基于攻击图模型的网络可能入侵估计研究

王继钢
(呼伦贝尔学院 计算机科学与技术学院,内蒙古 海拉尔 021008)

摘 要:提出了一种基于攻击图模型的网络可能入侵估计方法.该方法先将以往每次成功的网络入侵行为都当作一次网络状态的变迁,并以此为依据定义网络攻击图、网络入侵路径、网络攻击行动,并预测攻击者下一次入侵目标的可能性和选择入侵路径的可能性,在此基础上融合已知和潜在的网络入侵威胁因素构建网络入侵的原子攻击库,计算系统网络环境下入侵者所面临的攻击压力与收益期望,对网络入侵者在决策时的攻击意愿进行量化,以量化后的结果为基础建立网络可能入侵估计风险模型,利用该模型给出网络可能入侵估计量化的风险值,从而有效地完成对网络可能入侵的估计.实验仿真证明,基于攻击图模型的网络可能入侵估计方法具有良好的可行性和有效性,可大幅减少不可信报警数量.

关键词:网络攻击;攻击图;攻击模型
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1000-7180(2016)02-0116-04

Invade Estimation Research Based on Network Attack Graph Mode

WANG Ji-gang
(College of Computer Science and Technology, Hulunbuir University, Hailar 021008, China)

Abstract: This paper proposes a network based on attack graph model approach to estimate the possible intrusion. This method first before every successful network intrusion behavior as the change of network state at a time, and on this basis to define the network attack graph, the path of network intrusion, and network attacks, and to predict the likelihood of the attacker next invasion target and chose the path of the invasion of possibility, on the basis of the integration in the known and potential threat of network intrusion factors to build atomic attack library network intrusion, computing system under the network environment the invaders attack pressure and earnings expectations, facing the network invaders attack intend to quantify in decision-making, on the basis of the quantitative results after establishing network may be invaded to estimate risk model, by using the model given network intrusion estimates may be quantitative risk value, effectively completed the estimate of the network may be invaded. Experimental simulation show that based on network attack graph model approach to estimate the possible intrusion has good feasibility and effectiveness, and greatly reduce the amount of untrusted alarm.

Key words: network attack; attack graph; attack model

作者简介:

王继钢 男,(1982-),硕士,讲师.研究方向为计算机网络、计算机硬件,信息处理、嵌入式技术.
E-mail: wjg26712092@sina.com