

信息安全

基于用户可信度的误用入侵检测系统的研究

郭庆北

济南大学

收稿日期 2005-11-21 修回日期 2006-1-16 网络版发布日期 接受日期

摘要 提出了基于用户可信度的误用IDS模型,该模型对IDS框架结构、签名匹配策略及协同机制都进行了改进。鉴于通用入侵检测框架CIDF(Common Intrusion Detection Framework)结构中缺少对入侵等级划分的机制,提出了基于用户可信度量化的等级划分方法,提高了系统的合理性。定义了误用IDS安全级别,通过预警原理实现低安全级别IDS对未知入侵的预防作用。另外,在用户可信度IDS中使用了局部性原理,进而改善了签名匹配策略并提高了签名的匹配效率和准确率。

关键词 [用户可信度,局部性原理,预警,自动响应](#)

分类号

DOI:

对应的英文版文章: [5116153](#)

通讯作者:

郭庆北 guoqb@126.com

作者个人主页: 郭庆北

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (817KB)
- ▶ [\[HTML全文\]](#) (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“用户可信度,局部性原理,预警,自动响应”的 相关文章](#)
- ▶ [本文作者相关文章](#)
- ▶ [郭庆北](#)