	《计算机学报》文章摘要　　全文下载
文章题目	基于一种相对Hamming距离的入侵检测方法——RHDID
作者	张 琨1) 许满武2) 张 宏1) 刘凤玉1)
作者单位	1)（南京理工大学计算机科学与技术系 南京 210094） 2)（南京大学计算机科学与技术系 南京 210093）
发表年份	2003
发表月份	1期 （页码：65—70）
文章摘要	首先分析了传统入侵检测方法的不足，即误用入侵检测方法难于检测新形式的入侵，异常入侵检测方法难于建立合理有效的正常行为特征和检测方法.然后，通过对特权进程的系统调用和参数序列的研究，提出了一种相对Hamming距离入侵检测方法（RHDID）.应用RHDID检测入侵不仅能有效降低漏报率和误报率，而且使实时入侵检测成为可能.最后，原型系统证实了该方法的可行性，获得了在实时环境中检测入侵的技术效果. 关键词 入侵检测;海明距离;系统调用;网络安全中图法分类号 TP309