



攻击图算法在入侵防御系统中的应用

罗智勇, 孙广路, 刘嘉辉, 王卫兵

哈尔滨理工大学 计算机科学与技术学院, 黑龙江 哈尔滨 150080

Application of attack graphs algorithms in intrusion prevention system

LUO Zhi-yong, SUN Guang-lu, LIU Jia-hui, WANG Wei-bing

School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China

- 摘要
- 参考文献
- 相关文章

全文: PDF (KB) HTML (KB) 输出: BibTeX | EndNote (RIS) 背景资料

摘要 针对目前及时发现网络漏洞,增强网络安全十分困难等问题,提出了基于攻击图的入侵防御方法.该方法通过生成全局网络攻击图算法来建立网络初始攻击图,并调用攻击图优化算法来去除全局攻击图中不合理路径,达到简化攻击图目的.最后,通过计算攻击图各状态节点损失度算法来为管理人员提供优化网络安全策略的依据.实验证明,这种入侵防御方法合理有效,并具有简单易行等优点.

关键词: 网络安全 入侵防御 攻击图 漏洞 状态节点

Abstract: Now it was found that network loopholes in time and enhanced network security was very difficult. Aimed at these problems, the paper provided a method of intrusion prevention based on attack graphs. This method built network initial attack graphs by creating global network attack graphs algorithm. And we called attack graphs optimization algorithm to remove unreasonable paths in global attack graphs, so the attack graphs was simplified. Finally, by the algorithm of calculating attack graphs state node's loss degree, webmaster optimized the network security policy. Experiments proved that this intrusion prevention method was reasonable and effective, and had simple and easy to do etc.

Key words: network security intrusion prevent attack graphs loophole state node

收稿日期: 2011-09-26;

基金资助:国家自然科学基金资助项目(60903083);黑龙江省教育厅海外学人科研资助项目(1251HO18).

引用本文:

罗智勇,孙广路,刘嘉辉等. 攻击图算法在入侵防御系统中的应用[J]. 云南大学学报(自然科学版), 2012, (3): 271-275,284.

LUO Zhi-yong, SUN Guang-lu, LIU Jia-hui et al. Application of attack graphs algorithms in intrusion prevention system[J]. , 2012, (3): 271-275,284.

[1] SINGHAL A,OU X M.Security risk analysis of computer networks: Techniques and challenge// Proceedings of the 16th ACM Computer and Communications Security(CCS).Chicago,USA,2009.

[2] SAWILLA R,OU X M. Identifying critical attack as set s in dependency attack graphs//Proceedings of the 13th European Symposium on Research in Computer Security(ESORICS).Malaga,Spain,2008: 18-34.

[3] WANG L Y,TANIA I. An attack graph-based probabilistic security metric// Proceedings of the 22nd Annual IFIP WG11,3 Working Conference on Data and Applications Security(DBSec).London,UK,2008: 283-296.

[4] SHEYNER O, HAINES J, JHA S. Automated generation and analysis of attack graphs//Proc 2002 IEEE Symposium on Security and Privacy, Oakland, California, USA, 2002: 254-265.

[5] 李晓哲, 谭智勇, 戴一奇. 安全局域网主机入侵防御系统[J]. 清华大学学报: 自然科学版, 2010, 50(1): 54-57.

[6] XING Xu-jia, LIN Chuang, et al. A survey of computer vulnerability assessment[J]. Chinese Journal of Computers, 2004, 27(1): 1-11.

服务

- ▶ 把本文推荐给朋友
- ▶ 加入我的书架
- ▶ 加入引用管理器
- ▶ E-mail Alert
- ▶ RSS

作者相关文章

- ▶ 罗智勇
- ▶ 孙广路
- ▶ 刘嘉辉
- ▶ 王卫兵

- [7] 叶云,徐锡山,贾焰,等.基于攻击图的网络安全概率计算方法[J].计算机学报,2010,33(10):1 987-1 996.
- [8] 柴争义,刘芳,朱思峰.新型智能入侵防御模型[J].华中科技大学学报:自然科学版,2010,38(1):22-24.
- [9] 苟大鹏,杨武,杨永田,等.基于弱点关联和安全需求的网络安全评估方法[J].高技术通讯,2009,19(2):141-146.
- [10] 苟大鹏,杨武,杨永田.基于攻击图的网络脆弱性分析方法[J].南京理工大学学报:自然科学版,2008,32(4):416-419.

没有找到本文相关文献

版权所有 © 《云南大学学报(自然科学版)》编辑部

编辑出版: 云南大学学报编辑部 (昆明市翠湖北路2号, 650091)

电话: 0871-5033829(传真) 5031498 5031662 E-mail: yndxxb@ynu.edu.cn yndxxb@163.com