基于EA-DS证据理论的安全事件关联分析

龙 春[1,2],申罕骥[1],李 俊[1]
(1 中国科学院 计算机网络信息中心,北京 100190;2 中国科学院大学,北京 100190)

摘 要:为了对多源安全事件进行关联分析,提出了基于EA-DS证据理论的安全事件关联分析方法.该方法结合所在网络环境将来自多个不同种类的安全传感器数据进行证据融合,计算网络服务威胁状态置信度,能够快速发现高威胁状态的服务并采取相应的措施进行响应.通过在实际网络环境中进行实验和对比,该方法有较好的高危攻击发现能力.

关键词:安全事件;报警日志;关联分析聚合;EA-DS证据理论
中图分类号:TP393 **文献标识码**:A **文章编号**:1000-7180(2015)11-0046-07

Security Events Fusion Based on EA-DS Evidence Theory

LONG Chun[1,2], SHEN Han-ji[1], LI Jun[1]
(1Computer Network Information Center, Chinese Academy of Science, Beijing 100190, China;
2 University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: In order to correlate and analyze multi-source security events, this paper has proposed a security event correlation analysis method which is based on Environment Awareness Dempster-Shafer evidence theory (EA-DS). The method combined various security sensor data in the network environment for evidence fusion, computed threat state confidence of network service, and detected high threat state of the service rapidly. Extensive experiments show that EA-DS has good ability to find high risk threat in the real network environment.

Key words: security events; alert log; correlation analysis fusion; EA-DS evidence theory

作者简介:
龙 春 男,(1979-),博士研究生,高级工程师.研究方向为网络安全.Email:shenhanji@cstnet.cn
申罕骥 男,(1987-),硕士.研究方向为网络安全.
李 俊 男,(1968-),博士,博士生导师.研究方向为互联网技术.

收稿日期:2015-01-22;**修回日期**:2015-03-17
基金项目:国家科技支撑计划课题(2012BAH01B03);科技部"九七三"课题(2012CB315803);科技部"八六三"课题(2013AA010601);中科院战略性先导专项(XDA06010306)