红队攻防-外网快速打点方法&技巧总结

一、打点的基本认识

做过红队的小伙伴，对打点一定不陌生，这是一项基本技能。

所谓打点，就是拿到一台机器的shell。

打点的一般目的在于利用这台机器，做一个跳板，然后进入内网。

通常给予充分时间的情况下，打点不是一件很难的事情，因为系统总会有漏洞，就算系统没有漏洞，人也有漏洞，也可以进行钓鱼，甚至还可以近源，可以花钱买内鬼，一切都只是打点的时间和价格成本与打到点进内网的收益的核算问题，本质就是一道数学题。

但是以在公司干活的普通员工视角出发，一般项目时间很紧，同时外部资源少，基本能用的东西就是自己的技术。

对个体而言，这种条件下，个人技术成为了主导因素，也就是说，一个红队人员快速打点能力的强悍与否，成为了一个普通红队和优秀红队的差别所在。

当然，这里有人会讲，那么有的地方可以给很多时间，或者说自己在实战中，在搞别的站的时候，不是特定项目中，是有大把时间来进行渗透和攻击的，可以慢慢搞。

主流的ctf赛事解题时间也只有1-2天，很多攻防项目也就是一周时间，src中第一个挖到洞的才给钱，这是客观条件，对大家都是平等的。

项目就只有几天，这就是游戏规则，是没有道理可讲的，所以还是不要找理由了，因为也没啥用。

当然，从公司的角度出发，因为项目时间紧，而很大程度上，打点又是个体力活，不涉及太多技术，所以投入信息搜集的人越多，效果一般是更加好的。

总而言之，打点本身就是一种遍历行为，被攻击的目标就好像一个被围墙保护的城堡，红队要做的事情就是围着围墙转来转去，敲敲打打，看看围墙哪里没修好，哪里空了一块，然后趁机溜进去，这是一个体力劳动，尤其在面对很多目标的时候，是一项繁重的体力劳动，在下文中会详细解释为什么我反复强调这是一项体力劳动。

二、打点的基本方法

基本方法，无非就是信息搜集-->找到脆弱资产-->漏洞利用→getshell，说起来是很简单的。

这其中最肝的一个部分，莫过于信息搜集了，纯体力活。

当然，过程可以用工具相对优化，但我依旧认为是最无脑的一个部分，就像大学生和小学生（高阶和低阶技术人员）一起用计算器（各种工具 fofa goby oneforall等）来算1w道加减乘除题（大量的资产 域名子域名 c段等）一样，其实是区分不开技术人员的水平的，很多头部的公司早就认识到了这一点，于是在大型攻防演练中，通常是派大量的人来进行资产收集，然后筛选出其中的脆弱资产后把资产给后续的利用人员来进内网快速拿分。

虽然信息搜集很无脑，但是该说还是得说，这个事情一般有以下几个步骤。

1、当项目经理告诉了你攻击目标的时候 →得到公司名→上企查查搜公司名→搜出来一堆公司和子公司

2、拿到这堆公司和子公司的名字→oneforall来跑一遍→然后得到了一堆子域名

3、拿到这堆子域名丢给Eeyes跑一遍→得到对应子域名对应的ip和c段信息

4、将对应ip和c段丢给fofa和fscan→fofa能快速得到c段资产信息，fscan能快速扫一遍，顺便帮你打一下常用漏洞

5、如果你的运气足够好，这个时候fscan已经有漏洞爆出来了，可以直接去利用了（小概率事件），但是如果你的运气不好，就要看接下来的第6步

6、刚刚fofa得到的资产看一眼，这里可以配合ehole的指纹识别来帮助快速筛选，通过筛选敏感资产，例如shiro，fastjson等直接能够反序列化getshell的资产（小概率事件），如果你的运气好，那么这个时候已经有漏洞了，可以直接利用了，如果你的运气不好，就要看接下来的第7步

7、通过上面一番筛选，时间已经过去很久了，但是目前却毫无进展，其实心里有点郁闷，这个时候就不建议再搞了，先休息一下，调整下心态，不然后续的几天会大幅度降低工作效率，休息好了感觉又可以了，就看看下面的步骤8继续吧

8、其实经过上面的一番筛选，web这块的基本已经过完了，但是依旧还没有漏洞，说明这个系统平时自查搞的比较多，基本的高危漏洞修复已经完成了，如果是大型攻防演练，那就建议换个目标再用上面的方法轮一次，如果是就某家单位做的定向攻防，就继续看步骤9吧

9、web的过完了，虽然没有直接能够rce的系统，但是我们获得了很多形形色色的登录后台\用户登录\注册\管理员登录等等等等交互类型的资产，这些资产虽然看起来没用，但是我这里要介绍一下攻防演练的三板斧漏洞，运气好的话，这些资产还是能够派上用场的

三板斧其一 反序列化漏洞：这个不用多说，我最喜欢的漏洞，只要有了这个漏洞，基本一台机子的shell就拿到了，看到就眼睛放光，但是可遇不可求，遍地都是shiro的时代已经渐渐过去了。

三板斧其二 文件上传：这个也是老熟人了，一般我会先看看是不是白名单，是白名单的话，就看看有没有文件包含之类的漏洞能组合利用下，如果是黑名单，就把文件上传的姿势对着上传点全部来一遍，看看有没有一个能中，如果能中，那就有了一个shell（没路径连不上但是确实是shell），虽然找上传路径也是一个拦路虎，但是至少比传不上去强。

三板斧其三 sql注入：这个更加老熟人了，注入之后，低权限，直接gg，高权限，试试吧，看能不能上shell。

至于其他漏洞，攻防演练就那么几天时间，八成是用不上，建议直接放弃，就把上面三个玩精（仅仅就攻防项目来说）。

10、对各种登录系统尝试弱口令/sql注入攻击，弱口令能登进去后台就找上传点，sql注入建议xray+burp来测，看到有戏的再上sqlmap。

还有一些信息搜集的方法，比如fofa搜关键字，title="单位名"等，这种方法可以自行穿插灵活使用，有时候有奇效，有时候没啥效果，看个人造化了。

还有些天选之人，直接一个弱口令登云桌面（horizon、vdi等）然后拿shell的，这种属于天赐shell，不在常规考虑范围之内，但也可以尝试。

11、弱口令如果爆不出账号密码，就考虑上网盘\github\sgk\泄露公开库搜对应人员的信息，看看好使不

12、如果还是没有用，就可以开始看公众号\app\小程序的信息

13、如果还是没有用，就要开始用域传送\备案号\ip反查网站\ssl证书\用google来搜c段

14、如果还是没有用，就用dirmap\dirsearch来对可疑的网站进行目录爆破，看看好使不

15、如果还是没有用，还可以钓鱼，发邮件也是一个体力活

16、如果还是没有用，拿上设备跟领导申请近源渗透吧

列了这么多，我就是想说明，虽然信息搜集是一项很重要的工作，是开启后渗透的基础，但这项工作是体力活真的是不争的事实，因为他没有门槛，基本谁都能做，无非就是用工具对着一项项checklist不断的去尝试而已。

因此通常意义上的快速打点，就是比谁先试完所有的checklist，虽然目前绝大部分工作都是由工具来完成，整个项目呈一个半自动化的流程，但是仍然架不住资产量的庞大，一个信息收集熟练的人，无非也就是流水线的工人而已，对着巨量的资产不断的用工具筛选而已。

而一些高端打点技巧玩得好的人，例如电话钓鱼成功率很大的人，钓鱼邮件的撰写和钓鱼样本的开发做的很牛的人，在做这些事情之前，同样需要信息搜集，而能够玩高端技巧的人是不愿意来做信息搜集的，因为他们也是从小白阶段过来的，明白信息搜集这项繁重且技术含量低的工作完全可以找别人来做。

从公司层面上来讲，要快速打点，就要投入更多的人。从个人层面上来讲，要快速打点，要忍受枯燥的打点过程，然后提升自己的工具使用速度，最好自己能够进行二次开发，把一些半自动化的步骤连接起来，优化现有的步骤，从而进一步提升效率。

三、打点的技术区分线

很多时候，找到了一个脆弱资产，自己没利用成功，别人利用成功了，这是很普遍的现象。

这就来到了打点的区分线，也就是漏洞利用上。

利用不成功有很多的原因，比如一台机器明明出网，但是反弹shell怎么都弹不回来。

比如一台机器能够反弹shell，但是时不时就会断开。

比如一台机器能够写入一个内存马，也能够连接上，但是一旦下载或者上传一些较大的文件，就会失败。

比如一台机器，他能够执行命令，也能反弹shell，连接也稳定，但是执行特定的命令，就会失败。

这个时候，一个技术人员就脱离了苦力劳动的阶段，进入到了区分技术的时候了。

区分一项工作是苦力劳动还是技术活其实很简单，看是不是谁都能做就行了。

有的漏洞利用在实战中涉及了一些很原理的东西，对于渗透人员的基本功考察以及联想能力的考查是很强的，因此这个时候技术更好的人就可以凸显优势。

举一个稍微极端的例子，那就是ctf，做题是需要理解的，不会就是不会，多久都做不出来，信息搜集只要告诉了基本方法，基本都能做，只是熟练度有差别，信息搜集的效率有差别而已。

就技术人员个体而言，单纯做一个熟练工，是很容易被淘汰的，应当花更多时间在技术的深化上，建立自己的竞争壁垒。

技术的深化，代码能力是基础，进一步对各个系统和漏洞原理的理解，是延申，不断的学习和突破，最后技术就会越来越好，也就会脱离信息搜集的循环，迈入更高的层面。

不过做项目时候的信息搜集，那是公司项目，是不可避免的，公司花钱请人来就是干这个的。

技术栈的突破和延申，是自己的事情。

我觉得更优的解法就是先集中花一部分时间练习信息收集，然后配合自研的小工具把效率提上去，练到了一定程度，做项目的时候信息搜集基本都能出东西了，公司这边能跟客户交差了，再把时间花到漏洞的突破和延申上。

文章大体是讲思路，具体的技术细节，很多论坛上都有，这里不再赘述。

这里更大程度上，只是想把做一件事的动机以及如何权衡利弊做好一件事情的方法分享出来，大部分也是个人理解，难免会有错误，不足之处希望大家指正。