第一篇：蜜罐技术及最新进展

诸葛建伟

引言

自从 1988 年的莫里斯蠕虫席卷尚处于萌芽阶段的互联网并使之瘫痪以来，互联网就一直遭受着来自黑客攻击和恶意代码的双重威胁，随着黑客攻击和恶意代码技术的不断发展，新的安全威胁不断涌现，如分布式拒绝服务攻击、僵尸网络、网络钓鱼等，而防御技术却不能够跟上攻击技术发展的步伐，这使得互联网的安全状况日益恶化。究其根源，会发现攻击者与防御者之间在进行着一场不对称的博弈，而不对称性体现在双方需要付出的工作量、对对方信息的了解程度以及博弈失败面对的后果代价。

蜜罐技术的提出

蜜罐（Honeypot）技术就是为了扭转这种不对称局面而提出的，蜜罐定义为一种安全资源，它并没有任何业务上的用途，它的价值就是吸引攻击者对它进行非法的使用。蜜罐技术本质上是一种对攻击者进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务以及信息诱使攻击者对他们进行攻击，减少对实际系统所造成的安全威胁，并增加攻击者的工作量及提高攻击成功的难度；更重要的是蜜罐技术可以对攻击行为进行监控和分析，了解攻击者所使用的攻击工具和攻击方法，推测攻击者的意图和动机；并在此基础上尽可能地追踪攻击者的来源，对其攻击行为进行审计和取证，从而能够让防御者清晰地了解他们所面对的安全威胁，通过技术和管理手段来增强对实际系统的安全防护能力。

蜜罐技术发展简史

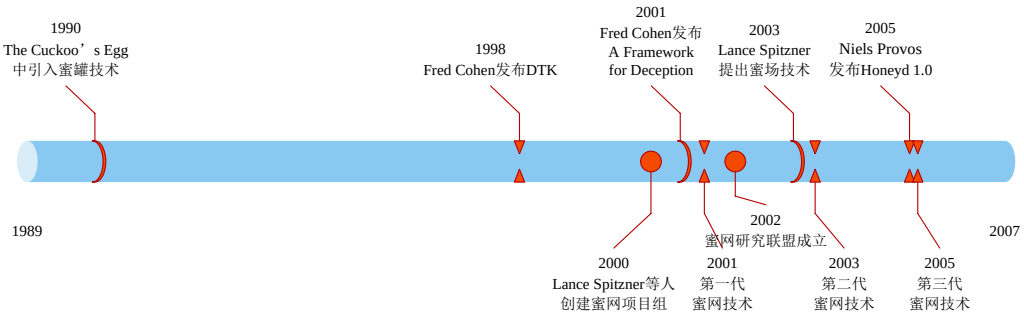

图 1 蜜罐技术发展历程图

蜜罐技术诞生于九十年代初期，最早出现在一本小说《The Cuckoo’s Egg》中，书中描述一个公司的网络管理员与入侵公司网络的商业间谍相互斗智的故事。从九十年代初蜜罐概念的提出直到 1998 年左右，蜜罐还仅仅限于一种思想，通常由网络管理员所应用，通过欺骗黑客达到追踪的目的。

从 1998 年开始，蜜罐技术开始吸引一些安全研究人员的注意，并开发出一些专门用于欺骗黑客的蜜罐工具，最为知名的由著名计算机安全专家 Fred Cohen（1983 年给出计算机病毒定义并证明了计算机病毒的存在）所开发的 DTK（欺骗工具包），Fred Cohen 还深入总结了自然界存在的欺骗实例、人类战争中的欺骗技巧和案例以及欺骗的认知学基础，分析了欺骗技术的本质，并在理论层次上给出了信息对抗领域欺骗技术的框架和模型，Fred Cohen 的研究工作也为蜜罐技术奠定了理论基础。

进入二十一世纪后，国外的一些安全公司开始看到蜜罐技术的实际应用价值，研发出了 KFSensor、Specter、ManTrap 等一些商业蜜罐产品。早期阶段的蜜罐技术和产品被称为虚拟蜜罐，即模拟成虚拟的操作系统和网络服务，对攻击者的攻击行为做出回应，增加攻击者的工作量，降低攻击者对实际系统的安全威胁，并对攻击行为进行监控。开源领域最为著名的虚拟蜜罐代表作是 Niels Provos 所开发的 Honeyd，和 Mwcollect.org 团队所开发的 Nepenthes。

由于虚拟蜜罐技术存在着交互程度低，较容易被攻击者识别等问题，2000 年由著名安全专家 Lance Spitzner 创建的 The Honeynet Project 蜜网项目组提出并倡导蜜网（Honeynet）技术，使用真实的主机、操作系统和应用程序搭建蜜罐系统，并且将蜜罐系统纳入到一个完整的网络体系中，提供强大的数据捕获、数据分析和数据控制功能，使得研究人员能够更方便地追踪侵入到蜜网中的攻击者，并对他们的攻击行为进行分析。

蜜网技术从概念证明性的第一代，经过逐渐成熟和完善的第二代，目前已步入较为完整、易部署、易维护的第三代，而各个研究团队通过部署蜜网捕获并深入剖析互联网最新安全威胁的实际案例也体现了蜜网技术的应用价值。

蜜罐技术分类及代表作

蜜罐技术分类

一种被普遍接受的蜜罐技术分类方法是根据蜜罐系统为攻击者提供的交互程度等级，划分为**低交互式蜜罐**和**高交互式蜜罐**。

低交互式蜜罐一般仅仅模拟操作系统和网络服务，较容易部署且风险较小，但攻击者在其中能够进行的攻击活动非常有限，因此我们能够收集的信息比较少，同时由于低交互式蜜罐通常是模拟的虚拟蜜罐，或多或少存在着一些容易被黑客所识别的指纹信息。

高交互式蜜罐则完全提供真实的操作系统和网络服务，没有任何的模拟，从攻击者角度上看，完全是其垂涎已久的“活靶子”，因此在高交互型蜜罐中，我们能够获得更多的攻击活动信息。高交互型蜜罐在提升攻击者活动自由度的同时，自然地加大了部署维护的复杂度和安全风险。

低交互式蜜罐代表作

低交互式蜜罐的代表作是开源的Honeyd软件和由KeyFocus公司出品的KFSensor产品。**Honeyd** 是一款非常优秀的**开源虚拟蜜罐软件**，由 Google 公司安全专家 Niels Provos 于 2003 年开始研发，2005 年发布 v1.0 正式版，目前已发布了 v1.5c。Honeyd 被设计成一个可扩展的虚拟蜜罐框架，支持直接路由、ARP 欺骗和网络隧道等模式接收网络攻击流，并能够通过可扩展的服务模拟脚本、灵活的配置文件模拟出复杂的虚拟蜜罐主机及网络，在构建反馈欺骗数据包时，利用个性化引擎使得数据包符合所模拟操作系统的特征，从而达到以假乱真的效果。但作为一款以研究应用为目标的开源软件，Honeyd 配置的复杂性和较差的易用性使其目标用户局限于安全研究人员和具有一定技术水平的安全管理员。（关于 Honeyd 的进一步详细信息，可参考北京大学狩猎女神项目组的技术讲义资料－“虚拟蜜罐软件Honeyd(v1.0)简介、安装与使用文档”，和 honeyd 官方网站 http://www.honeyd.org/）

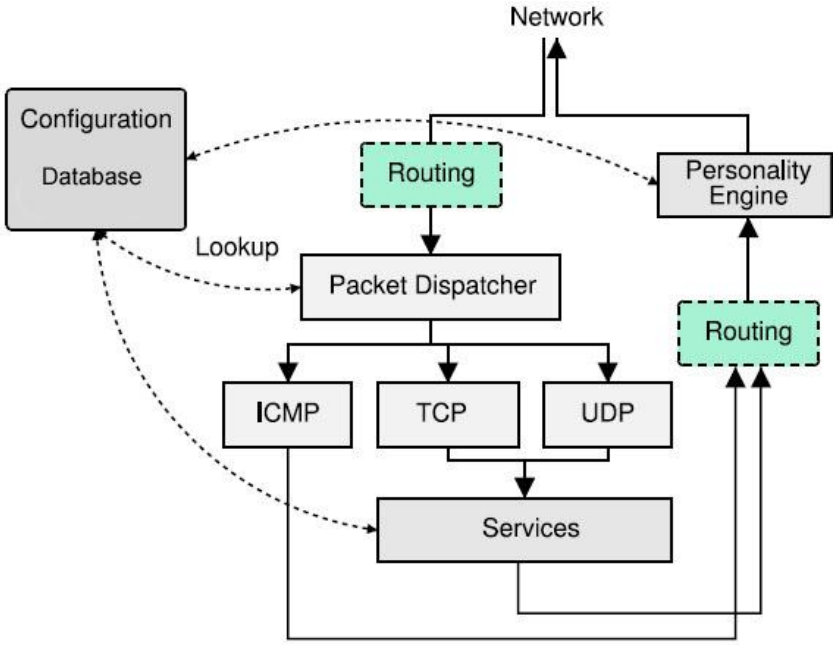

图 2 Honeyd 软件体系结构图

KFSensor 是一款 **Windows 平台上的虚拟蜜罐软件**产品，支持模拟 TCP、UDP、ICMP 协议，以及属于 Windows 工作站、服务器、互联网服务、Linux、木马和蠕虫后门服务等分类的多种网络应用服务，对黑客攻击和恶意代码进行诱骗和监测分析。（关于 Honeyd 的进一步详细信息，可参考北京大学狩猎女神项目组的技术讲义资料－“KFSensor 虚拟蜜罐的安装和使用”，和 KFSensor 官方网站 http://www.keyfocus.net/kfsensor/）

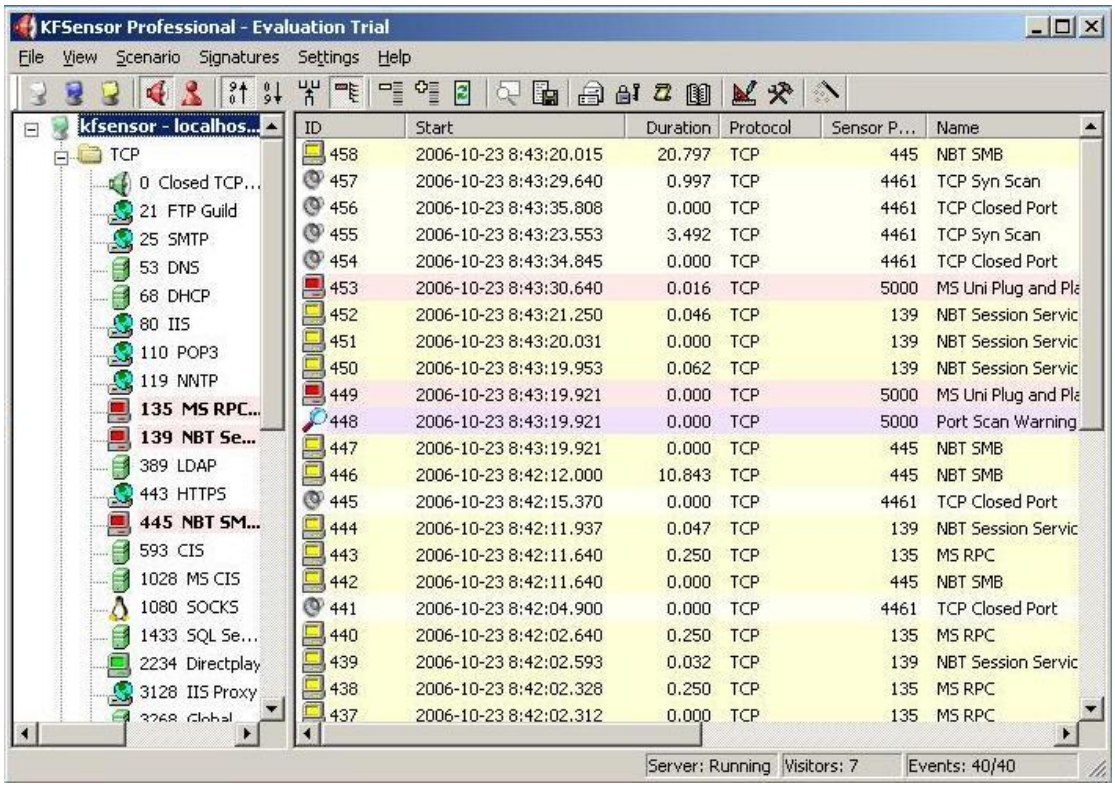

图 3 KFSensor 软件界面图

高交互式蜜罐代表作

高交互式蜜罐技术的代表作是 The Honeynet Project 研发的**第三代蜜网**体系，第三代蜜网技术的整体体系结构如图 5 所示，其中最为关键的部件是以桥接模式部署的蜜网网关（HoneyWall），蜜网网关包括三个网络接口，其中 eth0 连接外网，eth1 连接蜜网，两个接口以桥接方式连接，所有流入流出蜜网的网络流量都将通过这一桥接链路，接受蜜网网关的控制和审计。蜜网网关的另一网络接口 eth2 连接日志服务器，使得 HoneyWall 捕获的数据能够发往日志服务器，供安全研究人员进行进一步深入分析。

蜜网体系结构实现了三大关键功能：即**数据控制、数据捕获和数据分析**。数据控制是对攻击者在蜜网中对第三方发起的攻击行为进行限制的机制，用以降低部署蜜网所带来的安全风险。数据捕获，即监控和记录攻击者在蜜网内的所有行为，最大的挑战在于要搜集尽可能多的数据，而又不被攻击者所察觉。数据分析则是对捕获到的攻击数据进行整理和融合，以辅助安全专家从中分析出这些数据背后蕴涵的攻击工具、方法、技术和动机。（关于第三代蜜网的进一步详细信息，可参考北京大学狩猎女神项目组的技术讲义资料－“在 Win32 平台上基于 VMware 软件部署并测试第三代虚拟蜜网”，和 The Honeynet Project 官方网站 http://www.honeynet.org/）

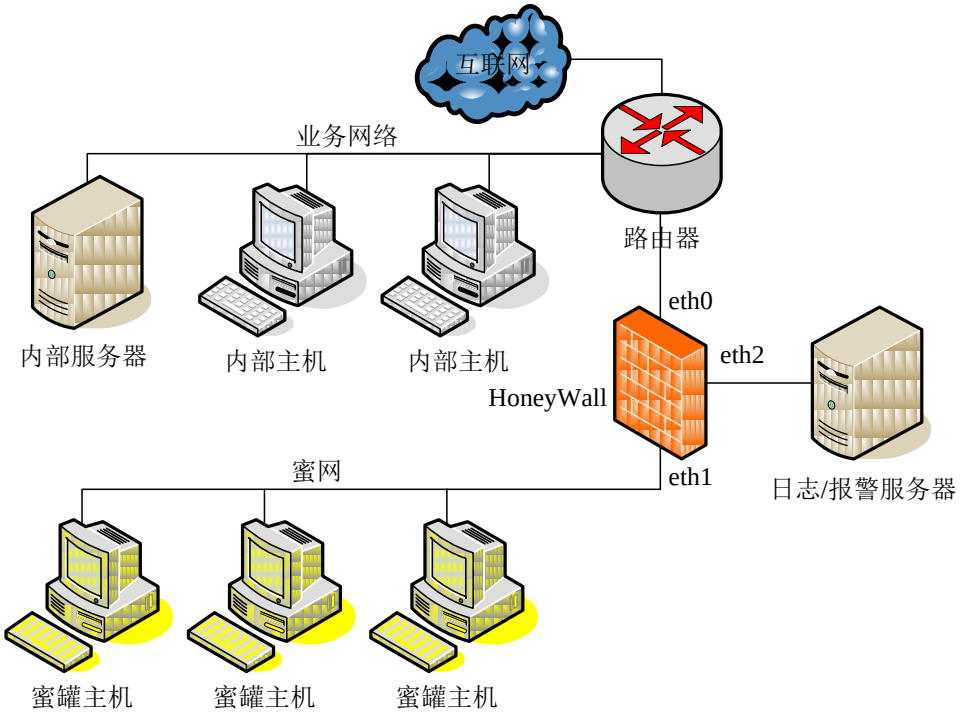

图 4 第三代蜜网体系结构图

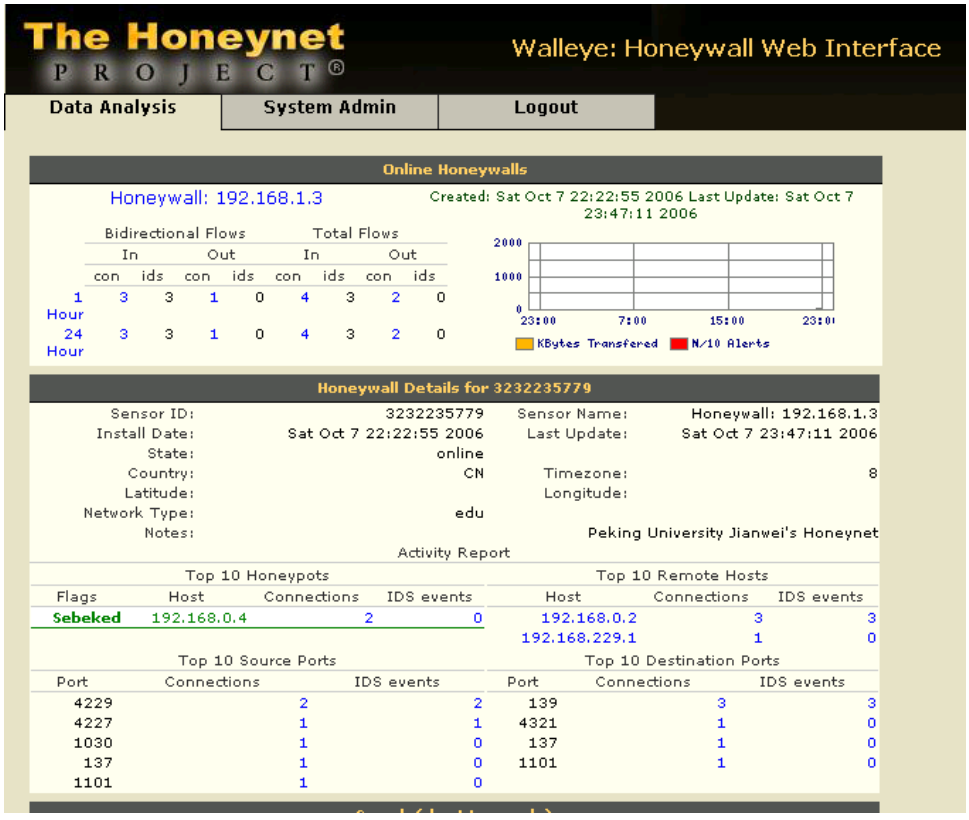

图 5 蜜网网关 Walleye 分析界面对网络渗透攻击的摘要视图

蜜罐技术的应用

蜜罐技术的应用途径包括**监测并研究安全威胁**，以及**为网络提供安全保护**两个主要方面。以前者为应用目的的蜜罐可被称为**研究型蜜罐**，通过在互联网或关键内部网络中部署研究型蜜罐，可以对实际的黑客攻击案例和恶意代码进行有效的捕获、追踪和分析，了解最新的黑客攻击方法和技巧，对最新爆发的恶意代码事件进行及时预警，从而支持安全研究人员、应急响应部门和网络防御者深入了解互联网和关键内部网络所面临的安全威胁，并进行及时有效地应对。

以提供安全防护为应用目的的蜜罐被称为**产品型蜜罐**，目前国外安全公司所研发的蜜罐产品均属于这一范畴，它们能够为一个组织的网络提供安全保护，包括检测攻击、隐藏真实业务服务、帮助管理员了解内部网络安全威胁并做出及时正确的响应等。但目前由于蜜罐技术对用户技术能力需要较高，安全检测覆盖面较窄等因素，产品型蜜罐还未得到网络安全市场的广泛接受。

蜜罐技术最新发展与趋势

蜜罐作为一种新兴的攻击欺骗技术，近年来在安全研究领域和开源领域中得到了不断的拓广和进一步发展，主要的三个发展趋势为：

(1) 从蜜罐系统的部署和组织体系结构上，蜜罐技术的发展趋势为**“蜜罐(Honeypot)→蜜网(Honeynet)→分布式蜜网(Distributed Honeynet)→蜜场(Honeyfarm)”**。

为了使得蜜罐能够更加全面地监测互联网和关键网络上实际安全威胁，就不可避免地要扩大蜜罐系统的部署范围：蜜罐技术发展早期的蜜罐系统基本上采用单点部署的方式；蜜网技术的提出使得安全研究人员可以在一个蜜网体系中融合多个多种不同类型的蜜罐系统，并结合数据控制、数据捕获和数据分析等机制进行高效地安全威胁监测与分析；而为了能够应用蜜罐技术构建跨网段和跨地域的网络安全监测基础设施，研究者在蜜网技术基础上进一步提出和构建了分布式蜜网体系，通过分布式安全威胁的监测和对监测数据的融合分析，从而能够有效地对大规模传播恶意代码和影响面较广的安全事件进行有效预警和响应；蜜场技术提供了将蜜罐技术用于直接防护大规模业务网络，并对安全威胁进行深入分析的一种应用途径，即在安全操作中心（SOC: Security Operations Center）中部署蜜罐，在各个内部子网或关键主机上设置一系列的重定向器（Redirector），若检测到当前的网络数据流或系统活动是攻击者所发起时，则将蜜场中的某台蜜罐动态配置成与目标主机相似的环境，并通过重定向器将攻击者流量重定向到这台蜜罐上，并由蜜场中部署的一系列数据捕获和数据分析工具对攻击行为进行收集、分析和记录。蜜场模型与分布式蜜网的差异在于将蜜罐系统在 SOC 集中式部署，安全专业研究和管理人员进行部署、维护和管理，可以形成一套规范化攻击捕获、分析和控制流程，从而更适合将蜜罐技术应用于网络安全防护的应用需求。

(2) 为了适应目前应用层安全威胁已经超过传统的网络层安全威胁，从而占据主要地位的现状，蜜罐技术的另一个发展趋势是**研究重心从传统网络层蜜罐逐渐向应用层蜜罐转移**。

应用层蜜罐技术通过部署网络应用层上的蜜罐网络服务或主机中的蜜罐应用程序，如蜜罐网站，蜜罐 SMTP 邮件服务器等，能够针对某些特定的应用层安全威胁（如针对网站的

攻击、使用开放的 SMTP 邮件服务器发送垃圾邮件），对攻击者更具诱惑力和欺骗性，并且能够获取到攻击者更详细的信息，从而更加深入的剖析这些安全威胁。

(3) 互联网安全威胁变化的另一个趋势是新兴的针对客户端的安全威胁，如网站挂马、垃圾邮件、网络钓鱼、僵尸网络等，也逐渐超过传统的针对服务端的安全威胁，如渗透攻击、拒绝服务攻击，占据主流位置。为了适应这一变化，研究者也已经提出**客户端蜜罐技术**并进行不断地深入研究，如邮件客户端蜜罐工具能够在一个可控的环境中通过打开病毒邮件的附件、访问垃圾邮件中的网络链接等方式激活病毒、访问恶意网站和钓鱼网站，并对整个过程进行详细的记录和深入的分析，从而获取病毒样本以及找到恶意网站和钓鱼网站。僵尸网络蜜罐工具则冒充僵尸网络中被控制的一个僵尸程序混入其中，对僵尸网络的情况、攻击者对僵尸网络的控制指令等进行详细地记录，并挖掘出被僵尸网络控制的僵尸主机以及背后操纵的攻击者，上演网络攻防对抗中的“无间道”。

结束语

随着蜜罐技术的不断发展和成熟，相信在一定程度上能够扭转攻击者和防御者之间的不对称局面，让攻击者成功攻击所需要付出的工作量更大，所需具备的技术能力更高，同时让防御者能够对攻击者的来源、方法和意图有更深入的了解，并且能够通过一定的手段追究攻击者的责任，从而对攻击者造成威慑作用。“路漫漫其修远兮，吾将上下而求索”，我们（北京大学计算机所狩猎女神项目组）正在路上，也邀您同行。