计算机工程与应用 2009 45 (28): 109-111 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

提高Snort规则匹配速度的新方法

王 杰，王同军，孙珂珂

郑州大学 电气工程学院，郑州 450001

收稿日期 2008-5-27 修回日期 2008-9-4 网络版发布日期 2009-9-29 接受日期

摘要 对于基于特征的开源入侵检测系统Snort来说，如何提高规则匹配速度以适应高速网络的发展是关键。对Snort的规则匹配算法以及现有的两种著名的匹配算法BMH与BMHS算法进行比较分析，提出一种简单实用、易于理解的规则匹配改进算法。该算法通过减少模式串的移动次数以及增加最大移动距离m+1的出现次数来减少规则匹配所需要的时间，进而提高了Snort 规则匹配速度。实验测试结果表明该算法能够有效地提高Snort的规则匹配速度。

关键词 入侵检测系统 Snort 规则匹配

分类号 TP393.08

Research of new method for increasing rule matching speed of Snort

WANG Jie，WANG Tong-jun，SUN Ke-ke

College of Electrical Engineering，Zhengzhou University，Zhengzhou 450001，China

Abstract

In order to accommodate to the development of high-speed network，this article analyzes the rule-matching algorithm of Snort，an open source-code NIDS，and puts forward a new improved algorithm on the basis of original rule matching algorithm of Snort.This new algorithm can increase the rule matching speed efficiently through reducing the times of moving pattern strings and increasing the times of the furthest moving distance m+1 appearing.Finally，experiments are carried out for evaluating the efficiency of this algorithm.The results show that the approach can greatly improve the rule matching speed of Snort.

Key words intrusion detection system Snort rule matching

DOI: 10.3778/j.issn.1002-8331.2009.28.032

通讯作者 王 杰 wangtongjun117@163.com

扩展功能

本文信息

Supporting info

PDF(571KB)

[HTML全文](0KB)

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“入侵检测系统”的相关文章

本文作者相关文章

· 王 杰
· 王同军
· 孙珂珂