**安全杂谈**

对当前蜜罐的一些简单的看法

首先是蜜罐的仿真，身为蜜罐的作用就是诱敌，针对攻击方就要”利而诱之“，“利而诱之”的关键是要摸准对方贪什么“利”。

常见的克隆方式 应用类（tomcat、outlook、ecshop、weblogic）、系统服务类（ssh、rdp、ftp）、数据库类（mysql、redis、mongoDB）、网络设备类（路由器、交换机）。以及最重要的动态克隆类，一般基本都是动态克隆，如果放到公网甚可能还需要定制化（曾经见过配置短信验证码功能的蜜罐）。

图形用户界面

中度可信度描述已自动生成

当然，现在蜜罐的检测手段也很多<https://github.com/Ghr07h/Heimdallr>，使用jsonp识别。访问蜜罐页面后，web页面会使用jsonp来获取其他网站信息且不收到同源策略影响。

关于jsonp可以参考文章，<https://www.cnblogs.com/ph4nt0mer/p/16538600.html>，<https://blog.csdn.net/a1598452168YY/article/details/127879262>。

关于引流

1. 正常业务引流跳转到蜜罐。
2. 互联网诱饵（github等网站）
3. 木马反制（蜜罐提供下载插件功能，不安装插件边无法使用蜜罐web功能）

至于部署位置一般是在内网中，或者内+外形式部署，现在已经有云的形式了，但还不是很清楚怎么部署。

关于溯源的话，一般市面上的蜜罐都会自动勾画出攻击者攻击路径和画像了，运气比较好碰到低级攻击者的话说不定也能获取到其社交账号信息，根据其社交信息所发布历史内容，溯源攻击者。比如ssh蜜罐，攻击者在尚不知道是蜜罐环境的前提下，会将蜜罐作为跳板机进行下一步的攻击，通常会将带有个人信息特征的工具上传到服务器上，在攻防演习中对溯源得分是很有帮助的。

一般来说，触发即告警，在公网环境中通常最多告警就是弱口令尝试，个人一般不是很关注，只有深入后的才是重点，通常逐个研判也要消耗一部分时间。当然也要提防”穿罐“的情况发生，因为之前发生过类似情况，现在很多企业都将蜜罐整套部署在dmz区域。这种个人不是很熟，暂时不往下表。

“利而诱之”，在攻防中就是“投其所好”，关键在于对攻击者的心理，仔细观察，认真研究分析，自己置身于攻击方的角度，想攻击方想要什么，求攻击者之所求，从而创建适销对路的蜜罐，以满足攻击者的需求。“利之”必致其至。