计算机应用 2014, 34(1) 108-112 DOI: 10.11772/j.issn.1001-9081.2014.01.0108 ISSN: 1001-9081 CN: 51-1307/TP

计算机安全

基于攻击图与报警相似性的混合报警关联模型

朱梦影,徐蕾

沈阳航空航天大学 计算机学院,沈阳 110136

摘要： 为了揭示入侵检测系统所生成的报警数据之间的关联关系和重构入侵攻击场景,提出了一种基于攻击图与报警数据相似性分析的混合报警关联模型。该模型结合攻击图和报警数据分析的优点,首先根据入侵攻击的先验知识定义初始攻击图，描述报警数据间的因果关联关系,再利用报警数据的相似性分析修正初始攻击图的部分缺陷,进而实现报警关联。实验结果表明,混合关联模型能够较好地恢复攻击场景，并能够完全修复攻击图中单个攻击步骤的缺失。

关键词： 报警关联 入侵场景 攻击图 报警相似性 关联模型

Hybrid model of alert correlation based on attack graph and alert similarity

ZHU Menging,XU Lei

School of Computer, Shenyang Aerospace University, Shenyang Liaoning 110136, China

Abstract: In order to reveal logic attack strategy information from alarms generated by intrusion detection system and reconstruct attack scenario, a hybrid model of alarm correlation was proposed, which was based on attack graph and alert similarity analysis. This model combined the advantages of attack graph and alert data analysis. First of all, it described the causal relationship between alarms, according to the initial attack graph defined by the prior knowledge of intrusion attack. Afterwards, it used the similarity analysis of the alert data to repair the defects of the initial attack graph. And then it implemented alert correlation. The experimental results show that the model can not only recover attack scenario but also be able to fully repair the attack graph in the absence of a single attack step.

Keywords: alert correlation intrusion scenario attack graph alert similarity correlation model

收稿日期 2013-07-01 修回日期 2013-09-05 网络版发布日期 2014-02-14

DOI: 10.11772/j.issn.1001-9081.2014.01.0108

基金项目:

通讯作者: 徐蕾

作者简介: 朱梦影(1989-),女,河南许昌人,硕士研究生,主要研究方向:网络与信息安全;徐蕾(1959-),女,上海人,教授,主要研究方向:网络与信息安全。
作者Email: xulei@sau.edu.cn

参考文献：

本刊中的类似文章

1. 谢丽霞 江典盛 张利 杨宏宇.漏洞威胁的关联评估方法[J]. 计算机应用, 2012,32(03): 679-682
2. 崔颖 章丽娟 吴灏.基于攻击图的渗透测试方案自动生成方法[J]. 计算机应用, 2010,30(8): 2146-2150
3. 杜志顺 吴国平 裘咏霄 黄文丽 陈茂源.复合板灰色自适应瑕疵检测[J]. 计算机应用, 2010,30(8): 2250-2253
4. 王纯子 黄光球.基于脆弱性关联模型的网络威胁分析[J]. 计算机应用, 2010,30(11): 3046-3050
5. 黄光球 李艳.基于粗糙图的网络风险评估模型[J]. 计算机应用, 2010,30(1): 190-195
6. 肖云 王选宏 彭进业 赵健.基于不确定性知识发现的入侵报警关联方法[J]. 计算机应用, 2009,29(3): 808-812

7．郭帆 涂风涛 余敏.基于报警序列的入侵场景自动构建[J]. 计算机应用, 2009,29(08): 2223-2226