

[本期目录](#) | [下期目录](#) | [过刊浏览](#) | [高级检索](#)

[\[打印本页\]](#) [\[关闭\]](#)

安全技术

防火墙过滤规则动态生成方案设计

赵跃华, 周万胜

(江苏大学计算机科学与通信工程学院, 江苏 镇江 212013)

摘要: 基于主机的包过滤防火墙只能提供单一层面的、静态的网络安全防护。为此, 设计一个可动态生成防火墙过滤规则的方案。利用专家知识检测网络层数据包的攻击行为和运行中应用程序的攻击行为, 通过专家系统推理, 实现防火墙过滤规则的动态生成。基于 Windows系统的实验结果证明, 该防火墙系统能检测出多种攻击行为, 并及时生成防火墙的过滤规则。

关键词: 防火墙 CLIPS推理机 过滤规则 规则动态生成 专家系统

Design of Dynamic Generation Scheme for Firewall Filtering Rule

ZHAO Yue-hua, ZHOU Wan-sheng

(Institute of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: In order to overcome the shortcomings that packets filtering firewall on host only provides single-level and static network security protection, a firewall filtering rules dynamical generation scheme is designed. Attacks behavior information from network layer packets and application processes are detected by using expert knowledge and corresponding filtering rules are generated by using expert system reasoning. Experimental results based on Windows system demonstrate that the scheme can detect various attacks, and generates corresponding rules in time.

Keywords: firewall CLIPS reasoner filtering rule rule dynamic generation expert system

收稿日期 2011-05-20 修回日期 网络版发布日期 2012-01-20

DOI: 10.3969/j.issn.1000-3428.2012.02.043

基金项目:

上海市信息安全综合管理技术研究重点实验室开放课题基金资助项目“基于Windows的智能化数据筛选防火墙”

通讯作者:

作者简介: 赵跃华(1958—), 男, 教授、博士, 主研方向: 网络与信息安全, 嵌入式系统; 周万胜, 硕士研究生

通讯作者E-mail: zhouwansheng@163.com

参考文献:

- [1] 赵一铂, 邹恒明. 基于个人防火墙的自适应优化策略[J]. 计算机工程. 2009, 35(10): 109-111 [浏览](#)
- [2] Rash M. Linux防火墙[M]. 陈 健, 译. 北京: 人民邮电出版社, 2009.
- [8] 朱雁辉, 朱雁冰. Windows防火墙与网络封包截获技术[M]. 北京: 电子工业出版社, 2002.
- [9] 国内最流行十大木马查杀[EB/OL]. (2006-06-25). <http://www>.

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(259KB\)](#)
- ▶ [\[HTML\] 下载](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [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](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

本文关键词相关文章

- ▶ [防火墙](#)
- ▶ [CLIPS推理机](#)
- ▶ [过滤规则](#)
- ▶ [规则动态生成](#)
- ▶ [专家系统](#)

本文作者相关文章

- ▶ [赵跃华](#)
- ▶ [周万胜](#)

PubMed

- ▶ [Article by Diao, T. H.](#)
- ▶ [Article by Zhou, M. Q.](#)

本刊中的类似文章

1. 王凤领, 陈荣耀, 张剑飞, 邢婷, 王知强. 基于GIS与ES的公路生态景观评价系统[J]. 计算机工程, 2012,38(01): 291-292,封三
2. 孟祥册, 李决龙, 张炎文. 基于专家系统的建筑自动化系统故障诊断[J]. 计算机工程, 2011,37(21): 273-275,278
3. 张瑞军, 黄彦. 基于专家系统的多角色烧结配矿决策支持系统[J]. 计算机工程, 2011,37(19): 233-235,238
4. 涂平晖;尹文生;徐帆;张恒喜.POADES知识库的构建[J]. 计算机工程, 2010,36(4): 28-29
5. 张林英;蒋艳荣. 基于GIS的干扰评价专家系统设计[J]. 计算机工程, 2010,36(4): 177-179
6. 梁建武, 龙晓梅, 刘军军. 基于LE-Trie的防火墙策略检测算法[J]. 计算机工程, 2010,36(22): 134-136
7. 彭智朝, 谢东, 陈代武. 基于协商处理的集群防火墙负载均衡算法[J]. 计算机工程, 2010,36(13): 134-136
8. 安峰, 谢强, 丁秋林. 基于Ontology的专家系统研究[J]. 计算机工程, 2010,36(13): 167-169,172
9. 陈兵;张峰;丁秋林. 基于ARM处理器的嵌入式防火墙设计与实现[J]. 计算机工程, 2009,35(6): 197-199
10. 张明;陈性元;杜学绘;钱雁斌. 基于防火墙钩子的IPSec VPN研究与实现[J]. 计算机工程, 2009,35(4): 154-156

文章评论

反馈人	<input type="text"/>	邮箱地址	<input type="text"/>
反馈标题	<input type="text"/>	验证码	<input type="text" value="2304"/>
<input type="text"/>			