蜜罐系统的定义

**蜜罐**（英语：honeypot）是一个电脑术语，专指用来侦测或抵御未经授权操作或者是[黑客](https://zh.wikipedia.org/wiki/%E9%A7%AD%E5%AE%A2" \o "黑客)攻击的陷阱，因原理类似诱捕[昆虫](https://zh.wikipedia.org/wiki/%E6%98%86%E8%9F%B2)的蜜罐因而得名。

蜜罐系统类型

低交互：模拟服务和漏洞以便收集信息和恶意软件，但是攻击者无法和该系统进行交互；

中等交互：在一个特有的控制环境中模拟一个生产服务，允许攻击者的部分交互；

高交互：攻击者可以几乎自由的访问系统资源直至系统重新清除恢复。

商业蜜罐产品

KFSensor：windows服务器蜜罐

长亭科技-谛听内网感知系统：内网威胁感知及蜜罐欺骗

默安科技-幻盾：设置脆弱性陷阱，混淆黑客攻击目标，利用SDN技术转移黑客攻击路线到沙箱中， 隔离攻击同时在沙箱里记录黑客攻击行为，并还原攻击者真实身份。

其他公司及厂商：Cisco, HP, IBM, Intel Security，Symantec, Kaspersky Lab, Sophos，Shape Security，Attivo Networks，Cymmetria，TrapX，GuardiCore，TOPSpin Security，KFSensor、Specter，Canary

开源蜜罐

系统蜜罐

模拟多种服务的蜜罐

Honeyd ：Honeyd是一个小的防护程序，它能够产生虚拟的主机，这些主机能够被配置以提供任意的服务，系统特征也是与之相适应，以至于使之看起来像真实的系统在运行。在一个局域网的网络仿真中，Honeyd能够使单个主机拥有许多IP（多达65536个）。最后更新时间4年前。C语言编写。

安装方式：

<http://www.honeyd.org/>

https://github.com/DataSoft/Honeyd

<http://fergusj.blog.51cto.com/8835051/1567799>

<http://www.yjs001.cn/view/60076647473100190857.html>

<http://297020555.blog.51cto.com/1396304/538183/>

Dionaea：Dionaea是运行于Linux上的一个应用程序，将程序运行于网络环境下，它开放Internet上常见服务的默认端口，当有外来连接时，模拟正常服务给予反馈，同时记录下出入网络数据流。网络数据流经由检测模块检测后按类别进行处理，如果有 shellcode 则进行仿真执行；程序会自动下载 shellcode 中指定下载或后续攻击命令指定下载的恶意文件。从捕获数据到下载恶意文件，整个流程的信息都被保存到数据库中，留待分析或提交到第三方分析机构。低交互蜜罐。最后更新15天前。

安装方式：

<http://www.freebuf.com/articles/system/12696.html>

<https://github.com/DinoTools/dionaea>

<https://dionaea.readthedocs.io/en/latest/>

HoneyDrive 3：**HoneyDrive是一款Linux蜜罐系统，它是以虚拟设备（OVA）的方式安装在Xubuntu 12.04.4版本上面。**HoneyDrive系统里面包含了10款预装和预配置的蜜罐软件，如Kippo SSH honeypot、Dionaea、Amun malware honeypots、Honeyd low-interaction honeypot、Glastopf web honeypot、Wordpot、Conpot SCADA/ICS honeypot、Thug和PhoneyC honeyclients等，并且系统上面还提供了一些脚本和工具来分析数据，并且数据通过可视化的方式呈现。如Kippo-Graph, Honeyd-Viz, DionaeaF和ELK stack等。最后更新3年前

安装方式：

http://bruteforcelab.com/honeydrive

MHN：MHN是一个开源软件，它简化了蜜罐的部署，同时便于收集和统计蜜罐的数据。用ThreatStream（http://threatstream.github.io/mhn/）来部署，MHN使用开源蜜罐来收集数据，整理后保存在Mongodb中，收集到的信息也可以通过web接口来展示或者通过开发的API访问。它能够提供多种开源的蜜罐，可以通过web接口来添加他们。一个蜜罐的部署过程很简单，只需要粘贴，复制一些命令就可以完成部署，部署完成后，可以通过开源的协议hpfeeds来收集的信息。最后更新3个月前

安装方式：

https://github.com/threatstream/mhn

<http://wps2015.org/drops/drops/%E8%9C%9C%E7%BD%90%E7%BD%91%E7%BB%9C.html>

<https://kylingit.com/blog/%E5%85%B3%E4%BA%8E-mhn-%E7%9A%84%E4%B8%80%E4%BA%9B%E9%83%A8%E7%BD%B2%E4%BB%8B%E7%BB%8D/>

<https://itandsecuritystuffs.wordpress.com/2015/02/03/honeypot-networks/>

opencanary：一个在内部网络上运行低互动开源蜜罐。最后更新20天前。

安装方式：

<http://vinc.top/2016/06/30/centos%E4%B8%8B%E5%AE%89%E8%A3%85%E9%83%A8%E7%BD%B2opencanary%E8%9C%9C%E7%BD%90/>

https://opencanary.readthedocs.io/en/latest/

https://github.com/thinkst/opencanary

**Beeswarm：Beeswarm是一个主动蜜罐系统，通过部署一些模拟真实用户的节点与蜜罐系统通信，从而引诱窃听了这些会话的攻击者攻击蜜罐系统，以捕获发现攻击。最后更新5个月前**

安装方式：

<http://www.freebuf.com/sectool/122214.html>

<http://www.beeswarm-ids.org/>

<https://github.com/honeynet/beeswarm>

Artillery ：Artillery 是一个集成了蜜罐功能、监控功能和警报功能的系统

安装方式：https://github.com/BinaryDefense/artillery

没文档

DCEPT：DCEPT(代表Domain Controller Enticing Password Tripwire)是Dell SecureWorks的研究人员 开源的 一个探测网络入侵尝试和识别被入侵网络端点的蜜罐工具，采用GPLv3授权，DCEPT包含了三个组件：CEPT Generation Server, 为Active Directory创造唯一的密标凭证；DCEPT Agent, 运行在每个网络端点的内存中；DCEPT Sniffer，寻找匹配蜜罐用户名的被渗透端点源头。

安装方式

https://github.com/secureworks/dcept

没文档

自助搭建window版本的蜜罐

安装方式

<http://www.xfocus.net/articles/200307/564.html>

服务蜜罐

应用蜜罐，针对自己的应用部署的蜜罐系统。例如ssh蜜罐，web蜜罐，邮件服务，dns服务。

SSH蜜罐:

HonSSH，

<https://github.com/tnich/honssh>

<https://github.com/tnich/honssh/wiki>

https://github.com/tnich/honssh/wiki/Setup-using-single-static-machine

Kippo，

<https://github.com/desaster/kippo>

<https://www.haiyun.me/archives/centos-install-kippo.html>

Cowrie.

cowrie。它是一个中等的交互式蜜罐

<http://www.freebuf.com/articles/network/112065.html>

<https://github.com/micheloosterhof/cowrie>

web蜜罐：

GHH(Google hack honeypot)蜜罐。对于我们没多大意义。

<https://sourceforge.net/projects/ghh/>

<http://www.arkteam.net/?p=160>

<http://ghh.sourceforge.net/>

Glastopf

<https://github.com/mushorg/glastopf> 8月前

<https://github.com/mushorg/tanner> 最近

https://shadowd.zecure.org/overview/introduction/

https://github.com/dustyfresh/HoneyPress 7个月

DNS蜜罐： Ghost Phisher.BIND.DNSChef.

DNSChef。它可以运行一个功能完整的DNS服务，但是无法定制假的回复.监控DNS的放大型DDoS攻击。

Mail—我运行的是一个全特性的开源smtp中转，它能够保存经过它的所有电子邮件，但是并没有发送任何东西。对此我使用从后缀来的smtp-sink。

模拟SMTP服务的蜜罐BOF，对于攻击，它只会返回一个“503 Service Unavailable”

Spampot是一个基于分布式低交互蜜罐的垃圾邮件捕获系统

<https://github.com/shiva-spampot/shiva>

<https://github.com/msurguy/Honeypot> 邮件蜜罐

ElasticSearch Honeypot

https://github.com/jordan-wright/elastichoney

Struts蜜罐

https://github.com/Cymmetria/StrutsHoneypot

http://www.zoues.com/2017/03/25/strutshoneypot%EF%BC%9Astruts2%E7%9A%84%E8%9C%9C%E7%BD%90%E3%80%90zoues-com%E3%80%91/

https://github.com/glaslos/honeyprint 打印机蜜罐

https://github.com/citronneur/rdpy 远程桌面蜜罐

https://github.com/fygrave/honeyntp ntp服务蜜罐

https://github.com/omererdem/honeything 路由器蜜罐

http://bruteforcelab.com/kippo-graph kippo与数据展示

安装方式：

开源蜜罐优缺点

优点：

安装、部署比较容易，有文档

自定义或扩展成本低，在开源代码基础上改

缺点：

容易被shodan这种东西暴露了这是一个蜜罐

想法：

攻击是针对服务应用发动的。蜜罐就可以是针对服务应用部署的。

一种服务就可以有一种蜜罐。

Agent可以部署在多个不同的节点上，通过检测本地的ssh log，确定是否有破解行为，如果有破解密码行为且超过3次，就会通过remote api接口在docker server中启动一个新的容器，然后将攻击者的流量转发到这个容器中。

<https://github.com/LiGhT1EsS/kokkuri>

https://www.xsec.io/2017/2/14/docker-remote-api-sec-misc.html

商业蜜罐

网络层面的态势感知系统（跟交换机，路由器相关的安全分析系统），开源或商业的

一些蜜罐相关文章

利用渗透工具的特性或者问题，针对性返回恶意代码，实现渗透反杀

http://www.freebuf.com/articles/network/116922.html

针对安全人员以及运维人员的蜜罐

http://www.freebuf.com/sectool/116942.html

现在一些商业蜜罐的思路：网络安全监控系统跟蜜罐相结合

安全探针

http://www.freebuf.com/sectool/104901.html

蜜罐数据分析

http://www.freebuf.com/articles/web/126340.html

蜜罐设计思路

http://www.freebuf.com/articles/network/111155.html

智能蜜罐分析软件

https://nullsecure.org/introducing-the-tango-honeypot-intelligence-app/

https://github.com/aplura/Tango

使用docker自建蜜罐。

https://www.xsec.io/2017/2/14/docker-remote-api-sec-misc.html

docker 沙箱

https://github.com/LiGhT1EsS/kokkuri

蜜罐组合使用

http://www.lofter.com/tag/%E8%9C%9C%E7%BD%90

Wifi蜜罐：国外个人做的

http://www.freebuf.com/sectool/6162.html

mariadb 蜜罐并反杀

http://www.freebuf.com/sectool/128947.html

一个github开源honeypot列表，里面有各种类型的开源蜜罐项目。

https://github.com/paralax/awesome-honeypots