Linux下主机入侵检测系统的研究

陈 远 周朴雄 （武汉大学信息管理学院 430072）

摘要：主机入侵检测系统主要是根据主机的进程、目录、文件、内存、TCP/IP端口以及到达主机的网络数据包等系统资源的变化情况，实时地判断主机是否被黑客入侵，并阻止黑客的进一步活动或通知防火墙阻断该黑客的源地址。本文主要介绍了当前较为流行的操作系统Linux下主机入侵检测系统的研究设计情况，它对设计其他操作系统平台如Unix、Windows2000下主机入侵检测系统及下一代安全防范系统都有一定的借鉴作用。

关键词：网络安全 入侵检测 黑客攻击 Linux

1 前言

计算机网络在现代生活和工作中的作用越来越重要，人们也越来越依赖网络，但是随之而来的计算机网络安全问题也不断增加，网络的安全成为人们关注的焦点。目前，解决网络安全问题的主要技术手段有加解密技术、防火墙技术、安全路由器等，虽能完成大部分安全功能，但它们多采用静态的安全策略，在防御网络入侵方面具有一定的局限性。网络安全是一个综合的、立体的工程，单纯依靠一些防御工具不可能满足全部的安全要求。入侵检测系统通过动态探查网络内的异常情况，及时发出警报，有效弥补了其他静态防御工具的不足。

2 入侵检测系统

2.1 入侵检测系统的定义

入侵检测系统是近年来出现的新型网络安全技术，它之所以重要就是因为它可以弥补一些传统的安全工具及方法的不足，提高了信息安全基础结构的完整性。入侵检测是指在监视或者在可能的情况下，阻止入侵或者试图控制你的系统及网络资源的那种努力。它主要是用于实现识别在计算机信息网络中未经授权使用计算机系统和滥用合法访问权的活动，检测一切危及计算机及网络系统的完整性、保密性和可用性活动的企图。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

2.2 入侵检测的一般工作过程

一般来说，一次成功的入侵检测分以下几步进行：

第一步：信息收集

入侵检测的第一步是信息收集，内容包括系统、网络、数据及用户活动的状态和行为。而且，需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这除了尽可能扩大检测的范围外，还有一个重要的因素就是从一个点来的信息有可能看不出疑点，但从几个点来的信息的不一致性却是可疑行为或入侵的最好标识。入侵检测利用的信息一般来自以下四个方面：

(1) 系统和网络日志文件

(2) 目录和文件中的不期望的改变

(3) 程序执行中的不期望行为

(4) 物理形式的入侵信息

第二步：信号分析

对上述四类收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过三种技术手段进行分析：模式匹配，统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

第三步：对检测到的入侵行为做出处理

对于检测到的入侵行为，入侵检测系统需要做出相应的反应。这种反应主要包括记录，报警，阻断，或者通知防火墙等方式。入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。

3 主机入侵检测系统

入侵检测系统按照检测的对象划分，可分成主机入侵检测系统和网络入侵检测系统。主机入侵检测系统是通过分析计算机系统提供的各种资源信息，日志信息来实现入侵检测，它运行在需要保护的机器上。当攻击数据包抵达目的主机后，防火墙和网络监控已经无能为力了。这时我们可以求助于"基于主机的入侵检测"，基于主机的入侵检测的优点是能够深入检测系统内部的活动，确切掌握系统活动的细节，检测在网络数据流中难以发现的活动，它可以检测操作系统级的事件(如系统调用、系统CPU资源、I/O资源、内存资源、磁盘资源、系统对象访问情况等)，也可以检测应用级的事件(如数据库应用、网络应用等各种应用程序运行情况)。基于主机的入侵检测不受网络拓扑结构和通信加密的限制，缺点是它需要占用宝贵的主机资源，而且基于主机的入侵检测强烈地依赖操作系统本身的安全性，本文所采用的正是这种技术。

3.1 主机入侵检测策略

黑客攻击过程可以分为信息搜集，寻找漏洞，实施攻击等三步，黑客要实现下一步的攻击步骤，必须有上一步的攻击结果为基础，也就是说，黑客攻击过程的每个环节都是紧密联系的，因此，如果我们能在黑客的每个攻击步骤都有所防范，能有效地检测出每个攻击步骤、每个攻击手法，并实时地加以阻止，不但能抑制这个步骤进一步活动，还能对下一步攻击过程产生影响，尤其对黑客的整个攻击过程有较大的阻碍作用。所以，主机入侵检测策略就是对每个攻击步骤、每个攻击手法都制定一个相应的检测模块，负责对该攻击手法进行检测监控，如果一旦发现有入侵检测行为，则立即加以阻止，或者杀死导致攻击的进程，或者阻挡实施攻击的主机地址。

3.2 主机入侵检测模型

根据主机入侵检测策略，在此介绍一个与它对应的主机入侵检测模型，该模型由系统检测监控管理模块、各种攻击检测监控模块、主机保护代理模块、主机保护模块组成。

(1) 系统检测监控管理模块：系统检测监控管理模块管理各个检测监控模块的配置、运行等，它从配置文件中读取配置信息，并启动需要运行的检测监控模块，该模块还对每个检测监控模块进行配置，供它们运行时使用。

(2) 攻击检测监控模块：攻击检测监控模块与每种攻击手法一一对应，用来检测监控各种攻击手法，当发现攻击时通知主机保护代理模块，由主机保护代理模块通知其他保护模块进行阻断保护。

(3) 主机保护代理模块：主机保护代理模块负责接受各个攻击检测监控模块发来的警告、阻断或保护等消息，根据收到的消息再转发给主机保护模块、系统监控台模块、以及防火墙实现保护和阻断。

(4) 主机保护模块：主机保护模块实现对主机的保护，主要包括阻断某个远程主机地址、杀死某个进程或停止某个用户的活动等。它接收主机保护代理模块发来的消息，根据消息的内容采取某种措施实施对主机保护，按照上述的主机入侵检测策略和各模块的功能，我们可以设计出主机入侵检测系统总体框架，(见图1)

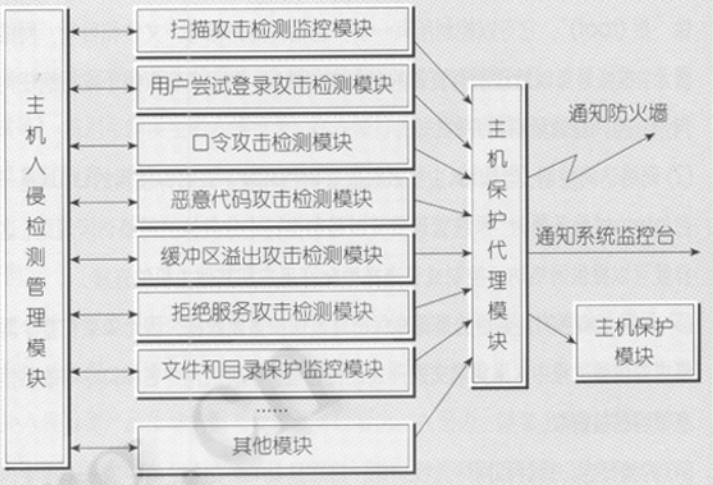

图1 主机入侵检测系统总体框架

4 Linux下主机入侵检测系统的设计

Linux是一个真正意义上的免费的操作系统，从它产生之日起，就以它的稳定性、免费性、可靠性、安全性、开放性受到广大用户的青睐，Linux作为一个多用户、多任务的操作系统，继承了UNIX系统的大部分特点，具有完美的多任务、虚拟内存、支持X Window系统、内置网络支持、支持共享库、同IEEE POSX.1标准兼容、非专有资源代码、费用低于大多数UNIX系统、GUN软件支持等优点，同时又比UNIX小、快而且便宜，这正是Linux流行起来的原因，随着Linux的推广，已经有越来越多的用户加入到Linux的行列，可以说Linux的发展趋势是不可阻挡的，因此基于Linux的主机入侵检测系统研究具有重要的现实意义。

4.1 Linux系统安全

在介绍Linux下主机入侵检测系统之前，我们需要对整个Linux系统自身的安全体系有一个了解，Linux的安全结构主要由以下几部分组成：根用户的自主访问控制、网络访问控制、加密、日志。

(1) 根用户的自主访问控制，Linux的各种管理功能都被限制在一个帐号中，叫

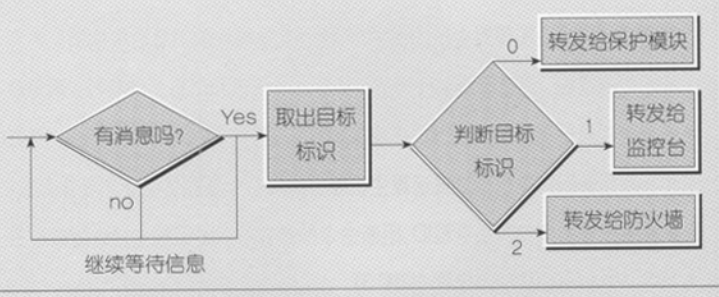

图2 主机保护代理模块流程

做“根(root)”，它可以控制所有一切，包括：用户帐号、文件和目录、网络资源，根帐号可以管理所有资源的各类变化情况，根用户有权授予或拒绝任何用户、用户组或所有用户的访问。

(2) 网络访问控制，当Linux主机系统处在网络环境下或者你使用的Linux是一台Internet服务器时，系统管理员可以强制推行十分具体的网络访问规则，这样就可以提供网络访问控制或有选择地允许用户和其他主机的连接。

(3) 加密，加密的主要目的是提高保密性或保护重要数据，因为如果在整个网络中的传输过程中，采用明文的形式进行通信，系统的用户名和口令等敏感信息很容易被窃取。

(4) 内置日志、审计和网络监视功能，日志是Linux安全结构中的一个重要内容，它可以记录时间信息和网络连接情况，为你提供攻击发生的唯一真实证据，这些信息将被重定向到日志中备查，Linux下有两个重要的日志守护程序：syslog和klogd，syslog以守护进程运行，在启动时它从/etc/syslog.conf文件中读取不同的选项，根据不同的应用程序把相关信息记录到相应的日志文件中，klogd是一个内核日志记录程序，它记录内核出现的任何错误和异常。

4.2 Linux主机入侵检测系统各功能模块

按照主机入侵检测系统的设计策略和组成结构，Linux下的主机入侵检测系统主要可分成主机入侵检测管理模块、主机保护代理模块、主机保护模块、攻击检测监控模块等，下面介绍每个模块的具体设计。

4.2.1 主机入侵检测管理模块

该模块比较简单，主要是管理各个监控模块以及主机保护模块和主机保护代理模块，是一个shell脚本程序，它从配置文件中读取信息，并启动和管理各个子模块的运行。

4.2.2 主机保护代理模块

主机保护代理模块是各个监控模块与主机保护模块、系统控制台和防火墙联系桥梁，它们之间通过socket进行通信，一方面它接收各个监控模块的消息，另一方面，它将这些消息转发给主机保护模块、系统控制台和防火墙，消息由两部分组成，首先是消息目标标识，表明是转发给主机保护模块或者是系统控制台还是防火墙，第二部分是消息具体内容，由主机保护模块、系统控制台和防火墙自己解释执行，主机保护代理模块仅仅将该部分转发给这些模块，图2是该模块的流程图。

4.2.3 主机保护模块

主机保护模块实现对主机的保护，它接收其他模块的消息后根据消息内容采取相应的措施，消息有两部分组成，消息命令标识和消息命令参数，消息命令标识代表需要采取的主机保护模块保护措施，目前具有两个保护措施：杀死进程还是阻断远程主机地址或远程主机名，消息命令参数是命令的具体参数，例如杀死进程指令参数是进程ID，阻断命令的参数可以是远程主机地址或远程主机名，主机保护模块的流程(见图3)。

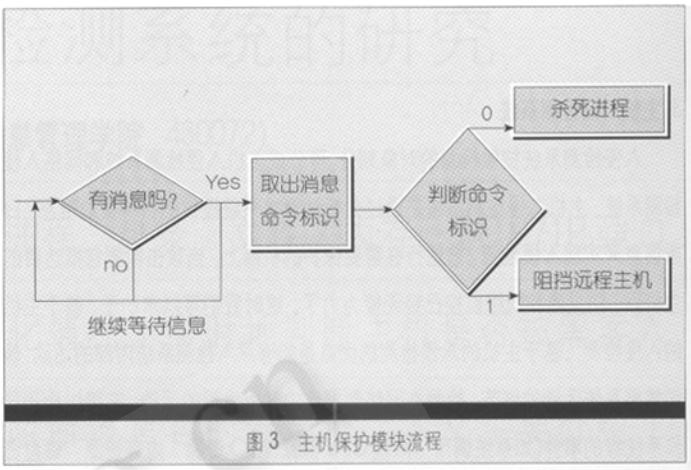

图3 主机保护模块流程

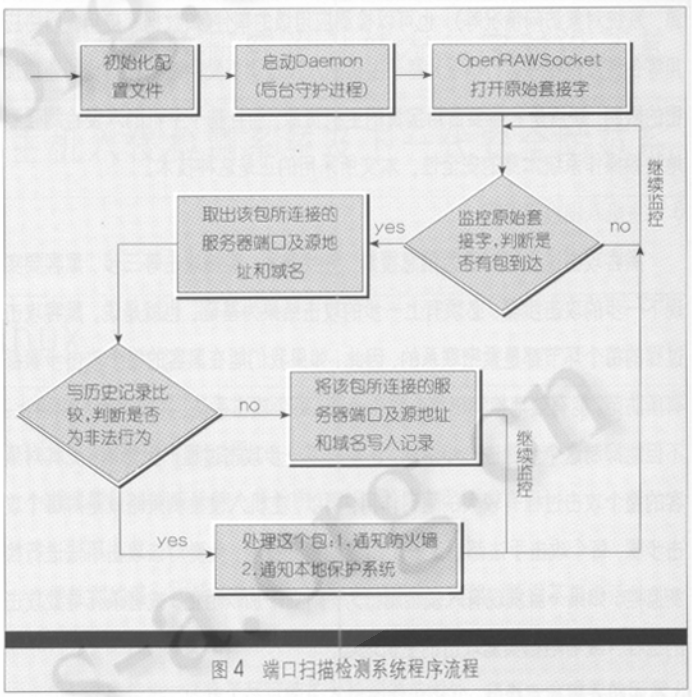

图4 端口扫描检测系统程序流程

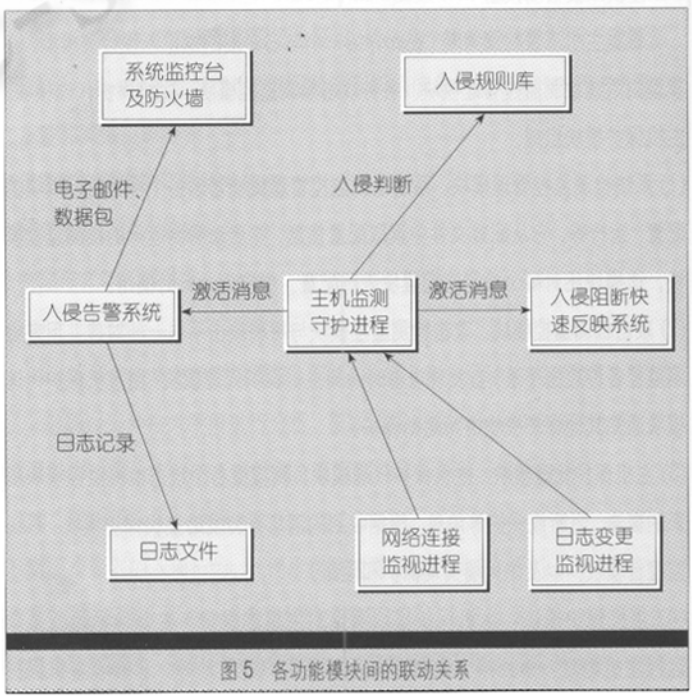

图5 各功能模块间的联动关系

4.2.4 攻击检测监控模块

攻击检测监控模块包括扫描攻击检测监控模块、日志监控模块、缓冲区溢出攻击检测模块、拒绝服务攻击检测模块、文件保护模块、进程保护模块等。由于篇幅的限制，我们仅介绍扫描攻击检测监控模块。黑客扫描主机的一个重要特征就是，黑客在一段极短的时间（一般在几秒以内）向主机大量端口进行连接，所以利用这种特征就可以检测出黑客是否正在进行扫描。要监控这些数据包主要是用到原始套接字，并在后台启动一个守护进程，然后不断地分析传到主机的数据包，如果在规定的几秒内来自某一固定远程主机的数据包连接到本地主机的不同端口的在一定的数量以上，则认为是受到了扫描攻击，并立即采取措施。端口扫描检测系统是用来监控TCP/IP端口活动的监控器。被端口扫描检测系统监控的端口活动都会被报告出来而且可以设置某些参数，包括根据端口活动的来源禁止其对系统进一步的访问。这是一个很重要的防御措施，因为黑客在入侵之前都会试图探查系统的弱点（通过端口扫描）。检测"探查"或端口扫描，可以彻底地防止潜在的黑客入侵系统，让黑客不可能在扫描过端口之后发动真正的攻击。图4是端口扫描检测系统程序流程图。

4.3 系统的各功能模块间的联动

主机入侵监测代理不间断地运行在受保护主机系统中，实时监测主机的各种状态（如进程、文件、网络连接、系统日志、登录尝试等），辨别可能发生的入侵行为，在入侵行为发生的时候自动阻断非法操作，保护主机系统不受入侵。主机入侵检测代理系统的各功能模块间的联动关系。（见图5）

5 入侵检测的智能化发展方向

入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到人们的高度重视，这从国外入侵检测产品市场的蓬勃发展就可以看出。在国内，随着上网的关键部门、关键业务越来越多，迫切需要具有自主版权的入侵检测产品。但现状是入侵检测仅仅停留在研究和实验样品（缺乏升级和服务）阶段，或者是防火墙中集成较为初级的入侵检测模块。可见，入侵检测产品仍具有较大的发展空间，目前，利用专家系统的思想，运用神经网络、遗传算法、模糊技术、免疫原理等方法的智能化入侵检测产品成为研究重点。

参 考 文 献

1 http://www.si.net.cn

2 [美] Simson Garfinkel, Gene Spafford 著， 王启智、申功迈、单和平、牛大刚等译， 实用UNIX和Internet安全技术，北京电子工业出版社，1999。

3 [美] 匿名著， 前导工作室译， 网络安全技术内幕，北京机械工业出版社，1999。

4 [美] 匿名著， 王讽、路晓村、王景中等译， 实用技术：Linux安全最大化，北京电子工业出版社，2000。