蜜罐

1.简介

蜜[罐](http://baike.baidu.com/item/%E7%BD%90" \t "http://baike.baidu.com/_blank)好比是情报收集系统。[蜜](http://baike.baidu.com/item/%E8%9C%9C/79956" \t "http://baike.baidu.com/_blank)罐好像是故意让人攻击的目标，引诱[黑客](http://baike.baidu.com/item/%E9%BB%91%E5%AE%A2/118396" \t "http://baike.baidu.com/_blank)前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器发动的最新的攻击和漏洞。还可以通过[窃听](http://baike.baidu.com/item/%E7%AA%83%E5%90%AC" \t "http://baike.baidu.com/_blank)黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络。

2.蜜罐的类型

(1)实系统蜜罐

实系统蜜罐是最真实的蜜罐，它运行着真实的系统，并且带着真实可入侵的漏洞，属于最危险的漏洞，但是它记录下的入侵信息往往是最真实的。这种蜜罐安装的系统一般都是最初的，没有任何SP补丁，或者打了低版本SP补丁，根据管理员需要，也可能补上了一些漏洞，只要值得研究的漏洞还存在即可。然后把蜜罐连接上网络，根据目前的网络扫描频繁度来看，这样的蜜罐很快就能吸引到目标并接受攻击，系统运行着的记录程序会记下入侵者的一举一动，但同时它也是最危险的，因为入侵者每一个入侵都会引起系统真实的反应，例如被[溢出](http://baike.baidu.com/item/%E6%BA%A2%E5%87%BA" \t "http://baike.baidu.com/_blank)、[渗透](http://baike.baidu.com/item/%E6%B8%97%E9%80%8F/9457427" \t "http://baike.baidu.com/_blank)、夺取权限等。

(2).伪系统蜜罐

什么叫伪系统呢?不要误解成“假的系统”，它也是建立在真实系统基础上的，但是它最大的特点就是“平台与漏洞非对称性”。

大家应该都知道，世界上操作系统不是只有Windows一家而已，在这个领域，还有[Linux](http://baike.baidu.com/item/Linux" \t "http://baike.baidu.com/_blank)、[Unix](http://baike.baidu.com/item/Unix" \t "http://baike.baidu.com/_blank)、OS2、[BeOS](http://baike.baidu.com/item/BeOS" \t "http://baike.baidu.com/_blank)等，它们的核心不同，因此会产生的漏洞缺陷也就不尽相同，简单的说，就是很少有能同时攻击几种系统的漏洞代码，也许你用LSASS溢出漏洞能拿到Windows的权限，但是用同样的手法去溢出Linux只能徒劳。根据这种特性，就产生了“伪系统蜜罐”，它利用一些工具程序强大的模仿能力，伪造出不属于自己平台的“漏洞”，入侵这样的“漏洞”，只能是在一个程序框架里打转，即使成功“渗透”，也仍然是程序制造的梦境——系统本来就没有让这种漏洞成立的条件，谈何“渗透”?实现一个“伪系统”并不困难，Windows平台下的一些[虚拟机](http://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E6%9C%BA" \t "http://baike.baidu.com/_blank)程序、Linux自身的脚本功能加上第三方工具就能轻松实现，甚至在Linux/Unix下还能实时由管理员产生一些根本不存在的“漏洞”，让入侵者自以为得逞的在里面瞎忙。实现跟踪记录也很容易，只要在后台开着相应的记录程序即可。

这种蜜罐的好处在于，它可以最大程度防止被入侵者破坏，也能模拟不存在的漏洞，甚至可以让一些Windows[蠕虫](http://baike.baidu.com/item/%E8%A0%95%E8%99%AB" \t "http://baike.baidu.com/_blank)攻击Linux——只要你模拟出符合条件的Windows特征!但是它也存在坏处，因为一个聪明的入侵者只要经过几个回合就会识破伪装，另者，编写脚本不是很简便的事情，除非那个管理员很有耐心或者十分悠闲。