通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

肖 喜,田新广,翟起滨,叶润国.基于shell命令和Markov链模型的用户伪装攻击检测[J].通信学报,2011,(3):98~105

基于shell命令和Markov链模型的用户伪装攻击检测

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
肖 喜	
田新广	
翟起滨	
叶润国	

摘要点击次数： 396

全文下载次数： 241

中文摘要：

提出一种新的基于shell命令的用户伪装攻击检测方法。该方法在训练阶段充分考虑了用户行为的多变性和伪装攻击的特点，采用平稳的齐次Markov链对合法用户的正常行为进行建模，根据shell命令的出现频率进行阶梯式数据归并来划分状态，同现有的Markov链方法相比大幅度减少了状态个数和转移概率矩阵的存储量，提高了泛化能力。针对检测实时性需求和shell命令操作的短时相关性，采用了基于频率优先的状态匹配方法，并通过对状态短序列的出现概率进行加窗平滑滤噪处理来计算判决值，能够有效减少系统计算开销，降低误报率。实验

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭

版权所有：通信学报
地址：北京东城区广渠门内大街80号通正国际大厦6层602室 电话：010-67110006-869/878/881 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司