计算机应用 2008 28 (04): 843-845 ISSN: 1001-9081 CN: 51-1307/TP

网络与通信

一种分布式入侵检测系统的通信机制设计

黄文文[1];郭帆[1];文剑[1];余敏[2]

江西师范大学[1]

收稿日期 2007-10-30 修回日期 网络版发布日期 2008-4-28 接受日期

摘要 基于关联和代理的分布式入侵检测模型，提出了一种分布式入侵检测系统的通信机制设计方案。其中通信Agent间的消息交换格式参照IDMEF标准，给出其消息内容详细设计，并根据需求扩充了警报数据XML描述；汇聚点通信Agent中使用基于subscription通信模式减少了系统的通信开销，具体描述了subscription的逻辑结构实现；还在通信机制中采用SSL技术较好解决了数据传输的安全问题。

Abstract According to the distributed intrusion detection model based on correlation and Agent, a kind of communication mechanism was proposed. With reference to the Intrusion Detection Message Exchange Format (IDMEF), a detailed message system was described for communication Agent, and in accordance with demand expanded XML description. Using the subscription communications model in order to reduce the overhead of communication, subscription logic framework was described. Based on SSL, a security communication mechanism can meet the demand of the distributed intrusion detection system.

关键词 分布式入侵检测 代理 通信机制 入侵检测消息交换格式 XML

Key words distributed intrusion detection;Agent;communication mechanism;Intrusion Detection Message Exchange Format (IDMEF);XML

分类号

DOI:

通讯作者:
黄文文 chinawenzi@gmail.com;hwen83@163.com

作者个人主页: 黄文文 郭帆 文剑 余敏