基于Honeypot技术的网络入侵检测系统

郑君杰[1]，肖军模[2]，刘志华[1]，王晓蕾[1]，王宏涛[1]

(1. 解放军理工大学气象学院 南京 211101; 2. 解放军理工大学通信工程学院 南京 211107)

【摘要】利用Honeypot(蜜罐)技术设计了一种新的网络入侵检测系统。Honeypot技术是入侵检测技术的一个重要发展方向，已经发展成为诱骗攻击者的一种非常有效而实用的方法，不仅可以转移入侵者的攻击，保护主机和网络不受入侵，而且可以为入侵的取证提供重要的线索和信息，成功地实现了对网络入侵的跟踪与分析，具有一定的实用价值。

关 键 词 攻击; 蜜罐; 网络安全; 入侵检测

中图分类号 TN393.08 文献标识码 A

Network Intrusion Detection System Based on Honeypot

ZHENG Jun-jie[1]，XIAO Jun-mo[2]，LIU Zhi-hua[1]，WANG Xiao-lei[1]，WANG Hong-tao[1]

(1. Institute of Meteorology, Liberation Army University of Science and Technology Nanjing 211101;

2. Institute of Communication Engineering, Liberation Army University of Science and Technology Nanjing 211107)

Abstract At present, the network security has become a global problem. The traditional network security measures can only detect the known intrusion. The honeypot has become a valid method to trap the attackers. In this paper, a new network intrusion detection system is designed based on the Honeypot technology. the tracking and analysis for network intrusion are realized. that this method is useful.

Key words attack; honeypot; Internet security; intrusion detection

近年来随着计算机技术的不断发展，网络规模不断扩大，网络系统遭受的入侵和攻击也越来越多，网络信息安全问题变得越来越突出。传统意义上的网络信息安全措施都只能检测到已知类型的攻击和入侵，对未知类型的攻击则无能为力。相比之下网络入侵检测技术是一种较新的网络安全策略，具有一定的智能与主动性。网络入侵检测技术的设计的目的是为了从现存的各种威胁中提取有用的信息，发现新的攻击工具，确定攻击的模式并研究攻击者的攻击动机，是一种新的主动防御技术。Honeypot(蜜罐)技术目前已经成为入侵检测技术的一个重要发展方向，它不仅可以转移入侵者的攻击，保护主机和网络不受入侵，而且可以为入侵的取证提供重要的线索和信息[1-2]。

1 Honeypot(蜜罐)技术

简单地说，“蜜罐”是一种在互联网上运行的、包含漏洞的计算机系统，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)而设计的，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，因此所有链接的尝试都将被视为可疑的。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。因此蜜罐也可以为追踪攻击者提供有用的线索，为起诉攻击者搜集有力的证据，从这个意义上说，蜜罐就是“诱捕”攻击者的一个陷阱。

在过去几年中，由于脚本攻击工具和自动攻击工具的大量使用，使得网络入侵变得越来越广泛，而传统意义上的信息安全要做的工作是单纯的防御，如防火墙、入侵检测等，目的是防止自己的资源不会受到入侵者的攻击。所谓信息安全就是要尽力保护自己的组织，检测防御中的失误并采取相关的措施。但是安全措施只能检测到已知类型的攻击和入侵，而对未知的攻击手段是无能为力的，因此网络安全专家们试图利用蜜罐技术诱骗并破译黑客的攻击方法，便诞生了Honeynet(蜜网)技术。

收稿日期：2005 – 04 – 13
基金项目：国家自然科学基金重点资助项目(69931040)
作者简介：郑君杰(1977 –)，男，博士生，讲师，主要从事信息安全方面的研究.

Honeynet不是一个单独的系统，而是由多个系统和多个攻击检测组成的网络，所有放在Honeynet中的系统都是标准真实的产品系统。

2 系统设计

在设计蜜罐系统之前必须注意以下问题：(1) 蜜罐系统必须与任何真实的实际系统相隔离，这是因为一旦蜜罐被攻陷，不能让攻击者利用蜜罐对网络中的其它系统进行进一步的攻击；(2) 尽量将蜜罐放置在距离因特网最近的位置，这样，真实的系统就不会因为位于蜜罐和Internet之间而暴露在网络上；(3) 需要有步骤地记录所有通过蜜罐的信息，使得攻击者不可能通过删除自己的日志记录来掩饰自己的行为；(4) 需要建立某种形式的防火墙来控制通过蜜罐的所有信息[3]。

基于Honeypot技术的网络入侵检测系统如图1所示。系统采用客户/服务器模式，包括取证服务器(Server)和安装在构成honeynet的各honeypot主机上的取证客户代理(Client)和IDS(Intrusion Detection System)。所使用的IDS是开放源码的Snort。根据保护目标不同，系统可以被配置在内网用来保护内网主机，也可以配置在外网用来保护FTP、HTTP和E_MAIL等服务器。

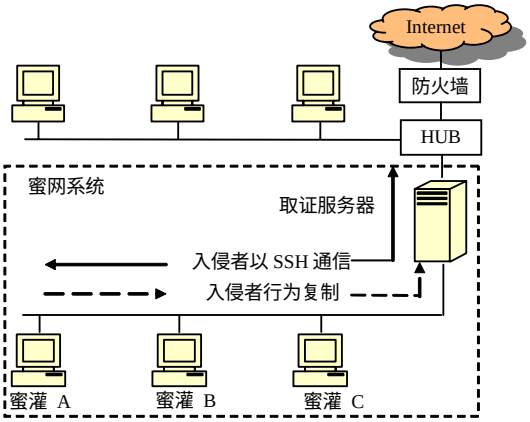

图1 蜜罐系统总体结构

3 系统实现

3.1 取证服务器

取证服务器是Honeynet系统控制和管理中心[4]，主要用来收集攻击者潜在的入侵犯罪证据，重建攻击者的入侵过程，并防止攻击者成功侵入honeypot后，以honeypot为“跳板”攻击其他正常主机。取证服务器采用桥(bridge)模式。桥模式工作在数据链路层，对从端口接收到的MAC帧根据目的地址进行转发和过滤。桥这种模式使取证服务器没有IP地址，没有MAC地址，没有数据报路由以及数据报的TTL消耗，这使取证服务器被构建成为一个对攻击者来说“不可见”的过滤控制设备，使攻击者更难以检测和觉察。通常取证服务器建立在Linux环境下，本系统使用Rad HatLinux9.0。而大多数版本的Linux在默认安装情况下支持桥的功能。另外，取证服务器具有网关功能，它将入侵检测系统同网络其它部分隔离开来，任何进出入侵检测系统的数据包必须经过取证服务器，这样就可以对数据包进行过滤，实现对无论是来自内网还是外网攻击的控制和取证。

攻击者侵入honeypot后，通常会使用明文协议(如FTP、HTTP、Telnet等)进行远程数据交互，通过使用数据流重组技术，入侵检测系统不仅可以看到入侵者所有的会话内容，而且可以看到入侵者看到的输出内容。然而，随着加密技术的发展，现在即使最普通的攻击者也可以利用SSL、SSH等加密手段保护同被入侵主机进行通信的通道。使用数据流重组技术我们得到的将是内容被加密的TCP数据流，如果通过解密的方法观察入侵者的会话内容，这将是异常困难的。因此可考虑设法绕过解密方法获得有关内容，在系统内核收集有关解密数据，这样入侵者在honeypot中的行为入侵检测系统完全透明。不仅可以获得入侵者的键入命令，而且如果入侵者向受害主机复制文件，取证客户代理将会记录该行为并产生完全相同的复制；如果入侵者上传会话，入侵检测系统将看到完全的交互信息。

3.2 取证客户代理Client

取证客户代理是数据捕捉工具，主要用来捕捉发生在honeypot中所有有关入侵的数据，帮助准确重建攻击者侵入系统后的行为。取证客户代理可以记录用户系统调用访问的所有数据，然后以标准格式表示，并采用UDP方式隐蔽发送给取证服务器。由于捕捉的数据以自定义标准格式的表示，因此服务器可以收集运行在不同操作系统上的honeypot发送的数据。

3.2.1 数据捕捉

在SSH会话中，键入命令被解密后发送到Linux的shell命令窗口执行，这是典型的系统调用。因此当数据刚被解密后，并准备发送给下一过程之前，我们可以在系统内核访问到该数据并进行必要的操作。这样就可以避开复杂地解密，实现捕捉攻击者的键入命令，传输文件和口令等取证目的。

当过程在用户空间调用标准的read()函数时，在

系统内核产生相应的系统调用，并指向系统调用来表示表中相应的位置。本文采用新定义的new_read()函数替代原标准read()函数。这样过程调用标准的read()函数时，就相当于调用New_read()函数，就可以看到系统调用访问的所有数据。New_read()函数完成的功能包括：调用原read()函数，将内容复制到包缓冲区内(Packet Buffer)，加上数据包头形成标准表示格式，然后发送给服务器等功能。

3.2.2　数据发送

取证客户代理捕捉到数据后，需要在入侵者无法觉察的情况下，将数据发送给服务器。如果客户代理程序简单使用UDP数据包发送数据，入侵者就可以使用sniffer等工具非常简单地检测这些数据的存在。因此数据包在发送之前，必须采用某些措施修改内核阻止入侵者看到这些数据包。蜜罐系统产生数据包的方式如图2所示。

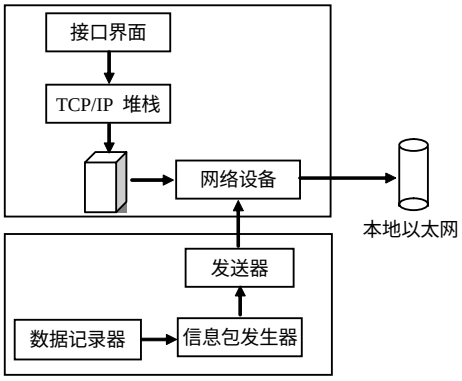

图2　蜜罐系统数据包产生概念图

首先构建数据包产生发送的隐蔽信道。对每个read()请求，取证客户端程序产生一个或多个日志数据包。每个数据包包括一条记录，这条记录记录了产生调用的用户、产生调用的过程，产生调用的时间，数据记录的长度以及数据本身等。数据包不使用TCP/IP堆栈，完全在取证客户端程序内产生，数据包产生后，绕过原始socket代码以及包过滤代码，被直接发送到网络设备驱动接口。这样任何主机内用户不可能使用Iptable阻止和使用基于Libpcap的Sniffer捕捉到该数据包。

另外，为防止不同honeypot主机之间相互检测到发送数据包，在数据包头内预设UDP端口号和相同的Magic字段数字标识，当其它主机收到并检测到这样的数据包后，就忽略该数据包。

取证客户代理同服务器之间的数据传送采用用户数据报协议UDP。为保证数据包安全发送和服务器正确接收和记录，发送的数据包增加了48字节的固定标识头。

当取证客户代理程序截获read()系统调用时，不仅记录读出的内容，而且记录过程ID、用户ID、文件描述符FD和键入命令的前12个字符等相关内容写入数据包的附加固定头中。如果记录的数据长度大于MTU，客户代理程序将数据进行分片，然后分别封装发送。

4　小　结

蜜罐技术已经成为安全专家们所青睐的对付黑客的有效工具之一。它的最大优势在于发现新型的攻击工具。本文利用蜜罐技术设计了一种新的网络入侵检测系统，成功地实现了对网络入侵的跟踪与分析，具有一定的实用价值。目前Honeynet工程已经实现了系统所需的一些基本功能并且源代码是开放的，诸如连接计数控制Counter、网络入侵防护控制Snort_inline、入侵检测系统snort和客户端代理等，为自主开发网络入侵检测系统提供了有利的条件。

值得一提的是入侵者们也在开发各种工具来对抗现有的侦听技术，如将数据包分片再进行重组等，入侵检测系统要想检查出其攻击特征将变的极其困难，所以必须对各种新的攻击方法保持高度的关注。另外，管理和分析Honeynet要耗费管理员大量的精力，管理员需要经常对可疑的网络时间进行深度分析，这需要很长的时间和熟练的分析能力[5]。因此提高系统的智能分析能力也是非常重要的。

参　考　文　献

[1] 肖军模, 刘　军, 周海刚. 网络信息安全[M]. 北京: 机械工业出版社, 2003.
[2] 王　影, 卢显良. 入侵检测规则共享机制[J]. 实验科学与技术, 2004, 2(3): 30-32.
[3] 刘宝旭, 许榕生. 主动型安全防护措施--网络陷阱的研究与设计[J]. 计算机工程. 2002, 12: 98-102.
[4] 齐爱民, 刘　颖. 网络法研究[M]. 北京: 法律出版社, 2003: 263-268
[5] 丁丽萍, 王永吉. 计算机取证的相关法律技术问题研究[J]. 软件学报, 2005, 16(2): 260-275.

编　辑　熊思亮