

网络、通信、安全

大规模网络安全态势评估系统

赵鹏宇, 刘丰, 张宏莉, 王爽

哈尔滨工业大学 国家计算机信息内容安全重点实验室, 哈尔滨 150001

收稿日期 2007-12-17 修回日期 2008-3-6 网络版发布日期 2008-11-18 接受日期

摘要 在大规模网络安全事件应急响应过程中, 一个网络安全态势评估系统可以起到很好的辅助决策作用。提出了一种计算网络安全危害指数的方法, 并在这种方法基础上设计实现了一个大规模网络安全态势评估系统。该系统通过对网络安全事件的模拟重放, 对网络安全状况进行评估, 给出网络整体的安全危害指数, 并提出针对安全事件的响应控制策略。系统运行结果表明, 这种安全态势评估的方法针对大规模网络安全行为是有效的。

关键词 [安全态势评估](#) [危害指数](#) [并行网络模拟](#) [安全事件](#)

分类号

Security situation evaluation system for large scale network

ZHAO Peng-yu, LIU Feng, ZHANG Hong-li, WANG Shuang

China National Computer Information Content Security Key Laboratory, Harbin Institute of Technology, Harbin 150001, China

Abstract

When processing large-scale network security events, a network security situation evaluation system can be useful and help user to deal with these security events. This paper proposes an approach that computes network security disaster index and designs a security situation evaluation system for large scale network. Using replaying network security events, this system can evaluate network security situation, compute disaster index of whole network and give a policy of processing these security events. The results of experiment illustrate that this approach is effective for evaluating large scale network security situation.

Key words [security situation evaluation](#) [disaster index](#) [parallel/distributed network simulation](#) [security events](#)

DOI: 10.3778/j.issn.1002-8331.2008.33.038

通讯作者 赵鹏宇 zhaopengyu@pact518.hit.edu.cn

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(582KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [复制索引](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ 本刊中 [包含“安全态势评估”的相关文章](#)

▶ 本文作者相关文章

· [赵鹏宇](#)

· [刘丰](#)

· [张宏莉](#)

· [王爽](#)