云环境下的 Linux 进程监控的设计与实现

陶海鹏　1，王　勇　1,2，俸　皓　1,2

（1 桂林电子科技大学 计算机与信息安全学院，广西 桂林 541004；

2 桂林电子科技大学 广西云计算与复杂系统高校重点实验室，广西 桂林 541004）

摘　要：随着云计算的发展，云虚拟主机不仅面临着传统主机的安全问题，也面临着云安全问题.针对漏洞入侵、虚拟主机逃逸等问题，云平台缺乏主机监控方法.Linux 系统内核的关键函数位置下插入探测点，在内核层收集所需要的系统进程信息，提出了基于内核 Kprobe 机制的进程信息监控方案的设计思路及实现方法.以上方案有助于保护云虚拟主机的系统安全和数据安全，完善云平台的监控系统.通过对系统安装应用的前后的系统性能测试，证明设计的进程监控方法占用系统资源较低，从而证实了所设计方案有良好的可行性.

关键词：　云安全；系统进程收集；云平台；Linux；监控

Design and Implementation of Linux System Resources Collected Under the Cloud

TAO Hai-peng　1,WANG Yong　1,2, FENG Hao　1,2

(1 School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China; 2 Guangxi Colleges and Universities Key Laboratory of Cloud Computing and Complex Systems, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract：With the development of cloud computing, cloud hosting is not only facing the security problem of traditional host, but also facing problem of cloud security. For vulnerability intrusion, virtual host escapes and other issues, cloud platform absence of host monitoring methods. Because of inserting the probe point in the key positions of the function of the Linux kernel and collecting the required information of system process in the kernel layer, the implementation method and the design process and of the monitoring system information which based on kernel Kprobe mechanism has been proposed. The scheme above can not only be helpful to keep security of the system and data of the cloud virtual host, but also Improve the monitoring system of the cloud platform. Through the system performance testing before and after the installation of application in the system, that the process monitoring method which designed can be proved to Occupy lower system resource, so that the design scheme of the system is proved to have better feasibility.

Key words：cloud security； system processes collecting； cloud platform； Linux； surveillance

作者简介：

陶海鹏　男，(1991-)，硕士研究生.研究方向为信息安全、云安全.

E-mail:lifox2012@163.com.

王　勇　男，(1964-)，博士，教授.研究方向为云计算、计算机网络技术及应用、信息安全等.

俸　皓　男，(1978-)，博士研究生.研究方向为计算机网络、无线传感器网络、软件定义网络及云计算等.