现代图书情报技术 2006 (4): 60-62 ISSN: 1003-3513 CN: 11-2856/G2

网络资源与建设

在SSH协议下的入侵检测

丁晓峰[1];[2];李周贤[1];[1];刘炳华[1];[3];顾 巍;;吴楠宁;

北京文献服务处[1]

总参警卫局管理处[2]

收稿日期 2005-9-22 修回日期 2005-10-11 网络版发布日期 2006-4-29 接受日期

摘要 阐述SSH协议下入侵检测系统存在的问题，论述SSH协议下入侵检测的必要性和需要注意的两个问题，提出一种新的入侵检测方法。

Abstract Widespread using the SSH protocol can greatly reduces the risk of remote computer access by encrypting the transmission of data. At the same time, because of the encrypted data, intrusion detection system based clear data can't identify the encrypted attack information. This paper outlines the role of SSH and types of intrusion detection, then proposes techniques for an intrusion detection under SSH protocol.

关键词 SSH协议 入侵检测系统 特征检测 异常检测 IDXP协议

Key words SSH;IDS;Signature based detection;Anomaly based detection;IDXP

分类号 TP393

DOI:

通讯作者:
丁晓峰 ding-xiaofeng@sohu.com
作者个人主页: 丁晓峰 李周贤 刘炳华 顾 巍 吴楠宁