计算机应用 2009, 29(10) 2644-2646 DOI: ISSN: 1001-9081 CN: 51-1307/TP

网络与通信

假设检验模型网络异常监控算法的研究和实现

高强,丁岳伟,何璐

上海理工大学

摘要： 针对传统安全监控方式对网络异常判断的不足，提出一种基于假设检验的网络异常分析算法。该算法提出一个新的概念“网络性能值”来描述网络状态。计算在网络正常情况下该网络主机的“网络性能值”分布参数，采集在检查的时间段内一定数量网络性能值样本，通过假设检验方法判断在该时间段内网络是否异常。对该算法进行程序测试，可以得出该算法与传统的监控方法相比降低了网络负荷，并提高了时间段内网络安全判断的正确率。

关键词： 网络监控 假设检验 网络性能 网络安全 网络负载

Research and realization of network security monitoring algorithm based on hypothesis verification model

Abstract: To overcome the disadvantage of traditional network security monitor system, this paper introduced a new definition—network performance (NP) which can describe the status of network. Calculate the distributing parameter in the security network environment was calculated, and the amount of NP during the monitoring time was collected, then whether the network is secure was estimated by using hypothesis verification. At last, the result of experiment shows the new algorithm can reduce the network burthen, and increase the accuracy of network security estimation.

Keywords: network monitoring hypothesis verification network performance network security network load

收稿日期 2009-04-16 修回日期 2009-06-18 网络版发布日期 2009-10-28

DOI:

基金项目:

上海市研究生创新基金项目

通讯作者: 高强

作者简介:

作者Email: kyo-gao@163.com

参考文献：

本刊中的类似文章

1．穆海冰 刘云 张长伦 .移动自组网中可逆证书状态管理模型[J]. 计算机应用, 2006,26(12): 2919-2921

2．张杰 赵政 熊晓 .一种半全局化的P2P信誉度模型[J]. 计算机应用, 2007,27(10): 2403-2405

3．王新昌 杨艳 刘育楠.一种基于局域网络监控日志的安全审计系统[J]. 计算机应用, 2007,27(2): 292-294

4．方旭明 张丹丹 .无线通信网络呼叫接纳控制策略研究综述[J]. 计算机应用, 2006,26(8): 1762-1767

5．宋金龙; 董健全;邹亮亮.一种P2P网络安全的信誉度模型设计[J]. 计算机应用, 2006,26(4): 833-835

6．李树军 .基于协议转变的拒绝服务攻击技术的研究[J]. 计算机应用, 2006,26(10): 2323-2325

7．康巧燕 余侃民 孟相如 王建峰.一种基于负载和队列的模糊主动队列管理算法[J]. 计算机应用, 2008,28(11): 2781-2783

8．史志才.网络风险评估方法研究[J]. 计算机应用, 2008,28(10): 2471-2473

9．郭晔 朱淼良 .面向Agent的网络蠕虫防御系统研究[J]. 计算机应用, 2006,26(12): 2931-2934

10．柳岸 龙雅琴 古乐野 .基于包过滤技术的网络安全的研究[J]. 计算机应用, 2006,26(9): 2160-2161

11．孙飞显; 徐明洁; 杨进; 王铁方; 刘孙俊.基于Web的教务管理系统安全方案设计[J]. 计算机应用, 2006,26(5): 1198-1201

12．谭长庚 张芝华 王建新 陈松乔.MANET能量与其他网络性能平衡路由协议[J]. 计算机应用, 2007,27(5): 1073-1076

13．汤念 王雷 姚焯善 张大方 徐红云.一种基于分组填充Mix策略的匿名通信机制[J]. 计算机应用, 2007,27(7): 1606-1608

14．聂朝恩 高荣芳.一种Linux平台上基于包过滤的网络流量采集系统[J]. 计算机应用, 2007,27(8): 1858-1861

15．马新新 耿技.对等网络信任和信誉机制研究综述[J]. 计算机应用, 2007,27(8): 1935-1938

16．张晗 万明杰 王寒凝 .战术互联网同质层基于信任评估的安全分簇算法[J]. 计算机应用, 2007,27(10): 2464-2469

17．王晓东 吕绍和 孙言强 孟祥旭.无线传感器网络中的Sybil攻击[J]. 计算机应用, 2008,28(11): 2801-2803

18．杨新宇 杨东旭 侯光霞 张国栋.移动IPv6网络中的DoS攻击[J]. 计算机应用, 2008,28(1): 74-76

19．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

20．刘岱坪 董小华 张明威 陈佳.网络安全态势多粒度分析的云方法[J]. 计算机应用, 2009,29(2): 370-373

21．谢松 郭忠文 曲海鹏 吕广鹏.基于多密钥空间的无线传感器网络密钥管理方案[J]. 计算机应用, 2009,29(4): 932-934,

22．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

23．田丰 王交峰 王传云 潘琢金 孙小平.无线传感器网络随机密钥预分配改进方案[J]. 计算机应用, 2008,28(6): 1388-1391

24．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

25．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

26．黄光球 赵煜.基于生物记忆原理的入侵检测模型 [J]. 计算机应用, 2009,29(05): 1279-1284

27．王衡军 王亚弟 张琦.移动Ad Hoc网络信任管理综述 [J]. 计算机应用, 2009,29(05): 1308-1311

28．杨宏宇 邓强 谢丽霞.网络安全组件协同操作研究 [J]. 计算机应用, 2009,29(09): 2315-2318

29．刘磊 王慧强 梁颖.基于模糊层次分析的网络服务级安全态势评价方法 [J]. 计算机应用, 2009,29(09): 2327-2331

30．黄萍 谭良.半分布式P2P Botnet控制服务器的设计与实现[J]. 计算机应用, 2009,29(09): 2446-2449
