蜜罐及蜜网技术简介

Introduction to Honeypot and Honeynet

北大计算机科学技术研究所
信息安全工程研究中心
诸葛建伟，2004-10-15

Abstract

The purpose of this paper is to overview the honeypot and honeynet technologies, including the concept, history, present and future. The most well known and applicable honeynet – Gen2 honeynet framework developed by The Honeynet Project is introduced. Furthermore, the emerging research directions in this area are presented.

摘要

本文给出了对蜜罐及蜜网技术的综述报告，包括蜜罐和蜜网的基本概念、发展历程、核心功能，并介绍了目前最为成熟的“蜜网项目组”推出的第二代蜜网架构。此外本文还给出了蜜罐及蜜网技术的进一步研究方向。

关键字

网络攻击；蜜罐；蜜网；诱捕网络

1 问题的提出

众所周知，目前的互联网安全面临着巨大的考验。美国 CERT（计算机应急

响应组）统计的安全事件数量以每年翻番的惊人指数级增长，在 2003 年已经达到了 137,529 次。

导致互联网目前如此糟糕的安全状况的原因有很多，一方面是由于互联网的开放性和各种操作系统、软件的缺省安装配置存在很多安全漏洞和缺陷，同时，大部分的网络使用者还未真正拥有安全意识，也还很少进行安全加强工作，如及时打补丁、安装防火墙和其他安全工具等，从而导致了目前的互联网具有巨大的安全隐患。另一方面，随着网络攻击技术的发展，特别是分布式拒绝服务攻击、跳板（Step-stone）攻击及互联网蠕虫的盛行，互联网上的每一台主机都已经成为攻击的目标。此外，黑客社团也不像互联网早期那么纯洁，不再仅仅为了兴趣和炫耀能力而出动，而更多的由于国家利益、商业利益及黑暗心理等因素促使其对互联网安全构成危害。同时攻击者也不再需要很多的专业技术和技巧，他们可以很方便地从互联网上找到所需的最新攻击脚本和工具（如 PacketStorm 网站）。而这些由高级黑客们开发的攻击脚本和工具越来越容易使用，功能也越来越强，能够造成的破坏也越来越大。特别值得注意的一个趋势是多种攻击脚本和工具的融合，如大量的内核后门工具包（Rootkit），及能够集成多种攻击脚本并提供易用接口的攻击框架（如在 2004 年 DEFCON 黑客大会中引起广泛关注的 Metasploit）的出现。

针对如此严重的安全威胁，而我们却仍然对黑客社团所知甚少。当网络被攻陷破坏后，我们甚至还不知道对手是谁（黑客、脚本小子还是蠕虫？），对他们使用了哪些工具、以何种方式达成攻击目标，以及为什么进行攻击更是一无所知。

“知己知彼，百战不殆”，安全防护工作者，无论是安全研究人员、安全产品研发人员、安全管理人员和安全响应服务人员，都需要首先对黑客社团有深入的了解，包括他们所掌握的攻击技术、技巧和战术、甚至心理和习惯等。只有在充分了解对手的前提下，我们才能更有效地维护互联网安全。而蜜罐和蜜网技术为捕获黑客的攻击行为，并深入分析黑客提供了基础。

2 蜜罐

2.1 蜜罐的概念和发展历程

“蜜罐”这一概念最初出现在 1990 年出版的一本小说《The Cuckoo’s Egg》中，在这本小说中描述了作者作为一个公司的网络管理员，如何追踪并发现一起商业间谍案的故事。“蜜网项目组”（The Honeynet Project）的创始人 Lance Spitzner 给出了对蜜罐的权威定义[1]：蜜罐是一种安全资源，其价值在于被扫描、攻击和攻陷。这个定义表明蜜罐并无其他实际作用，因此所有流入/流出蜜罐的网络流量都可能预示了扫描、攻击和攻陷。而蜜罐的核心价值就在于对这些攻击活动进行监视、检测和分析。

蜜罐技术的发展历程可以分为以下三个阶段。

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，通常由网络管理人员应用，通过欺骗黑客达到追踪的目的。这一阶段的蜜罐实质上是一些真正被黑客所攻击的主机和系统。

从 1998 年开始，蜜罐技术开始吸引了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开源工具，如 Fred Cohen 所开发的 DTK（欺骗工具包）、Niels Provos 开发的 Honeyd 等，同时也出现了像 KFSensor、Specter 等一些商业蜜罐产品。这一阶段的蜜罐可以称为是虚拟蜜罐，即开发的这些蜜罐工具能够模拟成虚拟的操作系统和网络服务，并对黑客的攻击行为做出回应，从而欺骗黑客。虚拟蜜罐工具的出现也使得部署蜜罐也变得比较方便。

但是由于虚拟蜜罐工具存在着交互程度低，较容易被黑客识别等问题，从 2000 年之后，安全研究人员更倾向于使用真实的主机、操作系统和应用程序搭建蜜罐，但与之前不同的是，融入了更强大的数据捕获、数据分析和数据控制的工具，并且将蜜罐纳入到一个完整的蜜网体系中，使得研究人员能够更方便地追踪侵入到蜜网中的黑客并对他们的攻击行为进行分析。

2.2 蜜罐的分类

蜜罐可以按照其部署目的分为产品型蜜罐和研究型蜜罐两类，产品型蜜罐的目的在于为一个组织的网络提供安全保护，包括检测攻击、防止攻击造成破坏及帮助管理员对攻击做出及时正确的响应等功能。一般产品型蜜罐较容易部署，而且不需要管理员投入大量的工作。较具代表性的产品型蜜罐包括 DTK、honeyd 等开源工具和 KFSensor、ManTraq 等一系列的商业产品。研究型蜜罐则是专门用于对黑客攻击的捕获和分析，通过部署研究型蜜罐，对黑客攻击进行追踪和分析，能够捕获黑客的键击记录，了解到黑客所使用的攻击工具及攻击方法，甚至能够监听到黑客之间的交谈，从而掌握他们的心理状态等信息。研究型蜜罐需要研究人员投入大量的时间和精力进行攻击监视和分析工作，具有代表性的工具是“蜜网项目组” [2]所推出的第二代蜜网技术[3]。

蜜罐还可以按照其交互度的等级划分为低交互蜜罐和高交互蜜罐，交互度反应了黑客在蜜罐上进行攻击活动的自由度。低交互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，但黑客在低交互蜜罐中能够进行的攻击活动较为有限，因此通过低交互蜜罐能够收集的信息也比较有限，同时由于低交互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（Fingerprinting）信息。产品型蜜罐一般属于低交互蜜罐。高交互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，从黑客角度上看，高交互蜜罐完全是其垂涎已久的“活靶子”，因此在高交互蜜罐中，我们能够获得许多黑客攻击的信息。高交互蜜罐在提升黑客活动自由度的同时，自然地加大了部署和维护的复杂度及风险的扩大。研究型蜜罐一般都属于高交互蜜罐，也有部分蜜罐产品，如 ManTrap，属于高交互蜜罐。

2.3 蜜罐的优缺点

蜜罐技术的优点包括：

- 收集数据的保真度，由于蜜罐不提供任何实际的作用，因此其收集到的数据很少，同时收集到的数据很大可能就是由于黑客攻击造成的，蜜罐不依赖于任何复杂的检测技术等，因此减少了漏报率和误报率。

- 使用蜜罐技术能够收集到新的攻击工具和攻击方法，而不像目前的大部分入侵检测系统只能根据特征匹配的方法检测到已知的攻击。
- 蜜罐技术不需要强大的资源支持，可以使用一些低成本的设备构建蜜罐，不需要大量的资金投入。
- 相对入侵检测等其他技术，蜜罐技术比较简单，使得网络管理人员能够比较容易地掌握黑客攻击的一些知识。

蜜罐技术也存在着一些缺陷，主要有

- 需要较多的时间和精力投入。
- 蜜罐技术只能对针对蜜罐的攻击行为进行监视和分析，其视图较为有限，不像入侵检测系统能够通过旁路侦听等技术对整个网络进行监控。
- 蜜罐技术不能直接防护有漏洞的信息系统。
- 部署蜜罐会带来一定的安全风险。

部署蜜罐所带来的安全风险主要有蜜罐可能被黑客识别和黑客把蜜罐作为跳板从而对第三方发起攻击。一旦黑客识别出蜜罐后，他将可能通知黑客社团，从而避开蜜罐，甚至他会向蜜罐提供错误和虚假的数据，从而误导安全防护和研究人员。防止蜜罐被识别的解决方法是尽量消除蜜罐的指纹，并使得蜜罐与真实的漏洞主机毫无差异。蜜罐隐藏技术和黑客对蜜罐的识别技术（Anti-Honeypot）之间相当于一个博弈问题，总是在相互竞争中共同发展。另外，蜜罐技术的初衷即是让黑客攻破蜜罐并获得蜜罐的控制权限，并跟踪其攻破蜜罐、在蜜罐潜伏等攻击行为，但我们必须防止黑客利用蜜罐作为跳板对第三方网络发起攻击。为了确保黑客活动不对外构成威胁，必须引入多个层次的数据控制措施，必要的时候需要研究人员的人工干预。

3 蜜网

3.1 蜜网的基本概念

蜜网是在蜜罐技术上逐步发展起来的一个新的概念，又可成为诱捕网络。蜜网技术实质上还是一类研究型的高交互蜜罐技术，其主要目的是收集黑客的攻击

信息。但与传统蜜罐技术的差异在于，蜜网构成了一个黑客诱捕网络体系架构，在这个架构中，我们可以包含一个或多个蜜罐，同时保证了网络的高度可控性，以及提供多种工具以方便对攻击信息的采集和分析。

此外，虚拟蜜网通过应用虚拟操作系统软件（如 VMWare 和 User Mode Linux 等）使得我们可以在单一的主机上实现整个蜜网的体系架构。虚拟蜜网的引入使得架设蜜网的代价大幅降低，也较容易部署和管理，但同时也带来了更大的风险，黑客有可能识别出虚拟操作系统软件的指纹，也可能攻破虚拟操作系统软件从而获得对整个虚拟蜜网的控制权。

3.2 蜜网的核心需求

蜜网有着三大核心需求：即数据控制、数据捕获和数据分析。通过数据控制能够确保黑客不能利用蜜网危害第三方网络的安全，以减轻蜜网架设的风险；数据捕获技术能够检测并审计黑客攻击的所有行为数据；而数据分析技术则帮助安全研究人员从捕获的数据中分析出黑客的具体活动、使用工具及其意图。以下结合“蜜网项目组” [2]及其推出的第二代蜜网技术方案[3]对蜜网的核心需求进行分析。

3.3 “蜜网项目组”及第二代蜜网技术

“蜜网项目组” [2]是一个非赢利性的研究组织，其目标为学习黑客社团所使用的工具、战术和动机，并将这些学习到的信息共享给安全防护人员。“蜜网项目组”前身为1999年由Lance Spitzner等人发起的一个非正式的蜜网技术邮件组，到 2000 年 6 月，此邮件组演化成“蜜网项目组”，开展对蜜网技术的研究。为了联合和协调各国的蜜网研究组织共同对黑客社团的攻击进行追踪和学习，2002 年 1 月成立了“蜜网研究联盟”（Honeynet Research Alliance），到 2002 年 12 月为止，该联盟已经拥有了 10 个来自不同国家的研究组织。联盟目前的执行委员会主席为来自 Sun 公司的 Lance Spitzner。

“蜜网项目组”目前的规划分为四个阶段，第一个阶段即 1999 年－2001 年，主要针对蜜网技术进行一些原理证明性（Proof of Concept）的实验，提出了第一代蜜网架构；第二阶段从 2001 年到 2003 年，对蜜网技术进行发展，并提出了第

二代蜜网架构[3]，开发了其中的关键工具－HoneyWall 和 Sebek。第三阶段从 2003 年到 2004 年，其任务着重于将所有相关的数据控制和数据捕获工具集成到一张自启动的光盘中，使得比较容易地部署第二代蜜网，并规范化所搜集到的攻击信息格式。第四阶段从 2004 年到 2005 年，主要目标为将各个部署的蜜网项目所采集到的黑客攻击信息汇总到一个中央管理系统中，并提供容易使用的人机交互界面，使得研究人员能够比较容易地分析黑客攻击信息，并从中获得一些价值。

目前“蜜网项目组”已经完成了前三阶段的任务，即已经开发出较为完善的第二代蜜网架构，并以一张可启动光盘的形式提供部署和维护第二代蜜网所需的关键工具：HoneyWall 和 Sebek。

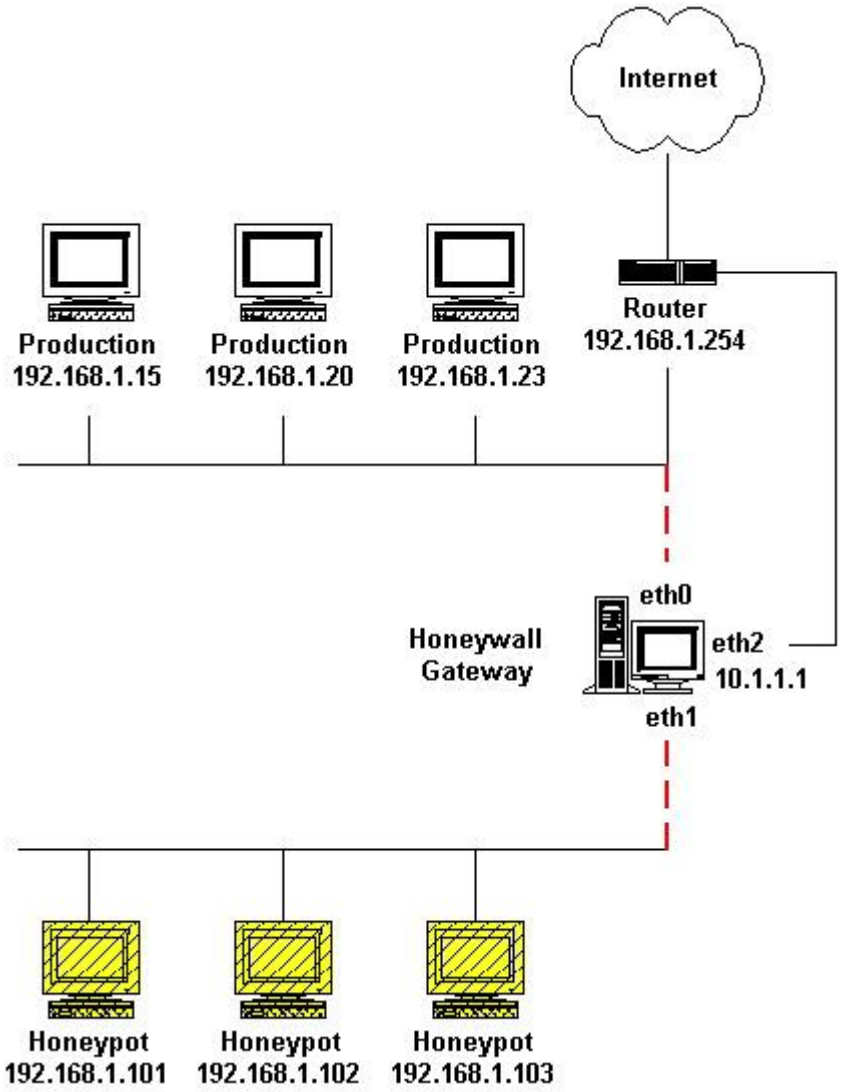

图 1 第二代蜜网体系架构

第二代蜜网方案的整体架构如图 1 所示，其中最为关键的部件为称为

HoneyWall 的蜜网网关，包括三个网络接口，eth0 接入外网，eth1 连接蜜网，而 eth2 作为一个秘密通道，连接到一个监控网络。HoneyWall 是一个对黑客不可见的链路层桥接设备，作为蜜网与其他网络的唯一连接点，所有流入流出蜜网的网络流量都将通过 HoneyWall，并受其控制和审计。同时由于 HoneyWall 是一个工作在链路层的桥接设备，不会对网络数据包进行 TTL 递减和网络路由，也不会提供本身的 MAC 地址，因此对黑客而言，HoneyWall 是完全不可见的，因此黑客不会识别出其所攻击的网络是一个蜜网。

首先，HoneyWall 实现了蜜网的第一大核心需求－数据控制。如图 2 所示，HoneyWall 对流入的网络包不进行任何限制，使得黑客能攻入蜜网，但对黑客使用蜜网对外发起的跳板攻击进行严格控制。控制的方法包括攻击包抑制和对外连接数限制两种手段。

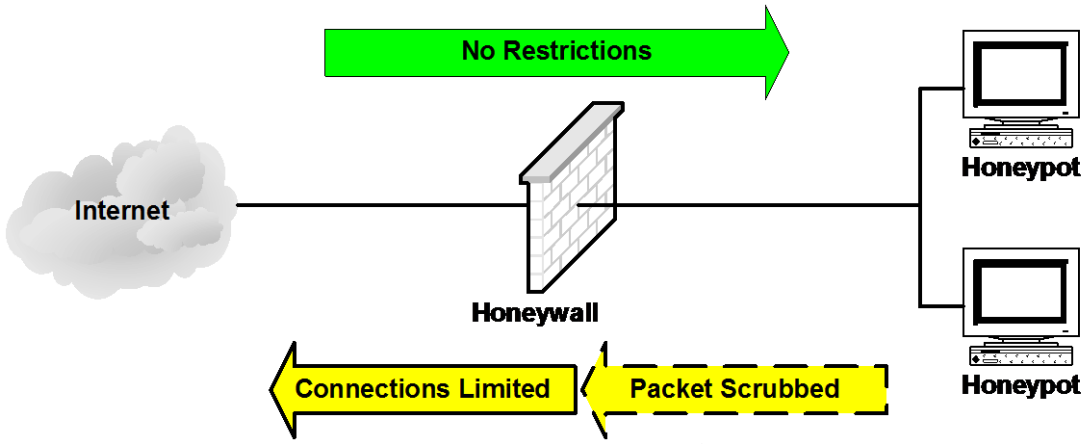

图 2 HoneyWall 的数据控制机制

攻击包抑制主要针对使用少量连接即能奏效的已知攻击（如权限提升攻击等），在 HoneyWall 中使用了 snort_inline 网络入侵防御系统（NIPS）作为攻击包抑制器，检测出从蜜网向外发出的含有的攻击特征的攻击数据包，发出报警信息并对攻击数据包加以抛弃或修改，使其不能对第三方网络构成危害。

而对外连接数限制则主要针对网络探测和拒绝服务攻击。HoneyWall 通过在 IPTables 防火墙中设置规则，当黑客发起的连接数超过预先设置的阈值，则 IPTables 将其记录到日志，并阻断其后继连接，从而避免蜜网中被攻陷的蜜罐作为黑客的跳板对第三方网络进行探测或拒绝服务攻击。

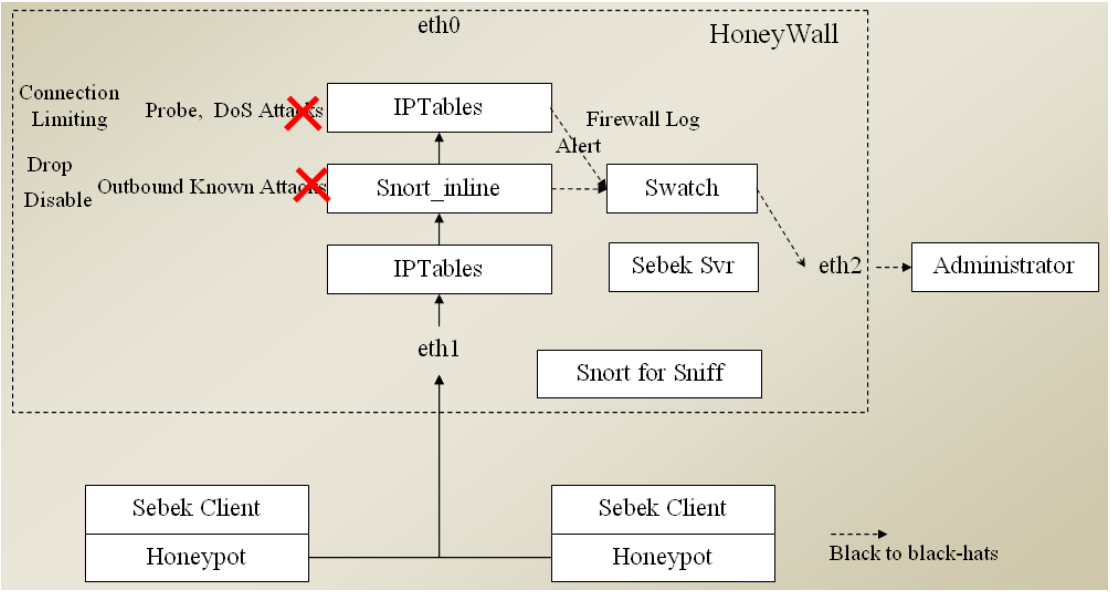

图 3 HoneyWall 中数据控制的具体流程

图 3 给出了 HoneyWall 中实现的数据控制机制（即攻击包抑制和对外连接数限制）的具体工作流程。Swatch 监视工具将 snort_inline 和 IPTables 产生的报警日志通过 Email 等方式通知管理员。

图 4 则给出了 HoneyWall 中实现的数据捕获机制的具体工作流程，黑客攻击数据包从 eth0 流入后，通过 IPTables 防火墙，根据防火墙规则，将对流入的连接活动进行记录，由于我们无需对流入的攻击进行过滤，因此可以直接跳过 snort_inline，但在 eth1 流出的时候，由一个作为网络监听器使用的 snort 记录全部的网络流量，以供后继的攻击分析所使用。另外，如图 5，在蜜网中的各个蜜罐上，通过安装 Sebek 的客户端，能够对黑客在蜜罐上的活动进行记录，并通过对黑客隐蔽的通道将收集到的键击记录等信息传送到位于 HoneyWall 的 Sebek 服务器。管理员可以通过 eth2 隐蔽通道对 HoneyWall 中收集到的数据进行分析，从而学习到黑客所发动的攻击方法。

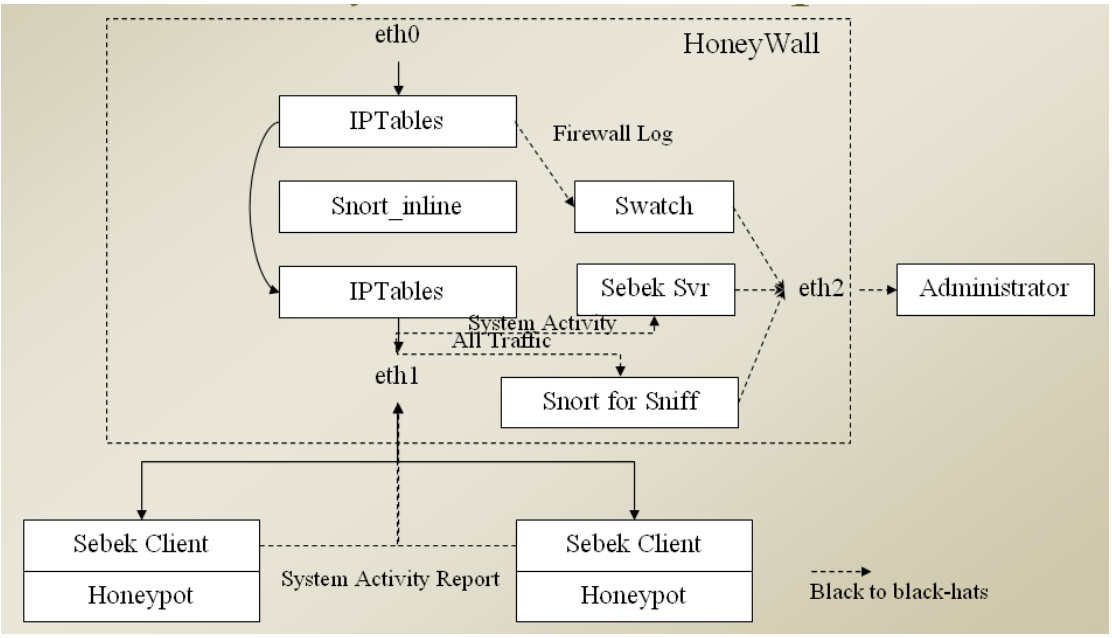

图 4 HoneyWall 中数据捕获的具体流程

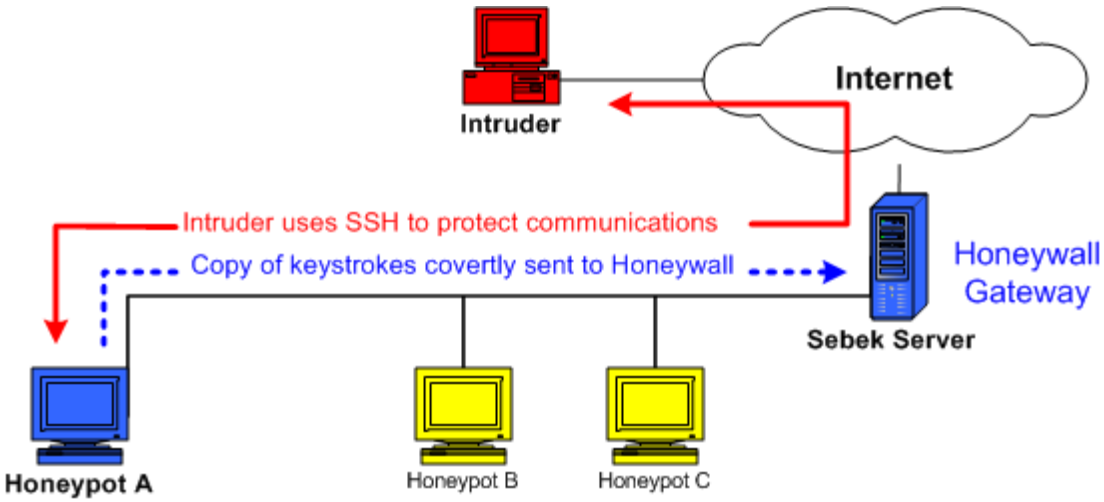

图 5 Sebek 工具工作原理

图 6 给出了 Sebek 服务器端的一个用户界面，使得研究人员能够较容易地从收集到的黑客键击记录中分析出其攻击方法。“蜜罐项目组”在数据分析方面的工作（即第四阶段）还未完成，因此目前对数据分析的支持还较弱。

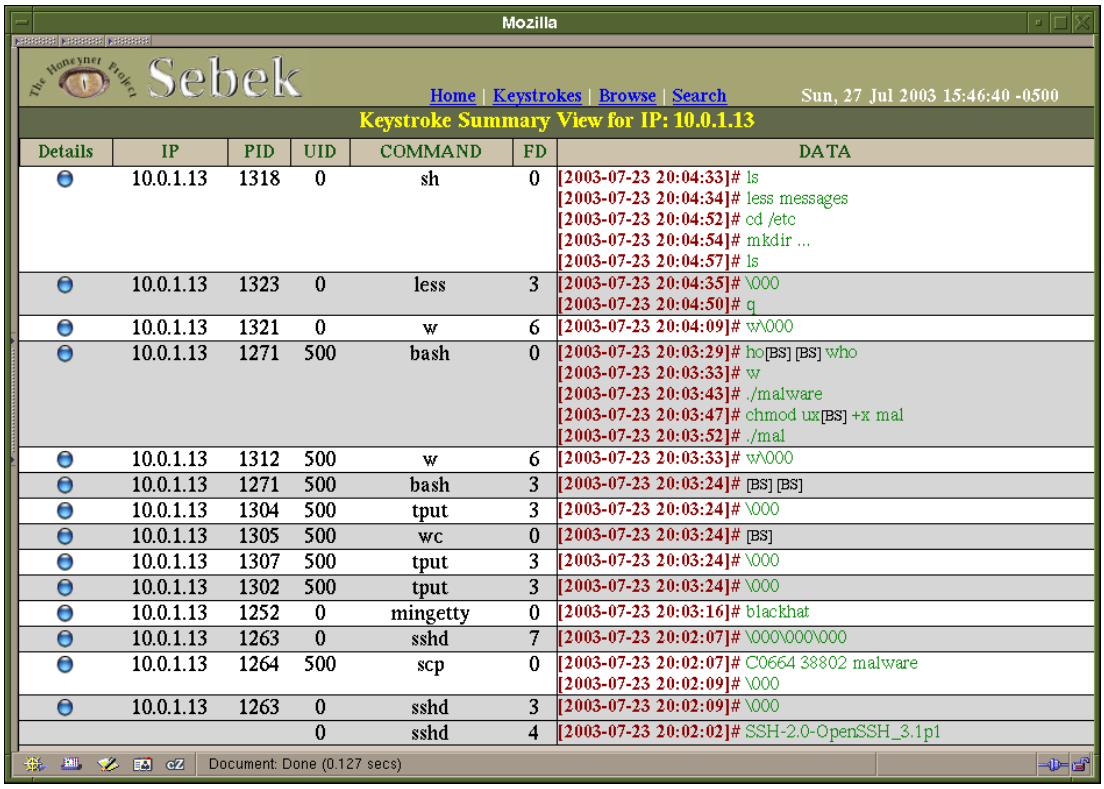

图 6 Sebek 服务器端的用户界面

4 研究方向

对蜜罐和蜜网技术的研究还处于早期阶段，目前蜜罐和蜜网的部署和维护还比较复杂，同时能够提供的数据分析工具的功能也较为有限，因此还需要专业的网络安全研究人员投入相当多的时间和精力。

除了“蜜网项目组”正在开发的数据分析工具外，Lance Spitzner 还给出了以下三个主要的研究方向。

4.1 动态蜜罐（Dynamic Honeypot）[4]

动态蜜罐能够通过被动监听其所处的网络中的流量，从而获得当前网络的部署状况，然后在无需人工干预的前提下自动地配置一些虚拟蜜罐，并隐藏在当前网络中，等待黑客的攻击。当网络的部署状况发生变化时（如操作系统版本更新），动态蜜罐技术能够实时地识别出这些变化，并动态地进行自适应，保证部署的虚拟蜜罐反映当前网络的典型配置。

4.2 蜜场（Honey Farm）[5]

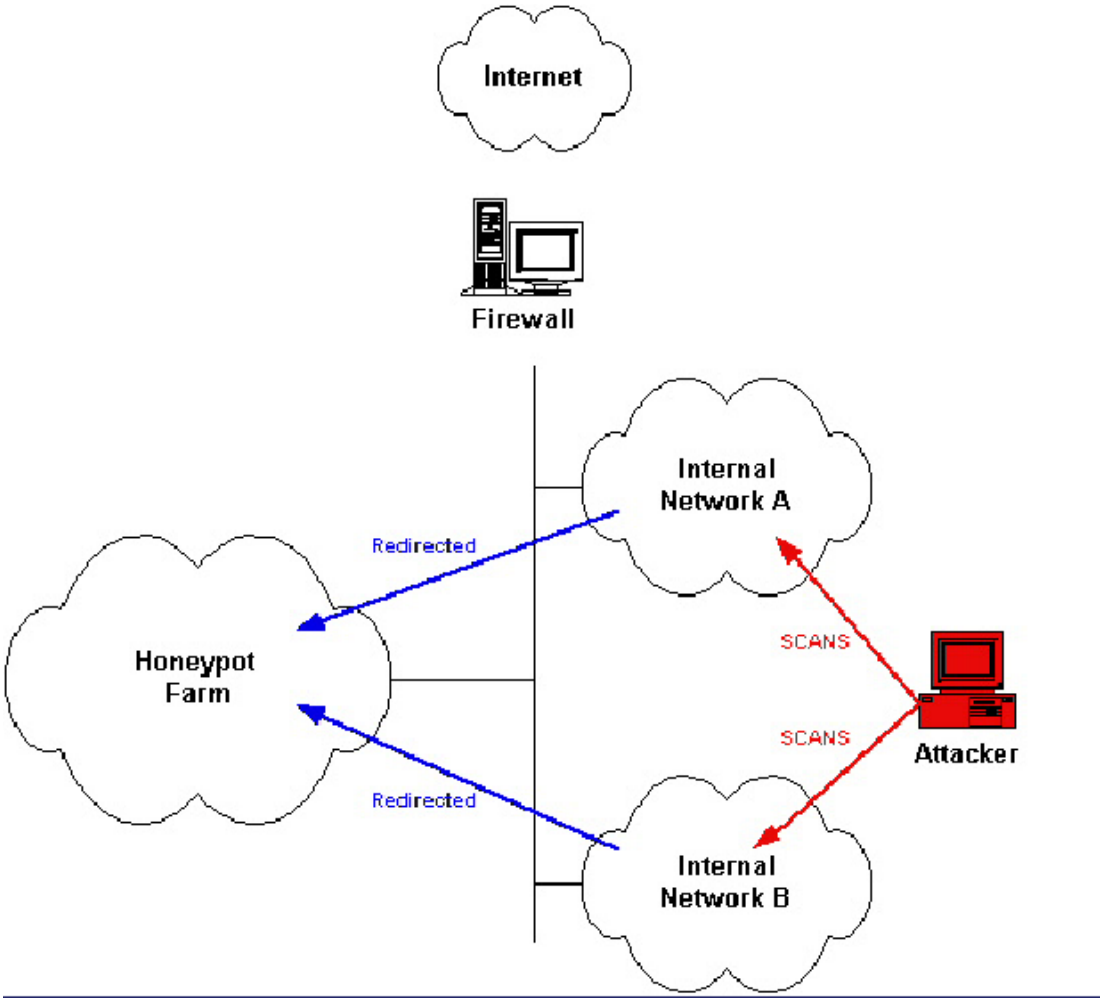

图 7 蜜场的基本概念图

如图 7，为了在大型的分布式网络中方便地部署和维护一些蜜罐，对各个子网的安全威胁进行收集，提出了蜜场的概念。即所有的蜜罐均部署在蜜场中，而在各个内部子网中设置一系列的重定向器（Redirector），若检测到当前的网络数据流是黑客攻击所发起时，通过重定向器将这些流量重定向到蜜场中的某台蜜罐主机上，并由蜜场中部署的一系列数据捕获和数据分析工具对黑客攻击行为进行收集和分析。

蜜场模型的优越性在于其集中性，使得其部署变得较为简单，即蜜场可以作为了安全操作中心（SOC: Security Operations Center）的一个组成部分，由安全专业研究和管理人员进行部署和维护。蜜场模型的集中性也使得蜜罐的维护和更新、规范化管理及数据分析都变得较为简单。此外，将蜜罐集中部署在蜜场中还减少了各个子网内的安全风险，并有利于对引入的安全风险进行控制。

蜜场模型的实现牵涉到两个重要的问题：重定向器和蜜罐的内容。目前在蜜场模型的方向下，初步原理证明性的例子有 Honeyd 的代理特性和 NetBait 工具。

重定向机制的引入使得我们可以以蜜罐来伪装具有高价值的目标，通过重定向器将恶意的或未授权的活动进行重定向到蜜罐中，并对这些活动进行监视和分析。

重定向的机制可以有以下三种不同的方式：

第一种重定向机制称为“Hot Zoning”，即将所有非规范的网络流量均进行重定向，非规范的网络流量包括发往非正常的目标端口的流量，由非正常的源端口发起的流量及非正常时间内的流量等一系列不符合正常网络情况的异常流量。

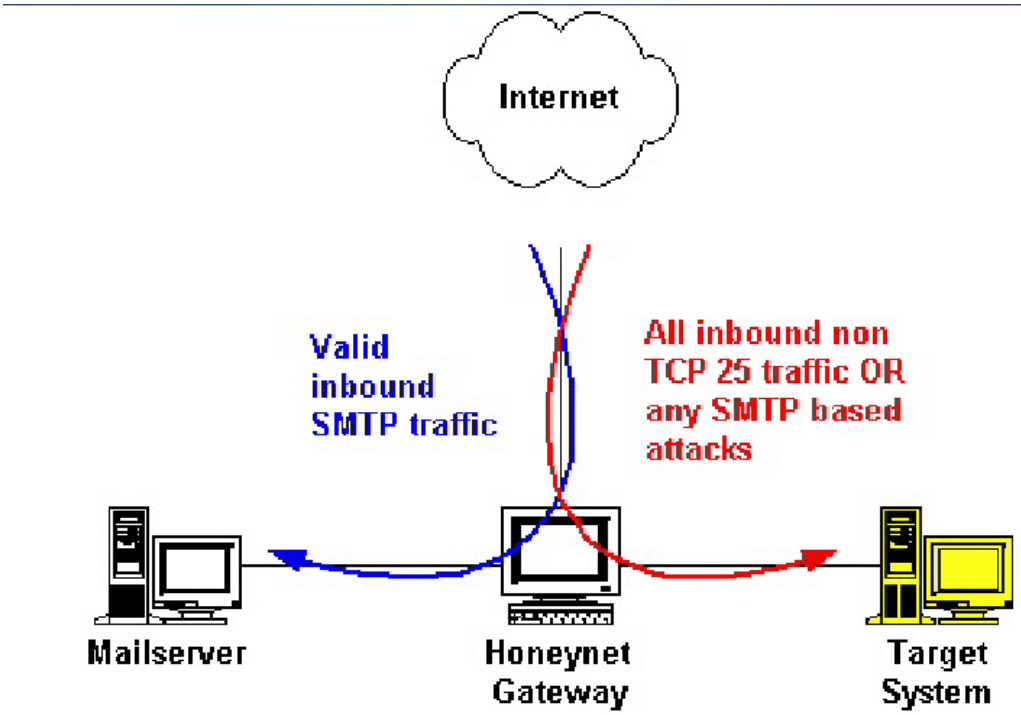

图 8 结合 Hot-zoning 和攻击检测两种重定向机制

第二种重定向机制通过部署入侵检测系统等对流量进行检测，将攻击的网络流量进行重定向到蜜罐，开源项目 Bait-n-Switch 即是属于此类的一个重定向器，它对著名的开源入侵检测系统 Snort 进行修改，使之作为内联网关和重定向器使用。

第三种重定向机制则在目标主机上进行监视异常和未授权行为，并对其进行重定向。与此相关的著名开源项目包括 PaX 和 Systrace。PaX 主要针对利用软件漏洞对攻击目标代码的内存空间进行读写滥用从而获取利益的攻击，如缓冲区溢

出和格式化字符串等攻击方法，通过一些防护和容忍等机制来抵制此类攻击。Systrace 则通过加强内核系统调用的安全策略，来严格限制应用程序对系统资源的访问权限，从而避免遭受一些攻击。这些研究项目都可以用来实现主机异常行为重定向机制。

重定向机制的引入还带来另外一个具有很大挑战的问题，即在不被黑客所发觉的前提下完成对其网络活动的重定向。其中最为核心的是蜜罐的内容问题。为了保证蜜罐的高度迷惑性，蜜罐必须使用真实的网络环境，同时拥有与攻击目标一直的操作系统、应用程序以及数据内容。其带来的好处是能够在高度真实的网络中，可以跟踪监视黑客的一举一动，从而获取价值度很高的攻击信息。但如何方便有效地保证蜜罐内容的高度真实性和迷惑性，还需要进行进一步的研究。

4.3 Honeytoken[6]

Honeytoken 概念提出的出发点是黑客社团的攻击目标不仅仅在于攻陷网络和主机本身，往往更多时候是对信息内容的攻击。由此，我们可以扩展蜜罐的概念，即使用一些正常情况下永远不会使用的信息内容（称为 Honeytoken）作为诱饵，一旦发现这些 Honeytoken 被访问，则预示黑客可能对信息内容发起攻击，从而我们可以发现并追踪黑客的攻击活动。

较容易实施的 Honeytoken 包括数据库中的某些无用数据项、以及伪装的用户帐号和及其弱口令等。

5 法律问题

蜜罐技术可能会涉及以下几类法律问题，首先是诱捕行动是否会触犯法律的问题，诱捕行为仅仅是一种防御方法，而不是攻击行为，因此诱捕行为不会触犯到法律，这里需要注意的原则是不要对部署的蜜罐进行宣传从而引诱黑客进行攻击。第二个可能会涉及到的法律问题是对隐私权的侵犯，在各个国家都制定了许多保护个人隐私权的法律，可能有些法律会保护个人网络通信的隐私权，但还没有直接针对蜜罐的法律。最可能引发法律纠纷的是黑客利用蜜罐对第三方网络发起攻击造成破坏后，被攻击的第三方可能会对蜜罐的部署方提出诉讼。因此对黑

客利用蜜罐向第三方网络发起的攻击需要采取强有力的控制措施，必要时完全切断蜜罐的网络连接，从而尽量避免此风险。

6 结论

本文综述了蜜罐及蜜网技术的基本概念、发展历程、核心功能及进一步的研究方向。可以看到，蜜罐和蜜网技术的发展已经使得我们能够部署一个蜜网，并对黑客攻击事件进行分析。同时蜜罐和蜜网技术还未完全成熟，还存在着大量的问题进一步的研究和解决。

参考资料

[1] L. Spitzner, “Honeypot - Definitions and Value of Honeypots” 2003/05/29. Available from http://www.tracking-hackers.com/papers/honeypots.html.

[2] L. Spitzner "The Honeynet Project: Trapping the Hackers," *IEEE Security & Privacy* vol. 1, no. 2, pp. 15-23, 2003.

[3] Honeynet Project. “Know Your Enemy Genii Honeynets”, 2003/11/03. Available from http://project.honeynet.org/papers/gen2/index.html.

[4] L. Spitzner "Dynamic Honeypots," 2003/09/15. Available from http://www.securityfocus.com/infocus/1731.

[5] L. Spitzner "Honeypot Farms," 2003/08/13. Available from http://www.securityfocus.com/infocus/1720.

[6] L. Spitzner "Honeypots: Catching the Insider Threat," *Proceedings of the 19th Annual Computer Security Applications Conference*, Las Vegas, Nevada, USA, December 08 – 12, 2003.