蜜罐取证的技术及法律问题研究

王剑虹[1] 何晓行[2]
(西南政法大学法学院 重庆 401120)[1] (重庆邮电大学法学院 重庆 400065)[2]

摘 要 蜜罐作为新兴的网络防御及动态取证技术,不仅能够主动防御网络攻击,而且还可以收集入侵者实施攻击的重要证据。它通过网络欺骗、端口重定向、报警、数据控制和数据捕获等技术,增强动态防护体系的检测与反应能力,提高网络的安全防护水平。蜜罐运行会产生一定的技术风险,而选择低风险蜜罐、强化系统的数据获取和报警功能以及增加连接控制和路由控制等能有效实现风险控制。对于蜜罐取证可能产生的陷阱、隐私权及责任等法律问题,则可采取避免过度主动引诱、隐私权提示及审慎监控等方式加以克服。

关键词 蜜罐,风险,欺骗,取证,责任
中图法分类号 TP393.08 **文献标识码** A

Research on the Technical and Legal Issues of Collecting Evidence by Honeypot

WANG Jian-hong[1] HE Xiao-xing[2]
(Law Institute, Southwest University of Political Science and Law, Chongqing 401120, China)[1]
(Law Institute, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)[2]

Abstract Honeypot is a new kind of the defense technology, which can defend the internet attack actively and collect the important evidence of the attackers. The techniques of realizing collecting evidence by honeypot include internet deception, port reaction, data seizure, data analysis and data control etc, which help to improve the detection level and reactivity of dynamic protection system. Running honeypot may result in some technical risks, therefore, it is necessary to control the risks by choosing low-risk honeypot, intensifying data seizure and alarm function and increasing the link control and route control therefore etc. As to the legal problems, including entrapment, privacy right and liability, we can solve them by undue-temptation prohibition, privacy right hint and cautious supervision.

Keywords Honeypot, Risk, Deception, Collecting evidence, Liability

随着计算机信息技术的飞速发展,人们对数字信息的依赖已达到前所未有的程度。与此同时,计算机犯罪率也出现了惊人的增长。公安司法机关要达到有效打击计算机犯罪的目的,就需要对电子取证领域进行深入的研究,而蜜罐取证技术即为目前较为广泛使用的取证手段。本文就如何利用蜜罐技术进行取证的相关技术及法律问题加以介绍与讨论,以期为我国电子取证的发展提供一定的理论及实践参考。

1 蜜罐的概念与分类

1.1 蜜罐的概念

学者 Lance Spitzer 在“Honeypots Definition and Value Of Honeypots”一文中给出了蜜罐的权威定义[1]:蜜罐是一种安全资源,其价值在于被扫描、攻击和攻陷。它是一种在互联网上运行的,目的在于吸引攻击者,然后记录下攻击者的一举一动的计算机系统[2]。

蜜罐作为一种新型安全工具,在攻击的检测、分析、研究及捕捉等方面具有优越的性能。相对于传统安全工具的被动防御,蜜罐最大的优势在于它能主动检测和响应网络入侵,在网络攻防战中赢得时间和主动。蜜罐技术通过部署作为诱饵的主机、网络服务以及信息,诱使入侵者对错误的目标开展攻击活动,减少对实际系统造成的安全威胁。同时蜜罐技术可以对攻击行为进行监控和分析,了解入侵者所使用的攻击工具和方法,推测入侵者的意图和动机,并在此基础上追踪入侵者的来源,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,并通过法律手段去追究入侵者的责任,或者通过技术和管理手段来增强对实际系统的安全防护能力[3]。

1.2 蜜罐的分类

根据不同的标准,蜜罐有如下分类。

1.2.1 依据蜜罐应用的目的,可分为产品型蜜罐和研究型蜜罐

产品型蜜罐的设置目的在于为某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。产品型蜜罐往往被作为诱饵,把黑客的攻击尽可能长时间地捆绑在蜜罐上,以赢得时间来保护真实的网络系统。产品型蜜罐也可能用于收集证据来作为起诉黑客的依据,它引入的风险较低,且具有易部署、节约资源等

到稿日期:2010-09-16 返修日期:2010-11-28 本文受西南政法大学校级重点项目(2010-XZZD25)资助。
王剑虹(1978—),女,博士,讲师,主要研究方向为电子证据与计算机应用技术,E-mail:wjh611@yahoo.com.cn;何晓行(1975—),女,博士,讲师,主要研究方向为电子证据与计算机应用技术。

优点。

而研究型蜜罐则主要应用于研究活动，它的设置目的主要在于通过吸引黑客侵入，对黑客的行为进行追踪和分析，以此来搜集信息、探测新型攻击、检索新型黑客工具，从而了解黑客和黑客团体的背景、目标及活动规律等。因此，研究型蜜罐在发现系统漏洞等方面具有较大的价值，但它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。

1.2.2 依据蜜罐的交互程度，可分为低交互型蜜罐、中交互型蜜罐以及高交互蜜罐

蜜罐的交互程度指攻击者与蜜罐相互作用的程度[4]。低交互型蜜罐通常是运行于现有操作系统上的一个仿真服务，黑客只能在仿真服务预设的范围内动作，只允许少量的交互动作。低交互型蜜罐类似于一个只能记录特征匹配的输入数据包的入侵检测系统。从某种意义上来说，低交互型蜜罐并没有真正的操作系统和服务，其结构较简单，部署较容易，因此使用该种蜜罐所引起的风险也相对较低，但是，低交互型蜜罐却不可能观察到与真实操作系统互相作用的攻击，它所能收集的信息也是极为有限的。

中交互型蜜罐则可以反馈攻击者更多的信息。这种蜜罐一般不提供真实的操作系统，而是应用脚本或小程序来模拟服务行为。中交互型蜜罐可以通过更多且更复杂的互动，让攻击者将其误认为一个真正操作系统，因此它能够记录和分析的数据更为丰富。当然，开发中交互蜜罐的技术相对复杂，它必须确保在模拟服务中不产生新的真实漏洞，防止为黑客渗透和攻击真实系统提供机会。与低交互型蜜罐不同的是，中交互型蜜罐可以监视和记录侵入者所使用的攻击工具和方法，但是所记录的信息多为侵入者攻陷蜜罐的过程数据。

高交互型蜜罐则必须依托真实的操作系统来加以构建，它给黑客提供真实的系统和服务。采用这种蜜罐有两个优点，一是可以给黑客提供一个真实的操作系统，从中了解黑客运行的全部动作，以收集更多有价值的信息；二是这种蜜罐能够提供一个完全开放的环境来获取所有的侵入行为数据。但是由于高交互型蜜罐将向黑客完全开放系统，这就带来了更高的风险，即黑客可能通过这个完全开放的真实系统去攻击其他的系统。

2 实现蜜罐取证的技术

蜜罐取证的实现主要依赖于低层网络技术的支持和运用。而对于蜜罐特殊的运作方式和实用目的，其原理的实现也在传统的网络技术上有新的要求。目前，实现蜜罐取证的主要技术包括网络欺骗、端口重定向、数据捕获、数据分析和数据控制等。

2.1 网络欺骗

由于蜜罐的价值只在其被探测、攻击或者攻陷时才得到体现，故网络欺骗技术是蜜罐取证体系中最为关键的核心技术。目前蜜罐主要的网络欺骗技术有如下几种。

2.1.1 模拟服务端口

侦听非工作的服务端口是诱骗黑客攻击的常用欺骗手段。当黑客通过端口扫描检测到系统打开了非工作的服务端口时，他们通常会主动向这些端口发起连接，并试图利用已知系统或应用服务的漏洞来发送攻击代码。而蜜罐系统就通过端口响应来收集所需要的信息，从而达到取证目的。不过由于简单的模拟并不是工作服务端口，因此它只能与黑客建立连接，而不能进行下一步的信息交互，所以通过模拟服务端口获取的信息数量是相当有限的。

2.1.2 模拟系统漏洞和应用服务

模拟系统漏洞和应用服务则交互相对更高，如某种蠕虫病毒正在扫描特定的漏洞，在这种情况下，我们就可以构建一个模拟 Microsoft IIS Web 服务器的蜜罐。只要入侵者对该蜜罐建立起 Http 连接，它就会以 IIS Web 服务器的身份加以响应，从而为入侵者提供一个与实际的 IIS Web 服务器进行交互的机会。这种级别的交互比端口模拟所收集到的信息更为丰富。

2.1.3 IP 空间欺骗

IP 空间欺骗则是利用计算机的多宿主能力在一块以太网卡上分配多个 IP 地址，这样入侵者在对某个空间进行搜索时，他们的工作量就会大大增加。将这项技术和虚拟机技术结合，就可以建立一个大的虚拟网段，而且这种技术的成本也相对较低。

2.1.4 流量仿真

产生仿真流量的目的是防止入侵者通过流量分析检测到欺骗。入侵者侵入系统后，他们往往会谨慎地使用某种工具来分析系统的网络流量，如果发现系统网络流量较小，那么这个系统的真实性就会受到怀疑。流量仿真就是利用各种技术产生欺骗的网络流量，以此来迷惑入侵者。现在流量仿真主要的方法有两种：一是采用实时或重现的方式复制真正的网络流量；二是从远程伪造流量。

2.1.5 网络动态配置

真实网络系统的状态具有动态性，如果蜜罐系统是静态的，那么在入侵者的长期监视下，这种欺骗就容易暴露。因此需要动态配置系统，使其状态随时间而改变，从而更接近真实的系统，以增加蜜罐的欺骗性。

2.1.6 组织信息欺骗

如果某个组织提供有关个人和系统信息的访问，那么欺骗也必须以某种方式反映出这些信息。例如，组织的 DNS 服务器包含了个人系统拥有者及其位置的详细信息，那么我们就有必要在欺骗的 DNS 列表中设置伪造的拥有者及其位置。

2.1.7 网络服务

网络服务往往与特定的系统漏洞联系在一起，网络服务往往是攻击者侵入系统的入口，网络服务可以吸引黑客的注意，同时也使蜜罐更接近于一个真实的系统。

2.1.8 蜜罐主机

蜜罐主机负责与入侵者交互，它是捕捉入侵者活动的主要场所。蜜罐主机可以是模拟的或真实的各种操作系统。与一般系统的不同之处在于，该系统处于严密的监视和控制之下。入侵者与系统的每一次交互都被日志记录。使用虚拟机技术主要有两个优点，一是在单机上运行多个客户操作系统，从而模拟一个网络；二是在客户操作系统被入侵者破坏后，宿主操作系统不会受影响，这样可以保护宿主操作系统的安全，增强蜜罐系统的取证能力。

2.2 端口重定向

端口重定向技术可以在工作系统中模拟一个非工作服务。例如我们正常使用 Web 服务时，用 TELNET(23)和 FTP(21)重定向到蜜罐系统中，实际上这两个服务并没有开

启，而是由蜜罐虚拟出来的。但攻击者扫描时却发现这两个端口已开启，这样攻击者就难以对其服务器产生实质的危害。

重定向可以在两种模式下进行：一种是代理模式，在该模式下，将外部连接经过地址转换后通过代理发送到带蜜罐的服务器上，从外部看不到带蜜罐服务器，只能看到服务器组内主机的 IP 地址；另一种是直接响应模式，在该模式下，当有外部连接到达服务器组内的主机时，重定向程序会将连接请求转发到带蜜罐服务器，由带蜜罐服务器直接与外部建立一个连接。从外部看到的连接的 IP 地址却是带蜜罐服务器的真实 IP 地址。

简言之，实现重定向是为了让黑客进入一个模拟的服务，从而使黑客入侵的是一个蜜罐系统，而真实操作系统的服务并没有开启。端口重定向并没有改变操作系统的端口号，而是利用相同的端口使模拟的服务代替了真实操作系统的服务。

2.3 数据捕获

数据捕获是蜜罐的核心功能模块。数据捕获的目标是捕捉攻击者从扫描、探测、攻击、攻陷蜜罐主机到最后离开蜜罐的每一步动作。为了实现这个目标，我们将数据捕捉可分 3 个层次来实现。最外层数据捕捉由防火墙来完成，主要是对出入蜜罐系统的网络连接进行日志记录，这些日志记录存放于防火墙本地，防止被入侵者删除更改。第二层数据捕捉则由入侵检测系统(IDS)来完成，IDS 抓取蜜罐系统内所有的网络包，这些抓取的网络包存放在 IDS 本地。最里层的数据捕捉由蜜罐主机来完成，主要是蜜罐主机的所有系统日志、所有用户击键序列和屏幕显示，这些数据通过网络传输送到远程日志服务器存放。

2.4 数据分析

数据分析包括网络协议分析、网络行为分析和攻击特征分析等。数据分析是蜜罐取证技术中的难点，要从大量的网络数据中提取出攻击行为的特征和模型是相当困难的。使用数学模型自动分析和挖掘出网络攻击行为的特征则是目前蜜罐取证过程中面临的最大难题之一。

2.5 数据控制

蜜罐系统作为黑客的攻击目标，其自身的安全尤其重要，如果蜜罐系统被攻破，那么将难以得到有价值的信息，同时蜜罐系统可能会被入侵者用作攻击其他系统的跳板。数据控制是蜜罐系统必需的核心功能之一，用于保障蜜罐系统自身的安全。

对蜜罐的访问是被允许的，但是从蜜罐系统外出的网络连接却需要有效控制。若蜜罐系统发起外出的连接，说明蜜罐主机被入侵者攻破了，而这些外出的连接很可能是入侵者利用蜜罐对其他的系统发起的攻击连接。对外出连接的控制不是简单地阻断蜜罐对外所有的连接，那样无疑在告诉入侵者他正身陷蜜罐系统当中，而入侵者成功侵入系统后的动作和企图是应当重点关注的，因此可以限制一定时间段内外出的连接数，甚至可以修改这些外出连接的网络包，使其不能到达它的目的地，同时又给入侵者网络包已正常发出的假象。

蜜罐通常有两层数据控制，分别是连接控制和路由控制。连接控制由防火墙来完成，通过防火墙限制蜜罐系统外出的连接。路由控制由路由器来完成，主要利用路由器的访问控制功能对外出的数据包进行控制，以防止蜜罐系统作为攻击源向其他系统发起 IP 欺骗、DOS 和 ICMP 攻击、SYN 和 SMURF 等攻击。路由器可用网关代替，网关没有网络地址，因此在网关上进行控制操作更加隐蔽，不易被黑客察觉。

3 蜜罐取证的技术风险及控制

3.1 蜜罐取证的风险

运行蜜罐也可能会产生以下风险。

首先，在蜜罐取证过程中，可能存在未被发现的黑客对蜜罐进行接管的风险。如果未意识到黑客对蜜罐的接管，那么这样的蜜罐是充满危险的。也就是说，如果一个蜜罐被入侵者攻陷，蜜罐管理员者却没有发现，那么蜜罐取证显然难以实现，而且还可能会给真正的系统带来一定的风险。

其次，对蜜罐和入侵者失去控制也可能产生一定的风险。一个优秀的蜜罐系统应该可以随时终止进出蜜罐的任何通讯，可以随时备份系统状态。操作者不应该过分依靠与蜜罐本身相关的任何机器，即使蜜罐被完全攻陷，也仍在控制之中。同时虚拟机也同样存在危险，它难以保证黑客不突破虚拟机而进入主机操作系统。

最后，蜜罐取证使用不当有可能对第三方产生损害，即高明的黑客甚至可能反过来控制蜜罐，把它作为进一步攻击的跳板[5]，如利用蜜罐做端口扫描、发起 DDOS 攻击等，这很可能涉及到法律赔偿问题，因此保护第三方和保护自己的资源同样重要。

3.2 蜜罐取证的风险控制

从技术角度来看，要在最大限度内降低蜜罐取证的风险主要可通过以下途径实现。

3.2.1 根据实际需要选择最低风险的蜜罐

如果只是想发现一个公司内部的入侵者，则使用中低交互的蜜罐就足够了，而不必一定要选择高交互型蜜罐。如确有需要使用高交互蜜罐，那么也可以尽量优先选择利用带防火墙的蜜网而不是单一的蜜罐。

3.2.2 强化系统的数据获取和报警功能

蜜罐的数据获取模块应尽可能获取包括网络中各种输入、输出包等在内的信息。数据获取包括主机数据收集和网络数据收集。其中主机数据收集用于获取本地计算机的网络数据流及其他信息，但这种信息收集容易被攻击者成功探测，从而给信息收集工作带来一定的障碍。而采用网络数据收集技术，对网络流量进行收集和分析，则相对难以检测，故它的安全性更高。网络数据收集既可以利用专门的模块来实现，也可以与防火墙或者入侵检测系统配合，简化收集过程。另外，还可以建立异常行为的数据库，在获取网络数据的同时，对一些非常可疑的行为进行报警，提醒系统的维护人员关注正在发生的攻击行为，对整个入侵过程进行监视。

3.2.3 增加连接控制和路由控制

连接控制是指对蜜罐系统的外出连接加以控制，防止攻击者利用系统作为跳板去攻击其他主机。它接受蜜罐系统所在网络的所有外来连接，但同时控制由蜜罐系统所发出的网络连接。入侵者完成对蜜罐系统的扫描、探测，或利用某种安全漏洞进入系统后，一般会将蜜罐系统作为跳板，对其他主机发起攻击。蜜罐系统则可以根据入侵者发出的连接请求和操作命令，根据自身的算法决定是否断开连接以及停止下一步的行为。同时，连接控制的另一个功能是记录所有外来连接和外出连接的情况，这些数据也是对蜜罐系统进行攻击分析

和来源分析的初步资料。

路由控制则对来自蜜罐系统所在网络的数据包进行初步处理，以防止入侵者利用系统对外进行地址欺骗，威胁网络内其他主机的安全。路由控制作为连接控制之后的第二层次的访问控制，对外出数据包加以控制。将连接控制与路由控制相结合，既能给入侵者提供较大的空间，又能有效控制入侵者利用蜜罐系统而发起的攻击行为，从而保护了蜜罐系统和周边系统的安全。

4 蜜罐取证面临的法律挑战

在司法实践中，利用蜜罐进行取证可能面临一些法律问题。由于蜜罐要为黑客入侵提供机会，因此它必然要设置一定的漏洞，但是其中很多漏洞属于高危级别，稍有不慎就会导致系统被渗透。一旦蜜罐被破坏，入侵者的行为则难以预料。例如，一个入侵者成功进入了一台蜜罐，并且用它作为跳板（指入侵者远程控制一台或多台被入侵的计算机对别的计算机进行入侵行为）去攻击别人[6]，这必然会引起一定的法律后果。总的来说，蜜罐取证所面临的法律问题主要包括以下几个方面。

4.1 陷阱

如果密罐所有者故意引诱攻击者进入蜜罐，那么就可能产生与陷阱有关的法律问题。通常来说，在犯罪嫌疑人或者被告人没有犯罪倾向的情况下，侦查人员对其加以引诱，从而导致其最后实施犯罪行为，这会被称为“犯意诱发型诱惑侦查”，侦查人员的这种行为在法理上就可能构成了“侦查陷阱”。在英美法系国家，一旦被告成功提起陷阱抗辩，便会导致一系列的法律后果，如在美国，被告人提起的陷阱抗辩为实体抗辩，即一旦陷阱抗辩成功，被告人的行为就不构成犯罪；在加拿大，被告成功提起陷阱抗辩会导致刑事诉讼的中止；在澳大利亚，如被告人成功提起陷阱抗辩，那么通过陷阱取得的证据的合法性就难以得到确认，而法院则必须启动非法证据排除程序[7]。

尽管我国的法律中对于诱惑侦查及陷阱抗辩的相关问题并未作出明确规定，但《全国部分法院审理毒品犯罪案件工作座谈会纪要》中规定：“对因‘犯意引诱’实施毒品犯罪的被告人，根据罪刑相适应原则，应当依法从轻处罚……行为人本来只有实施数量较小的毒品犯罪的故意，在特情引诱下实施了数量较大甚至达到实际掌握的死刑数量标准的毒品犯罪的……属于“数量引诱”。对因“数量引诱”实施毒品犯罪的被告人，应当依法从轻处罚……对不能排除‘犯意引诱’和‘数量引诱’的案件，在考虑是否对被告人判处死刑立即执行时，要留有余地”。由此可见，我国立法对于诱惑侦查并不排斥，但对于“犯意诱发型诱惑侦查”则在总体上持否定态度。而蜜罐取证类似于以诱惑侦查的方式取证，那么如何把握合法性界限就成为必须关注的问题。不过由于蜜罐在本质上是一种防御系统，只要不对部署的蜜罐进行过分的宣传或对潜在的攻击者进行过度的引诱（如许以利益等），那么设置蜜罐进行取证至多只构成“机会提供型”诱惑侦查，这种取证则具备法理上的正当性。

4.2 隐私权

蜜罐属于记录设备，蜜罐操作的特点就是要对侵入系统的信息交流进行记录、监控，这必然会涉及到隐私权问题。如果一台蜜罐被设计用于收集公司员工的活动数据，或者拦截并记录公司网络通讯信息，那么这就可能侵犯他人的隐私权。对于入侵某个蜜罐的黑客，蜜罐的使用仍有可能会侵犯其隐私权。黑客在侵入他人网络系统后，往往会将该系统用作一个交流平台，被黑客攻陷的系统就可能变为一个私人的交互式闲聊程序代理服务器。蜜罐的操作者则能够通过蜜罐监控这些交流。但是，这种监控就可能侵犯包括黑客在内的交流平台使用者的隐私权。

不过根据我国最高人民法院 1993 年《关于审理名誉权案件若干问题的解答》第七项之规定：“对未经他人同意，擅自公布他人的隐私材料或者以书面、口头形式宣扬他人隐私致他人名誉受到损害的，按照侵害他人名誉权处理”，由此可知，如果网络用户在进入某个网站时了解自己的信息可能被收集或被用于某种特定目的，这种收集用户信息的行为就不构成侵权。那么在蜜罐取证过程中，就可以给进入蜜罐者一定的隐私权提示，由其自行选择是否继续进入，如果继续进入系统则视为其对收集其个人信息的行为表示接受，比如我们可以使用“个人使用隐私选择平台（P3P）”等方式达到保护网络隐私权的目的。

4.3 责任

关于蜜罐的另一个法律问题即连带责任问题。一旦黑客攻入蜜罐，他就有可能会利用网络去侵害他人的合法权益。有漏洞的蜜罐往往会被用于诸多非法的目的，比如黑客可能会将其用来从事一些非法交易，如盗用他人信用卡、商业秘密等，甚至可能将被攻击的网络变成一个钓鱼网站或色情网站。如果发生这类情形，系统的所有者就有可能会因此而承担法律责任。因此，一旦使用蜜罐，对它的运行必须进行谨慎地监控。

结束语 传统的计算机取证多采用案后分析的静态取证技术，故其证据的获取缺乏实时性与连续性，而蜜罐技术是一种基于欺骗的主动防御及动态取证技术，它在深入剖析、应对互联网安全威胁方面具有明显优势。蜜罐能迅速查找并发现新型攻击和新型攻击工具，从而解决了入侵检测系统和防火墙中难以对新型攻击及时做出反应的问题，因此蜜罐具有较为广泛的应用前景。但是，随着网络入侵类型的多样化，蜜罐的运行也凸显出一定的技术风险及法律风险，如何有效防范这些风险及实现蜜罐的多样化演绎，将成为蜜罐技术研究和应用的重点和主要突破的方向。

参 考 文 献

[1] Spitzner L. Honeypots-Definitions and Value of Honeypots[DB/OL]. http://www.enteract.com/ lspitz/honeypot.html,2001

[2] 王永全，齐曼. 信息犯罪与计算机取证[M]. 北京：北京大学出版社，2010：165

[3] 杜彦辉. 利用蜜罐技术实现对互联网非法活动进行监控[J]. 中国人民公安大学学报：自然科学版，2007，4：78

[4] Spitzner L. The Honeynet Project: Trapping the Hackers[J]. Security and Privacy Magazine, IEEE, 2003, 1(2): 15-23

[5] 陈琳，李之棠，高翠霞. 一种自适应的动态取证机制[J]. 计算机科学，2009，11：66

[6] 纪佩宇. “蜜罐”取证及其法律属性[J]. 江苏警官学院学报，2005(6)：153

[7] Ian Walden D R, Flanagan A. Honeypots: A Sticky Legal Landscape[J]. Rutgers Computer & Tech. Law Journal, 2003