

论文

## 基于虚拟机技术的入侵检测系统攻击仿真平台的研究和实现

王汝传<sup>①②</sup>, 黄良俊<sup>①</sup>, 胡涛<sup>①</sup>, 孙知信<sup>①</sup>

<sup>①</sup>南京邮电学院计算机科学与技术系, 南京, 210003; <sup>②</sup>信息安全国家重点实验室, 中国科学院研究生院, 北京, 100039

收稿日期 2003-5-26 修回日期 2003-9-29 网络版发布日期 2008-5-4 接受日期

摘要

攻击仿真平台是入侵检测系统(Intrusion Detectoin System, IDS)测试平台的核心组成部分。该文从攻击测试的角度, 提出了一种基于虚拟机技术的IDS攻击仿真平台。首先介绍攻击仿真的测试目标和内容, 并提出了攻击仿真系统和仿真平台的设计和实现的详细方案; 同时, 在此基础上, 对该平台的设计和实现的3个关键技术: 测试数据的选择、攻击技术的分类研究、攻击测试域及其划分等进行了进一步的分析, 最后给出并分析了实验测试结果。

关键词 [入侵检测系统](#) [仿真平台](#) [虚拟机](#) [攻击测试](#)

分类号 [TP31](#) [TN918](#)

## The Research and Implementation of Attack Simulation Platform for Testing Intrusion Detection System Based on Virtual Machine Technology

Wang Ru-chuan<sup>①②</sup>, Huang Liang-jun<sup>①</sup>, Hu Tao<sup>①</sup>, Sun Zhi-xin<sup>①</sup>

<sup>①</sup>Dept. of Computer Science and Tech. Nanjing Univ. of Posts and Telecommunications Nanjing 210003 China; <sup>②</sup>State Key Laboratory. of Information Security Graduate School of Chinese Academy of Sciences Beijing 100039 China

Abstract

Attack simulation plays a key role in testing Intrusion Detection System(IDS). Prom the viewpoint of attack testing, an attack simulation platform is put forward for testing IDS based on virtual machine technology. First of all, the testing aims and contents of attack simulation are proposed. Then, the design and implementation of the attack simulation platform are presented in detail. Under the platform, that the authors build, three key issues in realization of the platform :the choice of testing datum, the classification of attack technology, and the attack testing zones and their compartmentalization are discussed in detail. Finally, the test results are given.

Key words [Intrusion Detection System \(IDS\)](#) [Simulation platform](#) [Virtual machine](#) [Attack testing](#)

DOI :

通讯作者

作者个人主页 王汝传<sup>①②</sup>; 黄良俊<sup>①</sup>; 胡涛<sup>①</sup>; 孙知信<sup>①</sup>

扩展功能
本文信息
▶ <a href="#">Supporting info</a>
▶ <a href="#">PDF(1512KB)</a>
▶ <a href="#">[HTML全文](OKB)</a>
▶ <a href="#">参考文献[PDF]</a>
▶ <a href="#">参考文献</a>
服务与反馈
▶ <a href="#">把本文推荐给朋友</a>
▶ <a href="#">加入我的书架</a>
▶ <a href="#">加入引用管理器</a>
▶ <a href="#">复制索引</a>
▶ <a href="#">Email Alert</a>
▶ <a href="#">文章反馈</a>
▶ <a href="#">浏览反馈信息</a>
相关信息
▶ <a href="#">本刊中 包含“入侵检测系统”的相关文章</a>
▶ 本文作者相关文章
<ul style="list-style-type: none"> <li>• <a href="#">王汝传</a></li> <li>• <a href="#">黄良俊</a></li> <li>• <a href="#">胡涛</a></li> <li>• <a href="#">孙知信</a></li> </ul>