Linux 系统内核级安全审计方法研究

贾春福　徐　伟　郑　辉
（南开大学信息技术科学学院，天津　300071）
E-mail：cfjia@nankai.edu.cn

摘　要　LKM（Loadable Kernel Modules-可加载内核模块）技术是 Linux 系统为了扩充系统功能而提供的一种机制。该技术已经被黑客用于系统入侵，同样也可以利用它提高系统的安全性。文章在分析了现行 Linux 安全审计系统所存在问题的基础上，提出了一个基于 LKM 技术的 Linux 系统内核级安全审计模型。

关键词　信息安全技术　安全审计　LKM 技术

文章编号 1002-8331-（2002）06-0053-03　**文献标识码** A　**中图分类号** TP316

Study on Kernel-level Security Audit Techniques of Linux System

Jia Chunfu　Xu Wei　Zheng Hui
（College of Information Technology and Science，Nankai University，Tianjin 300071）

Abstract：LKM（Loadable Kernel Modules）is an important technique used to extend system functions of Linux.LKM has been used by hackers for computer system intrusion，however，it can also be used to improve the security of Linux system.In this paper，The authors first analyze the disadvantages of current Linux audit system，then propose a kernel-level security audit model of Linux system based on LKM technique.

Keywords：Technology of Information security，Security audit system，LKM（Loadable Kernel Modules）

1　引言

安全审计是计算机系统安全管理的一个重要的组成部分。安全审计是记录用户的访问过程和各种行为形成审计数据的过程。对审计数据的分析可以发现系统中的安全问题、识别系统事故责任者、跟踪某些用户和站点，为及时采取相应处理措施提供依据[1,2]。

Linux 是当前流行的 Unix 操作系统家族中的一员，已经广泛受到人们的关注，被越来越多的网站选择作为服务器。与 Windows NT 等操作系统比较，具有开放性开发模式，代码完全公开，而且与 Unix 系统一样，提供了大量的系统工具。Linux 系统缺省的配置强调了系统的可用性，而非安全性，这使得 Linux 容易受到攻击。然而，也正是这一特性，为提高 Linux 系统级和内核级的安全性提供了机会。LKM（Loadable Kernel Modules--可加载内核模块）技术是 Linux 系统为了扩充系统功能而提供的一种非常有用的机制，利用该技术可以对系统的功能进行动态的扩充。这一技术已经被黑客用于系统入侵[3-5]，同样，该技术也可以用于加强系统的安全性，实现系统内核级的一些安全功能。

文章在分析了 Linux 系统现行的安全审计系统的基本状况基础上，提出了一个基于 LKM 技术的 Linux 系统内核级安全审计模型。

2　Linux 系统安全审计系统分析

Linux 系统现行的安全审计机制是在应用程序级实现的，即审计过程是通过一个应用程序实现的，基本结构功能图如图 1 所示。Linux 系统安全审计是利用独立于操作系统的审计程序 syslogd 记录用户登录和相关操作信息的，对用户正常或异常的操作所产生的警告或提示等信息以统一的格式记录下来。针对审计信息获取量不足，常常使用其它辅助程序来获得辅助信息，如利用 TCP Wrapper 等程序辅助记录网络连接信息，用 TripWare 等应用程序管理保留静态程序校验信息，各种相应的服务程序必须同审计程序相配合，提供相关的严格的审计信息，才能得到比较完备的审计记录。

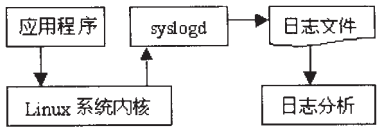

图 1　现行 Linux 审计逻辑结构

由于系统实现安全审计功能的是应用程序，因此，取得了一定权限的入侵活动，按照 syslogd 工作的方式，可以抹掉所有的审计信息和入侵记录；也可以绕过 syslogd，使得审计记录根本就不会产生，使得常规的审计技术对这些入侵活动根本不能察觉或记录入侵。而且，网络的开放性使得计算机系统的攻击者的技术水平很高，早已不是用常规的安全审计技术所能限制的了。

为了克服常规审计方法中的这些缺点，采取同应用服务程序无关的方式记录审计信息，并保护或隐藏保存审计信息文件，就成为了系统审计技术研究中非常重要的问题。从中国《计算机信息系统安全保护等级划分准则》（GB17859-1999）和 TCSEC（Trusted Computer System Evaluation Criteria）中也可以

基金项目：天津市自然科学重点基金资助项目（编号：013600711）
作者简介：贾春福，男，博士，研究方向：信息安全技术、CIMS 支撑技术和 CIMS 优化。

看到，较高安全级别的操作系统，系统管理员的权限也应该受到一定的限制。很明显，这种限制不能在应用程序一级来完成，而应该在系统内核一级来完成。

1999 年 3 月，德国最著名的黑客（Hacker）组织 THC（The Hacker's Choice）在 Internet 上发表了他们的第一篇关于在内核一级的入侵和防护讨论的文章——Complete Linux Loadable Kernel Modules[3]。然后又在 1999 年 7 月份和 2000 年 1 月份，发表了在 FreeBSD 和 Solaris 系统下利用可加载内核模块进行入侵和防护的文章[4,5]。可以说，如果安全技术水平与入侵技术不在同一级别上，也就没有对抗能力可言。因此，如果对于审计技术的研究重点一直放在常规安全审计方法上，很可能在面对黑客（Cracker）在内核一级的攻击入侵时束手无策。从目前大量的漏洞公布中可以发现，内核一级的攻击入侵正逐渐成为黑客（Cracker）入侵的主流技术。可见，安全审计技术也应该建立在系统内核级。

LKM（Loadable Kernel Modules--可加载内核模块）是操作系统内核为了扩展其功能所使用的可加载内核模块。LKM 主要优点是动态加载，无须重新编译整个内核。基于这一特性，LKM 常被用作特殊设备的驱动程序（或文件系统），如声卡驱动程序，等等。但加载后的 LKM 是一段运行在内核空间的代码，这个特性允许利用 LKM 访问操作系统最敏感的部分。黑客（Cracker）利用 LKM 技术可以实现最高级别——内核级的入侵。同样也可以利用 LKM 技术进行系统安全防护。利用 LKM 技术实现安全审计功能可以实现系统内核级的审计功能。

3 Linux 内核级安全审计系统设计

基于以上分析，为了对抗目前已经广泛被采用的内核级的系统入侵技术，Linux 系统安全审计机制在一定安全级别的要求下，应该具备以下特征：

(1)以独立于应用的方式进行审计，并获取足够充分的审计数据，使得审计过程不会受到非法用户的干扰或被获取一定权限的用户绕过。而这样的安全审计要求只能是在系统内核级实现。

(2)有效的审计数据的存储和访问控制，使得审计数据能够得到很好保护，防止用户非法访问审计数据。

(3)另外，自动、智能化的审计数据分析方法和技术，也是安全审计系统中非常重要的部分。对审计数据进行有效的分析，及时准确地发现与安全相关的事件，反映用户的行为，可以帮助系统及时做出响应。

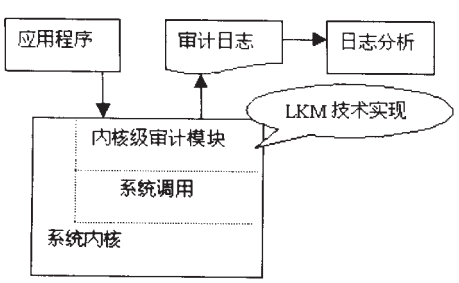

图 2 内核级审计逻辑结构

为此，作者提出了一个 Linux 系统内核级的安全审计模型：利用 LKM 技术实现审计数据的获取和保护，防止审计数据被非法访问；利用数据挖掘技术，实现用户行为的获取与识别，为系统的及时反应提供依据。内核级审计模块的逻辑结构如图 2 所示)。审计模型的具体设计步骤如下。

3.1 审计内容的确定

依据我国计算机信息系统安全保护等级划分准则（GB17859-1999）第三级中关于安全审计的要求，确定如下的审计事件：(1)身份鉴别机制的使用；(2)将客体引入用户地址空间；(3)客体的删除；(4)操作员、系统管理员或(和)系统安全管理员所实施的动作；(5)其它的与安全相关的事件，等等。而每一事件的审计记录项应包括：(1)事件的日期与时间；(2)用户；(3)事件类型；(4)事件成功与否；(5)对于身份鉴别事件审计记录还应包括：请求的来源(如，终端标识符)；(6)对于客体引入用户地址空间的事件及客体删除事件，审计记录还应该包括：客体的名称和客体的安全级别，等等。

3.2 敏感系统调用的确定

根据审计内容，确认直接与审计内容或安全事件相关的敏感系统调用，然后对这些系统调用进行封装，从而实现获取用户使用系统的审计信息。

3.3 审计数据的格式

对审计数据，在封装阶段可以自行定义，但输出格式要依据一定的标准和规范化，目标是实现审计数据获取方便，使用也方便，为审计数据分析奠定基础。依据 Bishop 标准审计格式，组织存储审计数据(参考 SVR4++和归一化审计数据格式)。需要说明的是在内核级获取的审计数据与现行的审计机制获取的审计数据在形式上有一些不同，但并不影响对审计数据的理解。

3.4 利用 LKM 技术实现内核级审计数据的获取

利用 LKM 技术实现基于以上步骤的审计数据获取功能。以上部分是内核级审计机制的最主要部分，是内核级审计技术的基础。由于过多系统内核级操作会影响系统运行速度，而且过多的审计信息会对系统产生很大负载，也会淹没其中最为重要的信息。为了确保对系统的运行和性能影响尽可能小，对审计数据需要依据安全要求进行过滤，设置有效的过滤开关，切实获取与安全审计直接相关的数据。同样的原因，审计数据的分析过程应在用户层进行，但需要采取妥善的办法，对审计数据进行保护。

3.5 审计数据的存储

审计数据在整个安全审计系统中占据着非常重要的地位，如果审计数据的安全性得不到保证，那么建立在这些审计数据之上的后续分析工作将是徒劳的，前期的工作也功亏一篑。在系统中，通过对审计数据实现多重保护来防止非法用户对审计数据的访问。Linux 文件系统本身有一套文件保护模式，它通过 9 个 bit 位来区分文件的属主、与文件属主同在一个组的用户和其他用户对文件的存取权限。然而，这一套保护模式对于超级用户(root)来说是毫无作用的，所以必须寻求其它的保护方法。

转储和隐藏是两种比较常用的方法。转储是指把生成的审计数据通过网络直接存放到另一台相对比较安全的机器上。隐藏必须通过 LKM 在内核级来实现，用户级的隐藏(通过将文件名的第一个字符设定为“.”)是毫无作用的。通过 LKM，最终可以达到隐藏文件名、文件内容甚至是文件使用的磁盘大小的效果。而在需要查看审计数据时，只需将原本为了隐藏文件信息而加载的 LKM 模块卸载即可。当然，对这个特殊的 LKM 要进行特殊的处理，就是加载该模块后，要把该模块的信息也隐藏起来，使得用户(包括超级用户)不能通过 lsmod 以及查看/proc/modules 文件获得任何关于该模块的信息。

3.6 审计数据的分析技术

审计数据的分析,目标是从审计数据中获取利于系统管理的信息 (主要是用户行为特征),并以此为依据对系统的问题及时做出反应。目前对于系统安全审计机制所产生大量的审计信息还缺乏有效的分析技术。对于审计信息往往是在通过其他路径发现用户的异常行为或出现问题之后才来分析这些审计数据,使得审计数据只是作为一种事后证据。这实际上浪费了这些对于系统安全具有重要意义的宝贵资源。

数据挖掘是一种新兴的、并且在很短时间内得到广泛应用的先进的智能化数据分析工具。数据挖掘旨在从大量的数据中提取隐藏的预测性信息,能发掘数据间潜在的模式,找出某些常常被忽略的信息, 以便于理解和观察的方式反映给用户,作为决策的依据。基于审计数据的数据挖掘技术应该说是发现用户访问行为的较为理想的审计数据分析方式,数据挖掘对审计数据的处理能力和智能化的处理方式,在审计数据的处理中都是最为理想的。

4 结论

随着内核级入侵手段的流行,内核级的安全技术更多地受到人们的关注, 成为信息安全技术研究的非常重要的方面,也将成为安全技术的主流。文章在分析了现行的安全审计系统的基础之上, 提出了一个利用 LKM 技术和基于日志文件的数据技术的安全审计模型。该模型在一定程度上实现了审计数据的内核级获取和保护的功能,防止审计数据的非法访问。

(收稿日期:2002 年 1 月)

参考文献

1.刘建伟.安全审计追踪技术综述[J].信息安全与通讯保密,2001,7:37-39
2.Wadlow T A.潇湘工作室译.网络安全实施方法[M].北京:人民邮电出版社,2001
3.pragmatic/THC.Complete Linux Loadable Kernel Modules.http://www.infowar.co.uk/thc/articles.htm
4.Pragmatic/THC.Attacking FreeBSD with Kernel Modules (example modules).http://www.infowar.co.uk/ thc/articles.htm
5.Plasmoid/THC.Attacking Solaris with Loadable Kernel Modules.http://www.infowar.co.uk/thc/articles.htm

(上接 49 页)

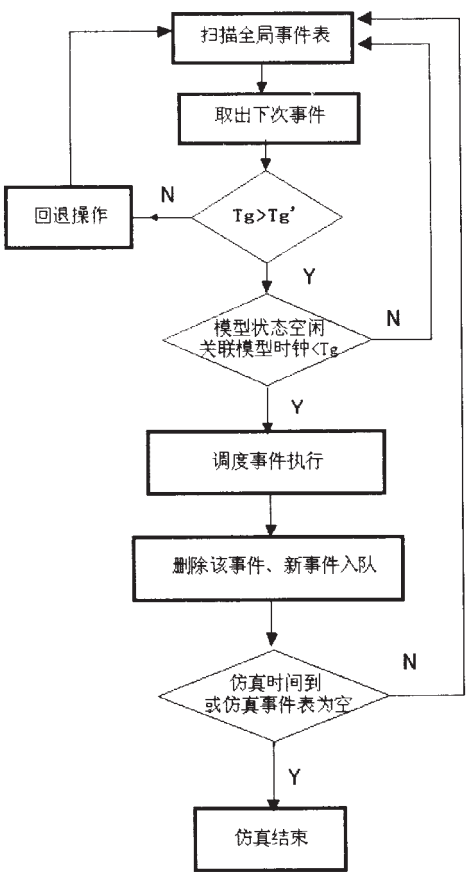

图 2 全局仿真调度流程图

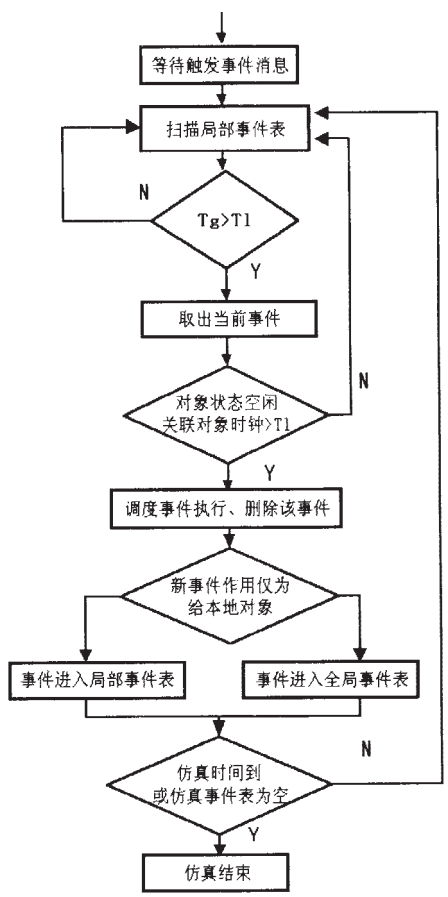

图 3 局部仿真调度流程图

1.Andrew S Tanenbaum.Distributed Operating Systems[M].电子工业出版社,1999.12
2.王维平,朱一凡等.离散事件系统建模与仿真[M].国防科技大学出版社,1997.8
3.林健,毛晶莹.并行离散事件仿真 PDES 策略比较研究[J].系统工程理论与实践,1998,9
4.张耀鸿,沙基昌等.分布离散事件仿真的集中同步算法[J].计算机仿真,2001,1
5.邢清华,刘付显.离散事件系统分布式仿真的集中并行控制[J].计算机仿真,2000,3
6.屠海滢,罗剑辉.离散事件仿真中的事件组合和合并事件策略[J].系统仿真学报,2000,5