主动防护网络入侵的蜜罐(Honeypot)技术

Honeypot －－Technology to Prevent Network Intrusion Proactively

殷联甫（嘉兴学院信息工程学院 314001）

摘要：本文首先介绍了蜜罐的概念、分类方法以及蜜罐所使用的主要技术，然后介绍了几种常见的蜜罐产品，同时阐述了蜜罐在网络系统中的部署情况，最后指出了蜜罐的发展方向和应用前景。

关键词：Honeypot　网络陷阱　网络安全

1　引言

随着信息技术的不断发展，信息安全正日益受到人们的重视，信息安全技术的核心问题是对计算机系统和网络进行有效的保护。信息安全中的网络安全技术主要包括防火墙技术、入侵检测技术、病毒防护技术、数据加密和认证技术等，这些技术大多数都是在攻击者对网络进行攻击时对系统进行被动的防护，而蜜罐(Honeypot)技术可以采取主动的方式，用其特有的特征吸引攻击者，同时对攻击者的各种攻击行为进行分析并找到有效的对付办法。

2　什么是蜜罐(Honeypot)

蜜罐(Honeypot)是一种在互联网上运行的计算机系统，它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人(如电脑黑客等)而设计的。蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标。由于蜜罐并没有向外界提供真正有价值的服务，因此所有对蜜罐的链接尝试都被视为是可疑的。蜜罐的另一个用途是拖延攻击者对真正目标的攻击，让攻击者在蜜罐上浪费时间。这样，最初的攻击目标得到了保护，真正有价值的内容没有受到侵犯。此外，蜜罐也可以为追踪攻击者提供有用的线索，为计算机取证提供有力的证据。从这个意义上来说，蜜罐就是诱捕攻击者的一个陷阱。

蜜罐系统最重要的功能是对系统中所有操作和行为进行监视和记录，网络安全专家通过精心的伪装，使得攻击者在进入到目标系统后仍不知自己所有的行为已经处于系统的监控中。为了吸引攻击者，网络安全专家还通常在蜜罐系统中故意留下一些安全后门以吸引攻击者上当。

总之，蜜罐是一个专门为了被攻击或入侵而设置的欺骗系统，表面上看很脆弱，易受攻击，实际上不包含任何敏感数据，也没有合法用户和通信，能够让入侵者在其中暴露无遗。设置蜜罐的目的主要有二个：一是在不被攻击者察觉的情况下监视他们的活动，收集与攻击者有关的所有信息；二是牵制他们，使他们将时间和资源都耗费在攻击蜜罐上，使实际的工作网络得到保护。

3　蜜罐的分类

可以有多种方法对蜜罐进行分类：根据蜜罐的设计目的不同，可将蜜罐分为产品型蜜罐和研究型蜜罐二种；根据蜜罐的工作方式不同，可将蜜罐分为牺牲型蜜罐和外观型蜜罐二种。

3.1　产品型蜜罐和研究型蜜罐

产品型蜜罐具有事件检测和欺骗功能，它们所要做的工作就是检测并对付恶意攻击者，目的是减轻受保护组织将受到的攻击威胁。它通常放置在一个部门的内部网络环境中，由于它对攻击者具有相当的吸引力，可以诱惑或欺骗攻击者将时间和资源都用于攻击这个蜜罐上，使它们远离实际的工作网络。因此从某种意义上来说产品型蜜罐减轻了实际工作网络的安全风险。一般情况下，商业组织利用产品型蜜罐对自己的网络系统进行保护。

研究型蜜罐是为了研究和获取攻击者的有关信息而设计的，这类蜜罐并不能增强特定组织的安全性，正好相反，蜜罐此时所要做的工作是研究组织可能会面对的各类网络威胁，并寻找能够对付这些威胁的最好的办法。一般情况下，商业组织不会使用研究型蜜罐，只有那些需要进行研究的组织，例如大学、政府、军队或安全研究机构才需要使用研究型蜜罐。

3.2　牺牲型蜜罐和外观型蜜罐

牺牲型蜜罐是可攻击的系统，可以建立在任何设备上，象 Linux 服务器、Cisco 路由器和 Windows NT 系统等。典型的实现包括加载操作系统，对一些应用程序进行配置，然后将蜜罐放置在互联网上，对发生的各种行为进行查看。系统管理员需要定期检验蜜罐系统，判断整个系统是否已被入侵，在被入侵的情况下还需要判断蜜罐所遭受的攻击类型。

大多数情况下使用蜜罐附近配置的网络嗅探器来收集数据。牺牲型蜜罐提供的是真实的攻击目标,所以得到的结果是真实系统上会发生的情况。牺牲型蜜罐可以对被入侵之前的系统进行分析,但是系统一旦被攻陷就不可能正常工作,因此必须为这类蜜罐配备系统管理员,对它们进行辅助管理。

外观型蜜罐是一个呈现目标主机的虚假映象的系统,通常作为目标服务或应用的仿真软件进行各种工作。当外观型蜜罐受到侦听或攻击时,它就会迅速收集有关入侵者的信息,为追踪攻击者提供有用的线索。外观型蜜罐的性能主要取决于它能够仿真什么样的系统和应用以及它的配置和管理。外观型蜜罐安装和配置比较简单,可以模仿大量不同的目标主机。

4 蜜罐中的主要技术

蜜罐中的主要技术有网络欺骗、端口重定向、报警、数据控制和数据捕获等。

4.1 网络欺骗技术

为了使蜜罐对入侵者更具有吸引力,就要采用各种欺骗手段。例如,在欺骗主机上模拟一些操作系统或各种漏洞、在一台计算机上模拟整个网络、在系统中产生仿真网络流量等。通过这些方法,使蜜罐更象一个真实的工作系统,诱使入侵者上当。

4.2 端口重定向技术

利用端口重定向技术,可以在工作系统中模拟一个非工作服务。例如,工作系统运行 Web 服务(端口 80),可以将 telnet(端口 23)和 SMTP(端口 25)重定向到一个蜜罐,由于这两个服务在工作系统中并没有打开,所有对这两个端口的访问(可认为是入侵行为)实际上都在蜜罐系统中,而不是工作系统。

4.3 报警技术

蜜罐必须具备报警功能,当系统被攻击时能够通知管理员,以便进行实时监视和跟踪。

4.4 数据控制技术

蜜罐是专门用于被攻占的系统,但不能允许入侵者将它作为跳板去攻击其他系统,因此要控制系统的数据流量而不被入侵者怀疑。入侵者攻占一个系统后,最需要的是网络连接,以便从网上下载工具包,这正是要分析的内容,因此必须给入侵者做这些事情的权利。

4.5 数据捕获技术

要在不被入侵者发现的情况下,捕获尽可能多的信息,包括输入/输出信息、击键和屏幕信息等,以便从中分析他们所使用的工具、策略和动机。这可能要对系统作一些修改,但尽量要少,以免被入侵者发觉。捕获的数据不能放在蜜罐主机上,否则容易被入侵者发现,让他知道这是一个蜜罐系统,这时他会销毁证据。因此要将数据记录在远程安全的主机上。

5 常见蜜罐产品介绍

蜜罐是一个可以模拟具有一个或多个攻击弱点的主机的系统,为攻击者提供一个易于被攻击的目标。下面分别对常见的蜜罐产品进行介绍。

5.1 DTK

DTK(Deception Toolkit,欺骗工具包)是由 Fred Cohen 开发的蜜罐工具,它是一个免费软件,可以在互联网上找到。它是 Perl 脚本的集合,运行于 Unix 平台,模拟了许多已知的漏洞。它提供了一个假的口令文件,欺骗入侵者花时间去破译口令。DTK 也有很好的报警功能,一旦检测到攻击就会通知管理员。DTK 的优点是可以修改脚本模拟任何你需要的漏洞,缺点是安装、设置比较复杂,而且只能收集针对已知漏洞的攻击。

5.2 BOF

BOF(Back Orifice Friendly)是一种简单但又十分实用的蜜罐,运行在 Windows 操作系统环境中,目前也已出现了基于 Unix 环境的产品。它模拟了一些基本的服务,包括 http、telnet、ftp、Back Orifice 等。一旦检测到对这些端口的连接,BOF 就进行监听并作记录。BOF 还提供了"假应答"选项,使攻击者可以顺利地连接。通过这种方式可以记录 http 攻击、telnet 暴力穷举登录以及其他的一些活动。当有人利用自动扫描工具扫描系统时,它可以产生一个报警信号,及时通知管理员。BOF 的主要价值在于检测,可以监控指定端口的行为,这些端口往往是攻击者最感兴趣的。

5.3 Spector

Spector 是属于比较简单的产品类蜜罐,运行于 Windows 平台。与 BOF 类似,它的主要功能是模拟服务,不过它可以模拟的服务和功能范围更加广泛,除了可以模拟服务之外,它还可以模拟多种不同的操作系统。Spector 能模拟 5 种不同的网络服务(SMTP、Telnet、Finger 和 Netbus),另外还能模拟 9 个不同的操作系统(Windows NT、Windows95/98、MacOS、Linux、SunOS/Solaris、Digital UNIX、NeXTStep、Irix 和 Unisys UNIX)。Spector 具有自动捕获攻击者活动的能力,所有连接的 IP 地址、时间、服务类型和引擎的状态等信息都记录在远程主机上。Spector 的价值在于检测,它可以快速并轻松地判断出谁在干什么。它在有些方面的信息收集相对比较被动,例如 Whios 和 DNS 查询;而在有些方面比较积极,例如收集端口扫描攻击者的信息。

5.4 Honeyd

Honeyd 是由 Niels Provos 创建的一种功能强大的具有开放源代码的蜜罐，运行在 Unix 系统上，可以同时模仿上千种不同的计算机，同时呈现上千个不同的 IP 地址。Honeyd 主要用于攻击检测，它对那些没有使用的 IP 地址进行监控，这些没有使用的 IP 地址自然也就没有操作系统。无论攻击者何时试图侦听或攻击一个不存在的系统，Honeyd 都会通过 ARP 欺骗通过模拟的服务与攻击者进行交互，这些模拟的服务其实就是一些对预先设定好的行为进行反应的脚本。例如，脚本可以伪装为一个具有 Cisco IOS 登录界面的 Cisco 路由器的远程登录服务。只要建立连接，攻击者就相信他们正在交互的是一个真正的系统。

Honeyd 不仅可以自动与攻击者进行交互，还可以检测任何端口上的行为。Honeyd 可以用于创建虚拟陷阱网络或者用于普通的网络监控。

5.5 Mantrap

Mantrap 是由 Recourse 开发的比较复杂的商业产品，运行于 Solaris 操作系统上。它不是简单地模拟一些服务，而是在 Mantrap 主机上创建了 4 个称为“监狱”的子系统，每个子系统都运行与主机相同的操作系统，但为了维护欺骗功能会有一些小小的改动。每个“监狱”在功能上可以是独立的，也可以相互关联。可以在这些“监狱”上安装应用程序、开启各种服务等，这使得它具有更大的灵活性。对攻击者而言有一个完整的系统可以交互，并有许多应用程序可以攻击，所有这些活动都被捕获或记录。

Mantrap 可以收集针对任何已知或未知漏洞的攻击，但它也有局限性，只能在 Solaris 系统上运行，而且一旦系统被攻占，可以被入侵者用来攻击其他的系统。Mantrap 一般作为产品类蜜罐，以减轻实际工作网络的安全风险。

6 蜜罐在网络系统中的部署

蜜罐可以放置在网络的任何位置，可在防火墙内或防火墙外。产品型蜜罐一般是单个的系统，通常与要保护的工作系统放在一起，以吸引攻击者。例如，若要保护公司网络内部主机的安全，可将蜜罐部署在网络内部(防火墙内)；若要保护 WEB、FTP、DNS、HTTP 等服务器，则将它部署在防火墙内外面。

是否成功地部署蜜罐依赖于许多因素，包括如何设置蜜罐主机名、部署在何处、蜜罐本身的可靠程度以及合适的蜜罐策略。如何命名蜜罐主机名是很重要的，攻击者往往对金融、管理、数据库服务器等比较感兴趣，可以给蜜罐取一个类似的名字以吸引他们的注意。制定一个合适的蜜罐策略也非常重要，因为蜜罐不仅可以吸引外部攻击，还可以吸引内部攻击，如何处理内部攻击就是需要预先制定的策略。没有合适的策略，面对大量的内部攻击往往会不知所措，最后可能撤消蜜罐以息事宁人。

7 蜜罐的发展方向

蜜罐为整个安全界注入了新鲜血液，它不仅可以用作独立的信息安全工具，还可与其他安全工具象防火墙、IDS 等协同使用。蜜罐可以查找并发现新型攻击和新型攻击工具，从而弥补了 IDS 中无法对新型攻击迅速做出反应的缺点。

面对不断改进的黑客技术，蜜罐要保持目前所具有的技术优势，就必须不断改进和发展。以下几点是蜜罐的发展方向：

7.1 增加蜜罐可以模拟的服务

只有不断增加蜜罐可以模拟的服务，才可以获得更多的黑客信息从而达到蜜罐的设计目的。

7.2 跨平台蜜罐

目前的操作系统多种多样，大部分蜜罐只能在特定的操作系统环境下工作。如果蜜罐能够在多种操作系统环境下工作，那么使用者的范围会不断扩大，同时使用者也可以更加方便地使用蜜罐。

7.3 提高蜜罐与入侵者之间的交互程度

蜜罐如果只支持简单的交互行为，入侵者就会很快发现自己所处的环境，并迅速退却。所以蜜罐技术不断进步的同时，必须尽量提高与入侵者之间的交互程度，以便更好地了解入侵者的行为。

8 结束语

蜜罐已经成为安全专家们所青睐的对付黑客的有效工具之一。它们不仅可以捕获那些不熟练的入侵者，还可以发现大量的新型攻击工具，并在这些工具广泛传播之前就由安全专家找到降低这些工具效用的有效方法。蜜罐不仅可以捕获到防火墙之外的入侵者，还可以发现自己组织内部的入侵者。可以预见，蜜罐的发展前景是非常美好的。

参考文献

1 马艳丽、赵战生、黄轩，Honeypot—网络陷阱，计算机工程与应用，2003，39(4)：162～165。

2 赵双红、刘寿强、夏娟，基于诱骗式蜜罐系统设计与应用，计算机安全，2003，10：19～22。

3 熊华、郭世泽等，网络安全—取证与蜜罐，人民邮电出版社，2003 年.97～136。

4 王利林、许榕生，基于主动防御的陷阱网络系统，计算机工程与应用，2002，38(17)。

5 刘宝旭、许榕生，主动型安全防护措施——陷阱网络的研究与设计，计算机工程，2002，28(12)：9～16。