第5卷第4期　　空军工程大学学报(自然科学版)　　Vol.5 No.4
2004年8月　　JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY(NATURAL SCIENCE EDITION)　　Aug.2004

Linux系统可加载内核模块安全应用研究

姚战宏[1]，赵海燕[2]，郑连清[1]
(1.空军工程大学 电讯工程学院，陕西 西安 710077;2.西安通信学院，陕西 西安 710063)

摘　要:介绍了Linux系统可加载内核模块机制(LKM)的用途、特点以及编写方法。提出了利用LKM提高系统安全性能以及防范攻击者利用LKM对系统进行入侵的措施。

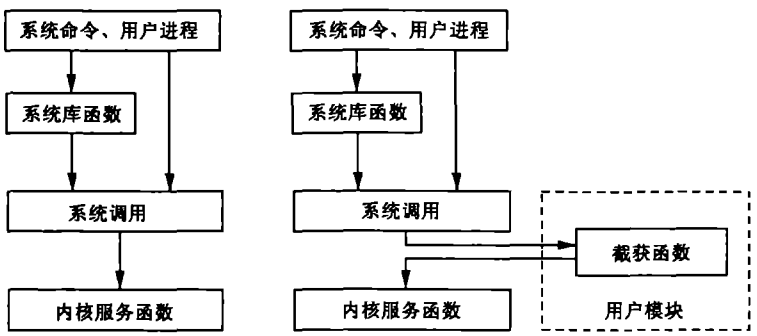
关键词:Linux;可加载内核模块;系统安全
中图分类号:TP393.08　　**文献标识码**:A　　**文章编号**:1009-3516(2004)04-0057-03

可加载内核模块(Loadable Kernel Module,简称LKM)是Linux系统提供给用户扩展其内核功能的一种机制。LKM是一项动态扩充内核功能技术,它使得Linux操作系统内核在运行状态就能对其功能进行扩充。编写完一个LKM程序,用编译器将其编译为目标文件,然后就可以根据需要动态加载,在不需要其所提供的功能时卸载它,LKM程序编写和编译的过程中无须对内核进行重新编译。由于LKM具有深入系统内部的特性,因此可以利用LKM有效地加强系统的安全防护能力。

1　LKM在安全方面的应用

系统调用是操作系统提供给用户应用程序的内核级基本操作,所有的Linux程序和命令都依赖于系统调用。因此可以通过截获系统调用来提高系统安全性能,原理如图1所示。

Linux中有一个重要的数据结构sys_call_table(定义在arch/i386/kernel/entry.S中),它记录了所有系统调用服务函数的入口地址。sys_call_table是内核级的内存区域,而用户的LKM能够访问到内核级的地址空间,因此,可以在LKM中对某个系统调用的sys_call_table表项进行替换,将服务函数的入口地址改为LKM中函数的地址,达到截获系统调用的目的。另外,为了不影响系统的正常运行,可以将原服务函数的入口地址保存下来,执行完LKM中的函数后再执行原服务函数。这样,就在原系统的基础上通过加载用户自定义内核模块(该模块包含具有改善安全性能的截获函数),提高系统的安全性能。



(a)未加载用户模块　　(b)加载用户模块

图1　截获系统调用原理示意图

1.1　控制入侵者对文件的访问

入侵者经常做的事情就是修改系统文件,留下后门。Linux内核为我们提供了一种机制:securebits。当securebits值为1时,就可以设置某些文件只能被添加(append-only),某些文件不可更改(immutable)。实现起来非常简单,在init_module中将securebits值设置成1,在cleanup_module中将其恢复为原来的值。这种方法虽然很简单,但是非常实用。

收稿日期:2004-02-25
基金项目:国家自然科学基金资助项目(60073051)
作者简介:姚战宏(1979-),男,陕西渭南人,博士生,主要从事网络对抗技术研究.

对于某些重要的系统文件,为了避免被攻击者轻易发现,也可以将其隐蔽起来,使得 ls 命令无法发现它们。ls 命令使用的系统调用内核服务函数是 sys_getdents,因此可截获该系统调用。截获函数首先调用原服务函数,在返回的目录项中查找与特定文件名称相同的目录项,找到后将该项从目录结构中删除,最后返回不包含特定名称目录项的目录结构。这样使用文件列表命令 ls 便无法看到该文件。

更高明的攻击者还会通过读取硬盘上的原始资料来搜索有用的文件信息,为了防止这种行为,必须禁止对原始盘的访问,为此应截获 sys_read 和 sys_write 系统调用服务函数。在这两个系统调用中,当传递参数信息为"/dev/hd *"时,就将其拒绝,这样调用者便无法直接访问到硬盘上的原始资料,同时也保护了硬盘资料不受恶意破坏。

1.2 实现内核级的安全审计

安全审计是计算机系统安全管理的一个重要的组成部分。它是记录用户的访问过程和各种行为形成审计资料的过程。对审计资料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[2]。

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。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。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,如此一来常规的审计技术对这些入侵活动根本就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,可以利用 LKM 完成安全审计功能。LKM 采取同应用服务程序无关的方式记录审计信息,在内核级完成安全审计功能,并保护或隐藏保存审计信息的文件。LKM 可以通过截获 sys_write、sys_read、sys_create 和 sys_open 等系统调用来监视用户的行为,也可以通过截获 recvfrom 系统调用的服务函数,对来自网络应用程序的资料包进行安全审计,并隐藏日志文件,使攻击者难以发现。这种借助于 LKM 完成的内核级的安全审计,使操作系统达到了一个较高的安全级别。

1.3 模块自身的隐藏

攻击者以超级用户权限登录到系统后,使用 lsmod 命令就可以看出目前系统已加载的所有模块的名称,当然他也可以卸载某个模块。因此为了避免被发现,管理员必须想办法隐藏自己安装的模块。

lsmod 命令是通过/proc/modules 来列出当前的 LKM 的。一个 LKM 在内核中由数据结构 struct module 表示。如果该结构中的 name 域和 reference 域为零,那么在/proc/modules 中将不会找到它[3]。这样就为实现模块的隐藏找到了一条途径。

一个模块是通过一个 init_module 系统调用来开始初始化函数的。init_module 获得一个参数:struct mod_routines * routines。这个结构包含着加载这个模块的十分重要的信息,有可能通过操纵这些信息来使得模块没有名字和引用记数。在此之后,系统就不会在/proc/modules 里面显示 LKM 了。

2 防范来自 LKM 的攻击

上述利用 LKM 提高系统安全性能的方法也可能被恶意攻击者利用,以达到其入侵系统的目的。攻击者可以利用 LKM 留下后门,放置木马程序,甚至是感染病毒。为了防止系统受到 LKM 的入侵,应做好以下几点:

1)加强帐号的保密管理,尤其是根用户。因为只有具备超级用户权限的根用户或经过根用户授权的用户才能加载和卸载内核模块,普通用户无权操作内核模块。高明的攻击者还可以先利用普通用户身份登录到系统,然后通过其它手段提升用户的权限[4]。例如,利用系统中某些命令的执行漏洞、利用系统管理员脚本程序中的错误,都可以使普通身份的用户获得超级用户权限,这样便能加载内核模块。因此,对普通用户帐号也必须严加管理,另外还要及时检查系统漏洞,升级系统内核。

2)不要安装任何没有源代码的 LKMs。目前 Linux 系统下软件都会附带其源代码,包括以 LKM 形式出现的设备驱动程序。有的软件也会提供其某一内核版本下的二进制代码,用户只需直接加载就可以了。对

于这种LKM,千万不能盲目加载,因为这些内核模块很可能包含攻击者的恶意代码。同理也不能随意加载从别处复制来的二进制形式的LKM。正确的加载方式是先检查LKM源代码,确保其不包含有恶意代码,再在本地编译后加载。

3)如果系统内核已经被攻击者入侵,那么管理员很难发现入侵模块在系统中的踪迹,因为攻击者会隐藏入侵模块的相关信息。文件完整性检查可以发现安装新模块或修改现有模块的时间。对/lib/modules目录树限制许可以及应用"chattr +i"令能够延缓使用脚本的黑客新手的攻击,但这很容易被获得root权限的攻击者识破和处理。对这类复杂攻击,现实可行的防御方法是使用类似于LIDS[4]的内核补丁,并进行合适配置,使得即便是root也不能在/lib/modules下安装文件或装载内核模块。另外,如果确信系统内核已经被入侵,一个最保险的办法就是重新编译内核。

参考文献:

[1] Alessandro Rubini, Jonathan Corbet. Linux Device Drivers(2nd Edition)[M]. USA:OReilly Press, 2000.

[2] 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.

[3] Progmatic. The Definitive Guide for Hackers, Virus Coders and System Admin[EB/OL]. http://www.thehackerschoice.com/paper/LKM_HACKING.html,2001-06-01.

[4] 孙乐昌. 计算机网络攻防概述[M]. 北京:解放军出版社,2003.

(编辑:门向生)

Research on the Mechanism and Security Application of Loadable Kernel Module of Linux

YAO Zhan-hong[1], ZHAO Hai-yan[2], ZHENG Lian-qing[1]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'na, Shaanxi 710077, China; 2. Xi'an Communication Institute, Xi'an, Shaanxi 710063, China)

Abstract: Based on the analysis of functions, characteristics and programming methods of Loadable Kernel Module of Linux system, this paper presents some ways to enhance system security by utilizing LKM's characteristics and to keep a lookout for the hachers taking advantage of LKM to intrude into the system.

Key words: Linux; Loadable Kernel Module; system security

(上接第52页)

LUI Yun-jiang[1], HUANG Guo-ce[1], ZHEN Shu-chun[2], LI Man[1]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China; 2. The Missile Institute, Air Force Engineering University, Sanyuan, Shaanxi 713800, China)

Abstract: Rain attenuation is the dominant cause of leading up to the signal degradation in satellite links operation at Ka - band. Presently, most of rain compensation algorithms come from the aspect of the application of power and bandwidth and are based on the use of a fixed, large fade margin in combating the occasional deep fades. However, such use of a fixed margin, especially for a rainy region, results in an inefficient use of channel capacity. Therefore, based on the effective utilization of the channel capacity, the paper discusses the performance of satellite channel capacity in the Ka - band in the presence of rain attenuation, presents some useful results on the basis of analysis.

Key words: rain attenuation; channel capacity; fade margin; BER