代码审计与编程在渗透中的重要性

博客连着断了一个月没更新，期间写过好几篇各个方向的文，都是写到一半就夭折，这篇文章强迫自己耐心写出来的。最近跟出版社沟通好了在写一本关于代码审计和安全编程的书，算是把我这几年的技术积累做一个总结，刚好昨天跟safekey team几个搞渗透的朋友说到编程的问题，就想写个文来好好讲讲。

这个文原想命名为《做个有创造力的海盗》，迎合一下刺（道哥）前段时间写的《我要找的是海盗》，在他的文章讲的找海盗一点上我的看法和做法跟他是一模一样的。至今我也只有一个身份证，高一错学，初中、小学毕业证应该也是找不到了，18 岁加入安全宝，所以我也没法对公司team成员有学历要求。另外在海盗这一点上，我的理解是有激情、有胆量、有智谋、有创造力的人，点到为止，留一个题目《创业路上的海盗军团》给海盗去思考吧，我要找的是有创造力的海盗。

仔细想了一下我还是有能力驾驭这个题目，我在高一就开始接触编程，到现在快 5 年的编程经验，渗透连着做了 4 年，国内外大大小小目标。代码安全审计也有两年多不断的积累。无数个通宵达旦搞技术研究。像余弦在TED的演讲上说他是一个有邪气的人一样，非纯粹的白帽子，我们俩有点类似，这是一个我不想丢掉的特质，怕丢掉了会失去创造力。如果有心可以翻翻我的blog，可以看到我这两年写的blog和安全软件基本都是带攻击性质，就像代码审计系统也是用来发现漏洞，可以说我不是一个单纯的技术爱好者。

首先抛出一个观点：代码审计和编程在渗透中有至关重要的作用。

这几年见过很多人，没有代码审计和编程能力做渗透都比较吃力，局限在用安全扫描做漏洞扫描以及利用网上公开的exp去攻击，也就是常说的脚本小子。即没有研究能力的攻击党，通常放出exp的人不可怕，可怕的是利用exp去批量攻击的人，这种人造成的危害最大。然而在攻击过程中，由于攻击对象的环境不一样，一个小小的问题也会导致攻击失败，这时候脚本小子的弱势就完美体现了，而有研究能力的攻击者（下面以文化流氓代称）能够分析攻击失败的原因，对exp进行改造以使攻击成功。这类的case见过很多，举两个例子。

情景一：

一个SQL注入漏洞(http://www.cnseay.com/?m=news&c=list&id=188)，因为目标网站存在waf（web application firewall），脚本小子使用自动化注入工具无法利用，通常会放弃这个漏洞。而文化流氓就不一样了，利用自己的SQL编程能力和对waf了解，通过提交不用的数据，根据server返回的数据信息、页面报错等来分析漏洞和waf的大致情况，最终会想出办法来绕过waf利用漏洞，成功入侵目标网站。类似的场景有代码、命令执行、XSS等等漏洞，扫描器在扫描出漏洞之后，都不会给出你能直接利用的exp，需要攻击者自己根据经验以及编程能力去分析构造利用脚本。

情景二：

这是一个在源码漏洞发现层次的场景，通过扫描器扫描到的一个源码包（http://www.cnseay.com/cnseay.rar），利用是该网站的程序源代码，通常攻击者都会利用源码包找一些配置文件一类，因为里面有数据库、api接口等等一类配置，如果环境有限制，如目标站数据库限制连接IP等，那么脚本小子可能

在源码包漏洞利用也就到此为止。换在文化流氓的手上就不一样了，他通过对源码包进行安全审计，发现网站目录下一个文件存在代码执行漏洞，于是通过该漏洞直接向网站服务器写入一个web后门，通过web后门提权得到服务器权限。

上面两个case可以很清楚的看到代码审计和编程在渗透中的重要性，多一种技能，也就多很多成功的机会。很简单的一个道理，给你一个漏洞，你也得要会用啊，不然给你有毛用。当然想要玩好代码审计也不是件简单的事，首页需要对编程语言足够的了解，起码要有代码阅读能力，另外还需要对各种漏洞进行深入理解，理解漏洞原理，即出现漏洞的原因以及利用和修复方法。