题，这就是渗透的沉思。招式不在多，在于精，力道不在狠，在于寸。故本系列并非是仅仅msf教程，仅仅是认为它能让笔者融会贯通，在结合到其它需求，借力发力的去进一步渗透。说到融汇贯通，必须要提到“链”，安全是一个链安全，攻击引入链攻击，后门引入链后门。具体参考：高级持续渗透系列的连载，它不是在讲述一个后门，而是一个概念的引入。

渗透的本质是信息搜集，每一次的项目如果碰到迷茫无解的时候，请继续搜集。而信息搜集的本质是渗透的沉思，与线索“链”的关联。每一次真实的攻击演练项目，最难得并非是入侵攻击，也并非是得到域控或最高权限。而是如何把渗透攻击演变成一次对己有利的一

个过程。后渗透需要沉淀，而沉淀需要给渗透留下沉思的时间。用“沉思”来化解五彩缤纷的工具，五颜六色的框架，日益骚奇的姿势，当戾气化解时，便形成一套了自我知识体系。

愿每一位读者能找到自己能融合贯通的“武功”，在结合吞噬其他“招式”，如行云流水，石便是器，枝便是剑。

- Micropoor