

发展趋势/热点技术

网络安全信息关联与分析技术的研究进展

彭雪娜; 闻英友; 赵 宏

东北大学计算机软件国家工程研究中心, 沈阳 110004

收稿日期 修回日期 网络版发布日期 2006-8-28 接受日期

摘要 介绍了网络安全信息关联分析技术的背景, 指出了该技术解决的问题。根据分析方法的不同, 将该技术的现有方法分为4类: 基于网络安全信息相似性的分析技术, 基于攻击场景识别的分析技术, 基于网络安全信息因果关系的分析技术, 基于网络安全信息统计因果关系的分析技术。对每类方法的基本思想、现有技术以及存在的问题进行了阐述和分析, 对未来的一些工作方向进行了展望。

关键词 [网络安全](#) [信息分析](#) [告警聚集](#) [告警关联](#)

分类号 [TP393.08](#)

DOI:

对应的英文版文章: [2006-17-001](#)

通讯作者:

作者个人主页: 彭雪娜; 闻英友; 赵 宏

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(122KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [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](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“网络安全”的 相关文章](#)
- ▶ 本文作者相关文章

- [彭雪娜](#)
- [闻英友](#)
- [赵 宏](#)