解析蜜罐技术在网络安全中的应用

孙印杰[1,2],王 敏[1],陈智芳[1]
(1.河南师范大学 计算机与信息技术学院,河南 新乡 453007;
2.阿克苏职业技术学院 计算机系,新疆 阿克苏 843000)

摘 要:随着网络环境的逐渐复杂,安全问题日益突出。文中着重讨论的蜜罐技术,不同于以往的被动防御,而是采取主动防守,诱惑黑客上钩,最后抓捕黑客。主要从蜜罐技术的概念、关键技术、与传统的安全工具相比的优势、蜜罐技术的发展及其实现等各方面进行详细分析。蜜罐主机采用伪装成多种主机或服务器系统,对黑客攻击具有主动应对策略,并能作出不同反应,因此提高了网络的安全性。结合具体实例,证明了蜜罐技术是网络安全由被动防守到主动防御的开始,具有广阔的发展前景。

关键词:蜜罐技术;黑客;入侵诱骗技术;网络安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)07-0129-04

Analysis Honeypot Technology Application in Network Security

SUN Yin-jie[1,2], WANG Min[1], CHEN Zhi-fang[1]
(1.Department of Computer Science and Information Technology, Henan Normal University, Xinxiang 453007, China;
2.Department of Computer Science, Akesu Vocational and Technical College, Akesu 843000, China)

Abstract: Along with gradual complications of the network environment, the safe problem is increasingly outstanding. Emphasizes a discussion of honeypot technology, differ from former passive defense, but adopt to defend actively, lure a hacker to take the bait, grasp a hacker finally. The advantage that this text mainly compares from the concept of the honeypot technology, the key technology, the traditional safe tool, the honeypot technology develop and its realizationin etc. The honeypot host disguised various hosts or server system, having to reply strategy actively to the hacker attack, and can do a response dissimilaritily, so raised the safety of network. Combine concretely examples, proved honeypot technology is a network safety from passive defend to the beginning of the actively defensive, have vast development foreground.

Key words: honeypot technology; hacker; invasion traps technology; network security

0 引 言

随着计算机网络的迅速发展,越来越多的人们依赖网络工作、学习,而网络环境却变得越来越复杂,网络安全问题日益突出。在保护网络安全方面,传统方法是利用防火墙(firewall)和各种防病毒软件,虽经仔细配置,通常能够降低网络的安全风险。但仅仅使用防火墙,网络安全是远远不够的。因为入侵者还可以寻找到防火墙背后敞开的后门,再加上性能的限制,防火墙通常是不能提供实时入侵监测的。所以研究新的网络安全技术已为迫切所需,为此提出了蜜罐技术。它与通常的入侵检测技术的不同之处在于它是一个诱骗技术,让黑客误以为已成功入侵,实则尽在掌握之中,能够使黑客迅速"落网"[1]。

收稿日期:2007-10-16
基金项目:河南省自然科学基金项目(0511013400,2006520031);河南省教育厅自然科学研究计划项目(0624220039)
作者简介:孙印杰(1964-),男,副教授,硕士生导师,研究方向为多媒体技术、网络安全。

1 蜜罐技术概述

蜜罐技术作为一种新型的网络安全技术,已经得到了国内外很多研究机构和公司的重视。

1.1 Honeypot(蜜罐)技术的概念

密罐技术是收集情报的系统,它是一个用来观测黑客如何探测并最终入侵系统的系统。它意味着包含一些并不威胁系统(部门)机密的数据或应用程序,但对黑客来说却具有很大的诱惑及捕杀能力的这样的一个系统。简单的说也就是放置在你网络上的一台计算机,表面看来像一台普通的机器,但同时通过一些特殊配置来引诱潜在的黑客并捕获它们的踪迹。

现在来比较一台蜜罐和一台没有任何防范措施的

计算机的区别,虽然这两者都有可能被入侵破坏,但是本质却完全不同,蜜罐是网络管理员经过周密布置而设下的"黑匣子",看似漏洞百出却尽在掌握之中,它收集的入侵数据十分有价值;而后者,根本就是送给入侵者的礼物,即使被入侵也不一定查到痕迹。所以说"蜜罐是一个安全资源,它的价值在于被探测、攻击和损害"。因此,设计蜜罐的目的就是为了让黑客入侵,借此收集证据,同时隐藏真实的服务器地址。

Honeypot 不会直接提高计算机网络安全,相反它会吸引黑客进入。所以一台合格的蜜罐必须拥有诸如:发现攻击、产生警告、强大的记录能力、欺骗、协助调查等功能。

1.2 Honeypot 技术与传统的安全工具相比的技术特点、优势

1.2.1 在功能上主动防御

蜜罐系统具有记录、分析黑客入侵过程的功能,这样就可以预先采取有效的手段防御以后类似的攻击;由于吸引了黑客的入侵,使其花在陷阱机上大量的时间和精力,从而确保了真实机的安全[2]。

1.2.2 在应用上适用范围广泛、使用灵活,可以伪装任何系统和服务

在任何规格的网络上都可以使用,模块化结构,便于实现功能的增减。远程主机的管理控制台,实时进行控制、配置、监视和跟踪。

1.2.3 能够捕获未知攻击,降低漏报率

使用蜜罐技术能够收集到新的攻击工具和方法,而不像目前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。

1.2.4 概念和技术简单

相对入侵检测等其他技术,蜜罐的误用和错误配置较少,使得安全人员能够比较容易地掌握黑客攻击的一些知识。

1.2.5 存在的不足

当然,Honeypot 技术也存在不足,比如 Honeypot 部署会给网络引入一定的安全风险,特别是高交互蜜罐。也只能检测和捕获那些和它进行交互的攻击行为,不能直接防护有漏洞的信息系统。

1.3 Honeypot 的关键技术

Honeypot 系统的主要技术有网络欺骗技术、数据控制技术、数据收集技术、报警技术、入侵行为重定向技术等。

1.3.1 网络欺骗技术

为了使 Honeypot 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 Honeypot 更像一个真实的工作系统,诱骗入侵者上当。

1.3.2 数据控制技术

数据控制就是对黑客的行为进行牵制,规定他们能做或不能做某些事情。当系统被侵害时,应该保证 Honeypot 不会对其他的系统造成危害。一个系统一旦被入侵成功,黑客往往会请求建立因特网连接,如传回工具包、建立 IRC 连接或发送 E-mail 等。为此,要在不让入侵者产生怀疑的前提下,保证入侵者不能用入侵成功的系统作为跳板来攻击其他的非 Honeypot 系统。

1.3.3 数据收集技术

这是设置蜜罐的另一项技术挑战,蜜罐监控者只要记录下进出系统的每个数据包,就能够对黑客的所作所为一清二楚。蜜罐本身上面的日志文件也是很好的数据来源。但日志文件很容易被攻击者删除,所以通常的办法就是让蜜罐向在同一网络上但防御机制较完善的远程系统日志服务器发送日志备份。

1.3.4 报警技术

要避免入侵检测系统产生大量的警报,因为这些警报中有很多是试探行为,并没有实现真正的攻击,所以报警系统需要不断升级,需要增强与其他安全工具和网管系统的集成能力。

1.3.5 入侵行为重定向技术

所有的监控操作必须被控制,这就是说如果 IDS 或嗅探器检测到某个访问可能是攻击行为,不是禁止,而是将此数据复制一份,同时将入侵行为重定向到预先配置好的 Honeypot 机器上,这样就不会攻击到人们要保护的真正的资源,这就要求诱骗环境和真实环境之间切换不但要快而且要真实再现。

在陷阱系统中如何保护蜜罐自身的安全也是一个很重要的同题。可以采用在真实操作系统上架构陷阱系统的方法。在系统内核和蜜罐之间创建一个内核套作为系统和蜜罐之间的接口。这样使蜜罐能直接访问到内核,起到很好的隔离作用。即使蜜罐被攻击者成功控制,也不会威胁到真实机的安全。所以需要蜜罐系统不断升级,并增强与其他安全工具和网管系统的集成能力。

2 蜜罐系统的实现

在实际的应用过程中,蜜罐系统的实现是多样的,可以是软件的,也可以是硬件的。最主要的是两类:模拟主机的诱骗(模拟易受攻击的服务器软件,如模拟 WWW,FTP,E-mail 服务器软件的某一版本,对前来的请求按照该版本的服务器软件的规范进行响应)和

模拟网络的诱骗(模拟路由器、交换机、各种服务,以及网络中的数据传输。这种方法的优点在于整个入侵诱骗系统的集成度高,易于控制和证据收集,也有利于数据的融合)。最常用的、最简单的蜜罐就是在外网上(与 Internet 相联)有一台计算机运行没有打上补丁的微软 Windows 或 Linux 或 NT 等,然后在计算机和 Internet 连接之间安置一套网络监控系统。如:BOF(Back Officer Friendly),模拟一些基本的服务,包括 HTTP、FTP、SMTP、POP3、IMAP2、Telnet、Back Office 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、远程登录、蛮力登录以及其他的一些活动。NetCat 被誉为网络安全界的"瑞士军刀",是一个简单而有用的工具,通过使用 TCP 或 UDP 协议的网络连接去读写数据。它被设计成一个稳定的后门工具,能够直接由其他程序和脚本轻松驱动,因而被黑客广泛使用。但同时,它也可以作为蜜罐使用。其原理是 NetCat 可以帮助人们在一些端口上绑定服务,这样就允许在 Linux,NT,FreeBSD 上建立一些如 Sendmail,DNS,Telnet,FTP 甚至是 Web Sever 等的虚假服务。Mantrap(捕人陷阱)是由 Recourse 公司开发的一个比较高级的业务型蜜罐,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 主机上提供了 4 个逻辑上的操作系统环境。每一个这样的环境都如同一个独立运行的操作系统。这些逻辑上的操作系统环境被称为"牢笼"。每个"牢笼"在功能上可以是独立的,也可以相互关联。Tigersuite 是一个安全具的汇编软件,其中有多个模块具有蜜罐的功能:ICMP 状态模块用于收集当前被哄骗之后流入和流出网络的 ICMP 消息;网络参数模块主要用于扫视定位信息,它对在受到攻击前检测成功的配置哄骗更改和当前路由/网络设置是很有益的;TCP 状态模块、UDP 状态模块可以用于监控攻击数据包;TigerSim 虚拟服务器可以模拟 DNS Sever,WEB Sever,FTP Sever,POP3 Sever,SMTP Sever,Telnet Sever 等服务器守护程序;会话嗅探器可以用于监听目标渗透、确认哄骗技术、记录攻击痕迹[3]。

3　Honeypot 的发展

3.1　Honeynet

Honeypot 物理上是一台单独的机器,简单的密罐已无法掌握人侵者的最新攻击技术。由多个系统和多个攻击检测应用组成的 Honeynet(蜜网)系统就应运而生。蜜网是一种高交互性蜜罐,不是单一的系统而是一个网络。现在以 HoneyWall 和 Sebek 为关键技术的第二代蜜网趋于成熟(如图 1 所示)。集成了第二代蜜网所需的所有数据控制和捕获工具的第一张自启动光盘(名为 Eeyore)也已推出。第三代蜜网技术产品—Roo 也已经研制出来。在 Roo 版本中,提供了一个基于 Web 界面的非常友好的数据辅助分析工具 Walleye,这使得蜜网技术更加完整。

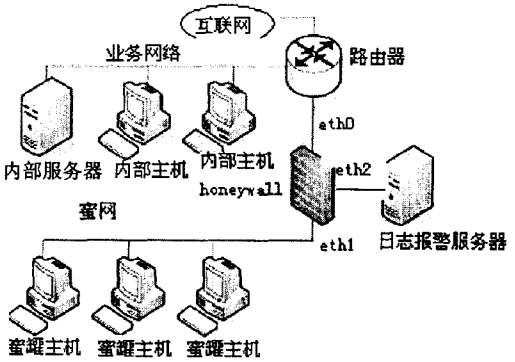

图 1　第二代蜜网系统

最常见的 Honeynet 建置元素有:

(1)防火墙。

它记录了所有进出的连线且提供了 NAT 的服务和 DOS 的保护。

(2)入侵检测系统(IDS)。

IDS 和防火墙有时会放置在同一个位置,对所有进出蜜网的数据进行捕获和控制,然后对所捕获信息加以分析,以便获取关于入侵者的一些情报。

(3)远端日志电脑。

稍微修改成所有的入侵者的指令能够传送到系统日志。系统日志通常设定成远端的系统日志。

(4)Honeypot。

可以放置任何类型的系统来充当蜜罐,如 Solaris、Linux、Windows NT、Cisco 交换机等。这样,就为入侵者创造了一个感觉更真实的网络环境。同时通过对各个系统配置不同的服务,例如 Linux DNS、Windows NT Web 服务器或者 Solaris FTP 服务器,就可以了解入侵者使用的各种工具和战术。当设定 Honeypot 时,要做小小的改变,以免入侵者查觉到这是一个 Honeynet。

蜜网技术最大的应用目标是提供一个高度可控的环境,对互联网上的各种安全威胁(包括黑客攻击、恶意软件传播、垃圾邮件等)进行深入的了解与分析,从而为安全防御提供知识和经验支持。以下是一个蜜网系统的应用实例,通过这个典型的攻击案例——Win32 平台"高波 蠕虫变种传播,来展示蜜网技术的应用价值。

整个分析过程如下:

a. 自动告警工具发出告警邮件,显示 Windows XP 蜜罐主机有指向外部 RPC 端口的网络连接。

b. 查看日志服务器上的 Sebek 服务器端页面，没有发现任何键击信息，判断是被恶意软件所感染。

c. 查看 HoneyWall 上的 Snort 报警信息，发现恶意软件通过攻击 RPC 端口感染蜜罐主机，随后蜜罐主机向攻击主机发起 TFTP 连接获取数据。

d. 分析 HoneyWall 上的记录全部网络流量的 pcap 文件，根据攻击主机 IP、TFTP 端口找到对应网络连接数据包。通过 ethreal 重组网络连接发现获取文件后存放在蜜罐主机上的

c: \ windows \ system32 \ msgdl1. exe，在蜜罐主机对应目录找到恶意软件样本。

e. 通过 www. virustota1. com 查询，确认该恶意软件为“高波”蠕虫变种。

f. 继续查看蜜罐感染“高波”蠕虫变种后的行为。在 IPTables 的日志中发现蜜罐对外部主机的 RPC 端口发起大量的网络连接，但由于 IPTables 的外出流量限制均被丢弃[4]。

3.2 虚拟蜜网

使用 VMWare 或 User - Mode Linux 将多个虚拟系统设置在一台物理机上，通过这种方式，在防火墙构架下，就构成了虚拟 honeynet（如图 2 所示的网络拓扑）。虚拟系统可以使我们在单一主机系统上运行几台虚拟计算机。虚拟蜜网大大降低了成本、占用空间以及管理蜜罐的难度。此外，虚拟系统通常支持“悬挂”和“恢复”功能，这样就可以冻结安全受危及的计算机，分析攻击方法，然后打开 TCP/IP 连接及系统上的其它服务[5]。

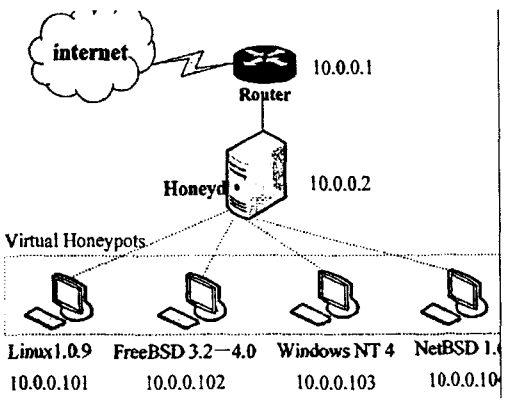

图 2 虚拟蜜网网络拓扑

4 结束语

讨论了基于 Honeypot 理论的网络入侵诱骗技术，它不同于一般的被动防范，而是一种主动防御的安全技术。随着越来越多的用户开始在网络中使用 Honeypot，更多的产品将会被开发。蜜罐技术的最终目标是能够对高智商和反应敏捷的黑客进行欺骗，而现有的蜜罐技术还远未成熟，在欺骗的复杂性、部署维护的难度及范围上都还存在着较大的缺陷，所以要形成成熟的蜜罐技术是非常具有挑战性的。另外，蜜罐技术作为网络安全中的一个新兴领域，是对现有安全体系的一个重要补充，对提高网络安全性起着重要的作用。随着网络入侵类型的多样化发展，蜜罐也必须进行多样化的演绎，只有这样才能够更好地保护国家集体以及个人的财产安全。

参考文献：

[1] 徐超汉，柯宗贵. 计算机网络安全实用技术[M]. 北京：电子工业出版社，2005.

[2] 张 斌. 黑客与反黑客[M]. 北京：北京邮电大学出版社，2004.

[3] 刘彦保. 入侵诱骗技术分析及模型建立[J]. 河南科学，2006，24(4)：532 - 535.

[4] 诸葛建伟，张芳芳，吴智发. 撒下蜜网研究黑客[J]. 电脑安全专家，2005(7)：21 - 23.

[5] Artail H, Safa H, Sraj M, et al. A hybrid honeypot - framework for improving intrusion detection systems in protecting organizational networks[J]. Computers & Security, 2006, 25(4)：274 - 288.

（上接第 128 页）

及开发支持 RAD 的 C/S 框架的必要性，给出了一个基于 MVC 的通用 C/S 应用开发框架，介绍和分析其主要功能及运行原理，并在各个主要方面与传统 C/S 框架做了比较分析。通过实际项目的使用，验证了框架的可行性和可靠性，大大提高了软件复用率和缩短了开发软件开发周期，保证了软件质量及按时交付。

参考文献：

[1] Chen Xin. 应用框架的设计与实现——. NET 平台[M]. 温昱，靳向阳，译. 北京：电子工业出版社，2005.

[2] Patrick A S. Building trustworthy software agents[J]. Internet Computing, IEEE, 2002, 6(6)：46 - 53.

[3] Gamma E. 设计模式：可复用面向对象软件的基础[M]. 李英军译. 北京：机械工业出版社，2007.

[4] Johnson R. J2EE Development Frameworks[J]. IEEE Computer, 2005, 38(1)：107 - 110.

[5] 杨 涛，周志波，凌 力. 基于 Struts 和 Hibernate 的 J2EE 快速开发框架的设计与实现[J]. 计算机工程，2006(10)：83 - 85.