计算机应用 2008, 28(9) 2255-2258 DOI: ISSN: 1001-9081 CN: 51-1307/TP

论文

基于D-S理论的入侵检测系统

赵晓峰

河北工程大学

摘要：

单一的检测方法很难对所有的入侵获得很好的检测结果。所以，怎样将多种安全方法结合起来，为网络提供更加有效的安全保护，已经成为当前安全领域的研究热点之一。提出了一种基于数据融合的入侵检测系统，并将证据理论引入到网络安全中的入侵检测领域。该系统能够有效地解决单一检测算法无法对所有入侵都有很好检测效果的缺陷，并且相对于单一检测方法系统具有更好的可扩展性和鲁棒性。

关键词： 入侵检测 证据理论 数据融合

D-S theory-based intrusion detection system

Abstract:

It is hard for single security measure to attain favourable detection result. Therefore, how to combine multiplicate security measures to provide the network system with more effective protection becomes one of the hot spots in current research. A data fusion based intrusion detection system was proposed in this paper. Multiplicate detection measures were "fused" in this system to solve the problem that single measures can not obtain good result for all intrusions, and the system has better scalabilities and robustness.

Keywords: intrusion detection evidence theory data fusion

收稿日期 2008-04-21 修回日期 2008-06-03 网络版发布日期

DOI:

基金项目:

通讯作者: 赵晓峰

作者简介:

参考文献：

本刊中的类似文章

1．蒋世忠; 杨进; 张英.基于免疫原理与粗糙集理论的入侵检测方法[J]. 计算机应用, 2006,26(5): 1077-1080

2．周炎涛; 郭如冰; 李肯立; 吴正国.基于前馈多层感知器的网络入侵检测的多数据包分析[J]. 计算机应用, 2006,26(4): 806-808

3．彭雅丽 章志明 余敏 .一种入侵检测系统的形式化建模及其检测方法的研究[J]. 计算机应用, 2006,26(7): 1643-1645

4．史志才.一种改善入侵检测系统性能的新方法[J]. 计算机应用, 2007,27(3): 619-620

5．符海东 袁细国 .基于模糊模式识别的免疫模型的设计[J]. 计算机应用, 2007,27(1): 89-91

6．王茜 傅思思 葛亮 .基于人工免疫的新型检测器生成模型[J]. 计算机应用, 2006,26(11): 2618-1621

7．林涛 胡华平 张怡 刘波 .基于度量模块的入侵检测模型的研究与实现[J]. 计算机应用, 2006,26(12): 2916-2918

8．张喆 白琳 .一种基于克隆网络聚类的入侵检测方法[J]. 计算机应用, 2007,27(1): 128-131

9．鲁红英;肖思和.基于改进的遗传神经网络数据挖掘方法研究[J]. 计算机应用, 2006,26(4): 878-879

10．符海东 李雪.免疫入侵检测中基于数据场的动态识别算法[J]. 计算机应用, 2007,27(9): 2160-2162
11．曾夏玲 余敏 彭雅丽 余文斌.基于免疫和模糊综合评判的入侵检测模型研究[J]. 计算机应用, 2007,27(9): 2163-2166
12．咎鑫 郑庆华 范宇倩 韩九强.攻击案例综合学习系统研究[J]. 计算机应用, 2007,27(9): 2177-2179
13． 王艳秋 兰巨龙 何斌 .一种基于FPGA的IPv6网络入侵检测系统[J]. 计算机应用, 2006,26(10): 2341-2343
14．包必显 曾庆凯.一种基于数据流依赖关系的可信恢复方法[J]. 计算机应用, 2008,28(10): 2467-2470
15．陆虎 李永忠.不确定聚类算法及其在入侵检测系统中应用[J]. 计算机应用, 2008,28(10): 2715-2717
16．胡蓓 李俊 郁维 陈昌芳 .对未知攻击进行检测的蜜罐系统的实现[J]. 计算机应用, 2006,26(10): 2336-2337
17．赵林惠 戴亚平 付东梅 董芳艳 .基于危险模型的三级模块式入侵检测系统[J]. 计算机应用, 2006,26(10): 2310-2314
18．张军 苏璞睿 冯登国 .基于系统调用的入侵检测系统设计与实现[J]. 计算机应用, 2006,26(9): 2137-2139
19．俞研 黄皓 .一种半聚类的异常入侵检测算法[J]. 计算机应用, 2006,26(7): 1640-1642
20．李战春;李之棠;黎耀.基于径向基函数的入侵检测系统[J]. 计算机应用, 2006,26(5): 1075-1076
21．杨帆 彭新光.分簇体制在MANET入侵检测中的应用[J]. 计算机应用, 2007,27(4): 832-834
22．付长龙 吕彦波 姚全珠 杜旭辉.基于样本密度的SVM及其在入侵检测中的应用[J]. 计算机应用, 2007,27(4): 838-840
23．赵晓峰 叶震.基于加权多随机决策树的入侵检测模型[J]. 计算机应用, 2007,27(5): 1041-1043
24．郭帆 余敏 叶继华.一种基于关联和代理的分布式入侵检测模型[J]. 计算机应用, 2007,27(5): 1050-1053
25．李恒杰.Online SVM在实时入侵检测中的应用研究[J]. 计算机应用, 2007,27(6): 1339-1342
26．柴晨阳 孙星明 吴志斌 智云生.基于神经网络集成的入侵检测研究[J]. 计算机应用, 2007,27(6): 1363-1364
27．谷保平 许孝元 郭红艳.基于粒子群优化的k均值算法在网络入侵检测中的应用[J]. 计算机应用, 2007,27(6): 1368-1370
28．曹晖 王青青 马义忠 罗平.基于动态贝叶斯博弈的攻击预测模型[J]. 计算机应用, 2007,27(6): 1545-1547
29．吴仲 刘衍珩 田大新 张元媛.基于Netfilter框架的分布式网络入侵检测系统[J]. 计算机应用, 2007,27(6): 1353-1355
30．成科扬.基于模糊滑窗隐马尔可夫模型的入侵检测研究[J]. 计算机应用, 2007,27(6): 1360-1362
31．倪霖 郑洪英 .基于聚类和支持向量机的入侵检测研究[J]. 计算机应用, 2007,27(10): 2440-2442
32．张秋余 孙磊 .基于PC-LINMAP耦合赋权及云理论的入侵检测系统[J]. 计算机应用, 2007,27(10): 2443-2445
33．倪霖 郑洪英.基于免疫粒子群算法的特征选择[J]. 计算机应用, 2007,(12): 2922-2924
34．高朝勤 陈元琰 李 梅.一种面向入侵检测的快速多模式匹配算法[J]. 计算机应用, 2008,28(1): 82-84
35．李恒杰.基于RS_Adaboost的入侵检测方法[J]. 计算机应用, 2009,29(1): 181-184
36．张巍 滕少华 傅秀芬.数据融合的协同网络入侵检测[J]. 计算机应用, 2009,29(1): 284-287,
37．唐少先 蔡文君.基于无监督聚类混合遗传算法的入侵检测方法[J]. 计算机应用, 2008,28(2): 409-411
38．张亚玲 康立锦.基于数据挖掘的Snort系统改进模型[J]. 计算机应用, 2009,29(2): 409-411
39．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
40．郭文忠 陈国龙 陈庆良.高维数据环境下网络异常检测的改进否定选择算法[J]. 计算机应用, 2009,29(3): 805-807
41．张家超.利用支持向量回归机设计IDS的检测算法[J]. 计算机应用, 2008,28(3): 609-611
42．聂晓文 卢显良 王征.基于数字垂钓的盲目入侵检测算法[J]. 计算机应用, 2008,28(5): 1130-1132
43．黄文文 郭帆 文剑 余敏.一种分布式入侵检测系统的通信机制设计[J]. 计算机应用, 2008,28(4): 843-845
44．王大伟 张凤斌 王胜文.一种采用混合检测器的入侵检测系统[J]. 计算机应用, 2008,28(5): 1136-1139
45．鱼静 王峰.基于免疫的入侵检测模型中空洞的分析及对策[J]. 计算机应用, 2008,28(6): 1407-1410
46．吕良福 张加万 孙济洲 何丕廉 孙立刚.网络安全可视化研究综述[J]. 计算机应用, 2008,28(8): 1924-1927
47．宋凌 李枚毅 李孝源.一种新的半监督入侵检测算法[J]. 计算机应用, 2008,28(7): 1781-1783
48．鲁小丫 谭颖 王景丽.基于危险信号协同检测的入侵检测的研究[J]. 计算机应用, 2008,28(7): 1784-1785
49．郭建华 杨海东 邓飞其.基于免疫网络的RFID入侵检测模型研究[J]. 计算机应用, 2008,28(10): 2481-2484

反馈人		邮箱地址	
反馈标题		验证码	9515