

基于数据融合分析的网络监控系统

框架构建与关键技术研究

程 军

(新时空科技有限公司, 山东 济南 250001)

摘 要: 针对增强复杂网络环境下监控预警能力的需要, 研究构建了一种基于数据融合分析的网络监控系统框架, 探讨了 IP 分组缓存管理、通联特征提取、目标关联识别、关系结构分析等关键技术, 对网络流量实现整体监控、综合挖掘和融合利用, 为网络监控技术手段的完善拓展提供方案借鉴.

关键词: 网络监控; 融合利用; 特征提取; 关联识别; 关系分析

Struct Construction and Key Technology Research of Network Monitoring System Based on Data Fuzzing Analyze

CHENG Jun

(New horizon Technology Ltd, Jinan 250001, China)

Abstract: Aiming at enhancing the ability of monitoring and reflection under complex network conditions, a new network monitoring structer based on data ALL analyse is established, and key skills such as IP packet buffer management, communication character abstract, correlated identify, and relationship structer analyze are discussed. The structer can improve overall monitoring, full dig, and all use of network flows, and important reference are offered for improving and extending network monitoring skills.

Key words: network monitoring; fuzzy usage; character extract; correlation identifaction; relationship analyze

作者简介:

程 军 男, (1976-), 博士, 高级工程师.研究方向为网络安全威胁智能识别技术的研究

E-mail: newhorizon@126.com.