**13 蜜罐**

0x01什么是蜜罐

蜜罐是存在漏洞的，暴露在外网或者内网的一个虚假的机器，具有以下这些特征：

1. 其中重要的一点机器是虚假的，攻击者需要花费时间攻破。在这段时间内，系统管理员能够锁定攻击者同时保护真正的机器。
2. 能够学习攻击者针对该服务的攻击技巧和利用代码

3.一些蜜罐能够捕获恶意软件，利用代码等等，能够捕获攻击者的Oday,同时可以帮助逆向工程师通过分析捕获的恶意软件来提高自身系统的安全性

4.在内网中部署的蜜罐可以帮助你发现内网中其他机器可能存在的漏洞。

蜜罐是把双刃剑，如果不能正确的使用，有可能遭受更多的攻击，模拟服务的软件存在问题，也会产生新的漏洞。蜜罐分为几下几类：

1.低交互式：低交互式模拟常规的服务，服务存在漏洞，但是模拟的这些漏洞无法被利用，开发和维护这种类型的蜜罐比较容易。

2 .高交互式：高交互式使用的是真实的服务，有助于发现服务存在的新漏洞，同时能够记录所有的攻击，但是，部署困难、维护成本高，一旦服务上存在的漏洞被利用，容易引发新的安全问题。

3.粘性蜜罐(Tarpits):这种类型的蜜罐，使用新的IP来生成新的虚拟机，模拟存在服务的漏洞，来做诱饵。因此攻击者会花费长时间来攻击，就有足够的时间来处理攻击，同时锁定攻击者。

还有其他类型的蜜罐，比如专门捕获恶意软件的，数据库漏洞利用程序和垃圾邮件等等。当部署两个或者两个以上蜜罐时可以称之为蜜网。

0x02密罐HFISH安装

<https://hfish.io/docs>

0x03使用

<http://192.168.2.132:9001> admin admin