红队思维1------关于红队攻防和玩俄罗斯方块的共性

0x01 红队的基本面

红队和渗透测试的不同就在于拿权限，渗透测试可以交很多不一样的漏洞，例如xss，ssrf，但是红队关注的点就是权限。

在之前的文章中也有提到过，红队拿权限主要靠

反序列化漏洞

sql注入

文件上传

这三类漏洞来实现rce，然后进去打内网。

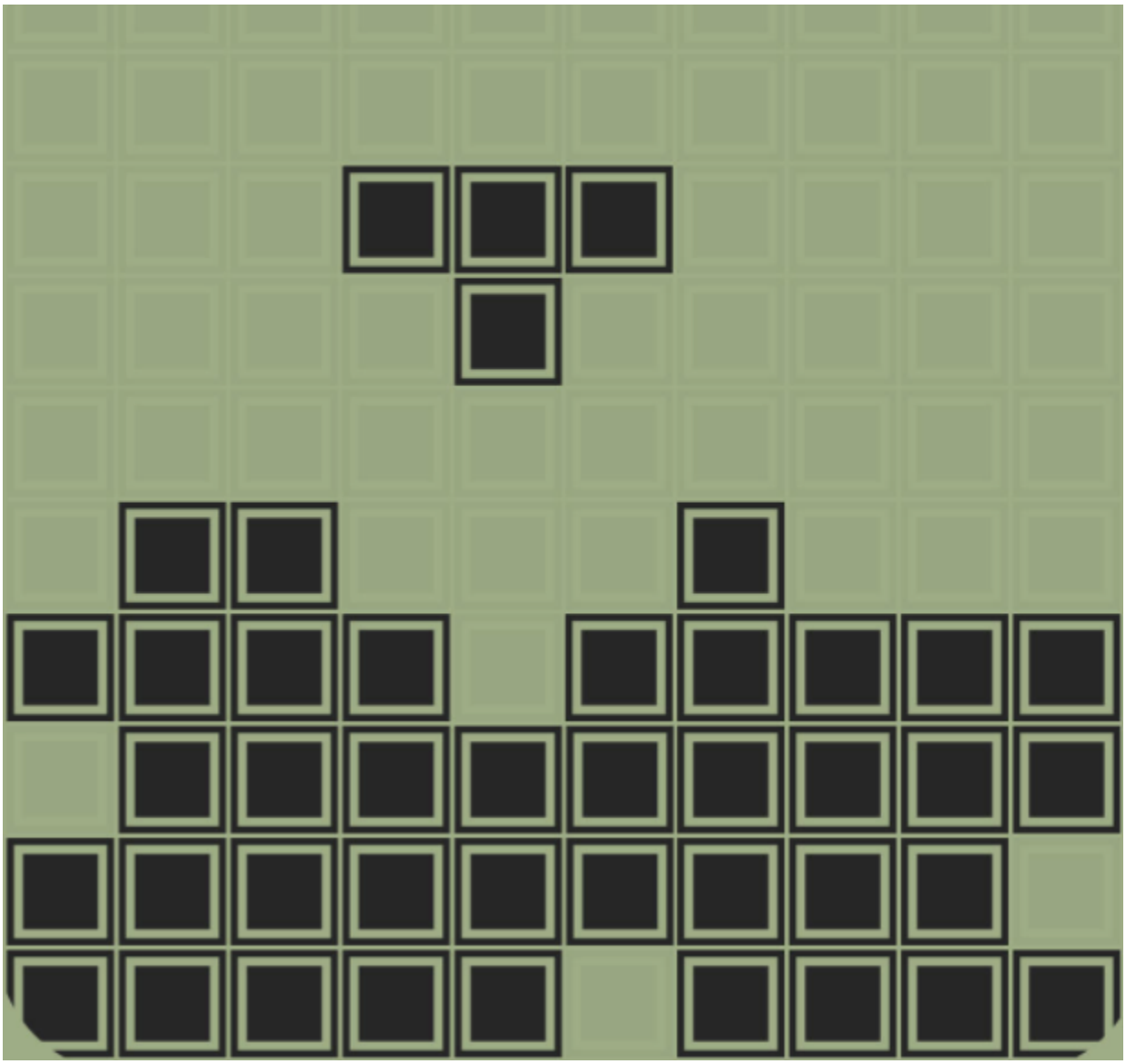
然而实战环境中，很多漏洞都不是一步就到位的，是通过不同的手法来进行组合，最后得到一个shell，哪怕是单纯的反序列化漏洞，一个反序列化的利用，可能还需要绕过流量waf，然后之后可能又遇到一个不出网的场景或者没有命令执行回显的场景。

这个时候，单点的线性思维失去了作用，需要使用其他的思维模式，也就是多种手法进行组合的思维，才能真正达到目的。

0x02 积木思维的基础

俄罗斯方块是有很多块的，很多不同的块。

不同的块叠在一起，看似没有规律，但是实际上最终只要填满了就可以消除。



这一点其实和打红队是一样的，不同的漏洞组合，不管是什么漏洞，只要最终符合要求，就能达到最后的目的，从而获取shell。

这里还是拿俄罗斯方块来举例子，因为大家都会这个游戏。

俄罗斯方块的训练方法其实也是循序渐进的

- **刚开始的时候，也别看啥攻略，先玩几把来熟悉一下**

因为在从来没有接触过一个游戏的时候，直接上手就是最好的方法。

这个时候因为没有玩过这个游戏，所以看攻略啥的，都只能停留在对一个客观物体，也就是这个游戏的表面的理论认识上，无法真正理解这件事。

只要自己上手去玩两把，虽然玩得可能不好，但是通过玩了几把之后，就能在心中建立对这个物体的感性认识。

真正接触过，玩过，才能切实的理解。

红队也是这样，一开始什么站也没搞过，就先看一堆文章，其实人都是蒙的，看了马上就忘记。

- **玩过几把之后，去看看攻略，先研究整体的策略，把握全局**

建立起一定的感性认知之后，这个时候就会遇到问题。

为什么玩得时候我老是挂掉，为什么有些方块在这里放就不行，在那里放就可以，有时候我虽然知道在这里放可以，但是比较片面，也没有理论依据，只是玩了几把，死的太多了，积累的一个初步经验，知道在这里继续放一定会死，以后就不在这里放了。

此时心里会产生一定的经验和困惑，也就是产生了问题，同时因为想玩得更好，想解决阻碍自己玩得更好的这些问题，那么这个时候，就是看攻略的时候。

因为在心中没有问题的情况下，看攻略是没有任何意义的，就算看了，获取的知识只能停留在纸面的基础上，不能作用于实际的问题上，因为你的心里没有问题，没有问题的原因是因为没有实战过，因此这也是为什么古人老是说，纸上得来终觉浅。

理论永远是用来指导实践的，而没有实践，单纯搞理论，很容易走上赵括的路子。

所以这里才使用了这样一个次序。

而在看攻略的时候，初期一定要把全局观把握好。

这里举一个反例，我们都知道俄罗斯方块有很多块，如果一个人一上来先研究一个问题，就是长条块怎么摆，然后读一大堆资料，看一大堆视频，这个时候基本就会放弃，因为他会陷入迷茫。

因为俄罗斯方块不止一种块，有很多种块，在没有建立全局观得前提下单纯得研究一种块，他的实战场景根本没有在心中建立。

也就是研究了很多，会让人产生一种没啥用的感觉，也不知道继续研究下去有什么意义。

这是大忌，也是很多人放弃做一件事的原因。

而建立了全局思维，就好比在搭建房子的时候，先把脚手架搭建好，然后再慢慢来做其他的事情，从来没有人建房子，是脚手架还没搭建好的时候，就开始给其中某一间屋子搞装修了，一个道理。

在全局思维还没建立起来的时候，对于一个事物的整体认知还没建立起来的时候，就过于专注于一个点，很容易把房子建塌。

在红队中也是，如果一开始整体攻防概念没有建立起来，先看xss，xss发现一开始看啥反射型，存储型，压根不知道啥玩意，然后发现javascript不会，又先从javascript看起，看了一堆语法语义，此时很多时间过去了，但是内心越来越想放弃，一方面感觉知识根本学不完，另一方面感觉这些东西学了屁用没有，这就很悲惨了。

- **全局思维建立起来之后，再返回去实战练习，然后不断往复看攻略和实战的过程，一个个弥补细节**

在整体的全局思维建立起来之后，此时已经知道俄罗斯方块怎么玩耍了，还能玩出一定的花样，但是水平，距离职业选手还有很大差距。

这个时候，其实自己弱在哪里，心里已经有数了，那么可以就自己的弱项，做针对性的弥补，然后去实战中检验是否有效，然后把反馈进一步强化，循环往复，水平就能够不断提升。

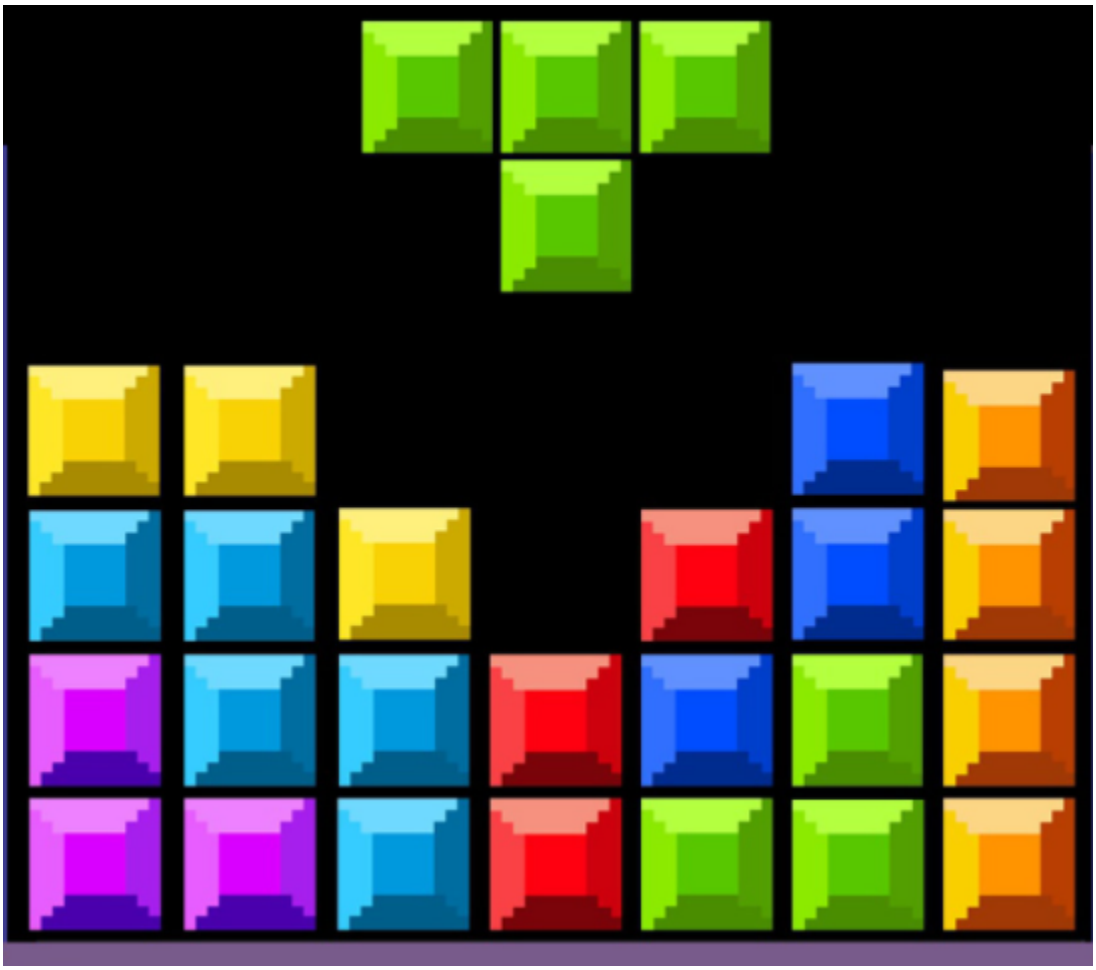
这一步，就好像建房子，把地基和脚手架搭建好之后，再逐层去施工，造毛胚房，一层层往上盖，不建空中楼阁，最终建成高楼大厦。

红队实战中也是，发现一个站日不下来，虽然这里有个sql注入点，但是sql注入的waf绕不过去，这个时候心里就知道自己弱在那里了，回头专门就waf继续研究，下次就不怕了。

上述是基本的训练阶段，在训练达到一定程度了，就到了连接阶段，也就是所谓的积木思维阶段。

0x02 积木思维的进阶

积木思维本质上就是连接思维，如下图所示：



要消除俄罗斯方块，可以用上面方块叠加，也可以用下面的方块叠加

这里可以把每一种方块抽象成一种漏洞，也就是说，不管什么漏洞，只要能够叠加在一起，然后最后能拿到shell，也就是类似于俄罗斯方块中的叠满消除，就能够达到我们的目的。

这里也就是所谓的漏洞连接，攻防中也叫组合漏洞。

这个思维是很重要的，要先放在心里，然后做刻意训练，不断地去强化，平常就要有意识的去组合各种漏洞。

这种思维主要是为了应对复杂的实战场景，也是攻防技术做到后期能不能往前提升的一个拦路虎。

组合的训练一方面需要阅读大量的历史数据，也就是别人是怎么组合漏洞来利用的，另一方面需要开阔自己的想象力，平常多看点科幻魔幻类的书籍，多看点其他学科的书籍，开阔自己的思路。

举一个例子 一套完整的外网打进内网的流程可能包括

外网上传-->上传绕过waf-->绕过waf之后文件找不到了-->发现存在cdn，文件传到cdn上去了-->找到真实ip进行上传-->上传之后webshell被杀了，需要免杀-->免杀完毕后成功上线，但是权限很低-->提权发现被360拦了→绕过360进行提权-->提权成功尝试横向→xxxxxx

这么多流程中，其实就是一层层的技术在累积木。

先需要对单点技术做突破，然后把每一个单点的技术连接起来，最后组合成一整套东西。

如果实在问还有什么窍门，那就是勤学苦练吧

done