计算机工程与应用 2008 44 (7): 136-138 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

HMM模型在检测复杂网络攻击中的应用

陶龙明, 史志才, 彭 丹, 马 武

大连大学 辽宁省智能信息处理重点实验室，辽宁 大连 116622

收稿日期 2007-6-21 修回日期 2007-8-20 网络版发布日期 2008-2-25 接受日期

摘要 对于隐蔽性强、持续时间长且分步完成的复杂网络攻击，现有的入侵检测技术仍无法有效地进行识别。详细地分析了复杂网络攻击的特征，并在此基础上建立了复杂网络攻击的HMM检测模型。通过关联分析不同网络监视器的报警事件，产生用于HMM模型训练及检测的报警序列，这些报警序列本质上反映了攻击者的行为。实验结果表明，该模型能较好地检测复杂网络攻击。

关键词 入侵检测 HMM模型 网络攻击 报警序列

分类号

Application of HMM to detecting sophisticated network attacks

TAO Long-ming,SHI Zhi-cai,PENG Dan,MA Wu

Liaoning Key Lab of Intelligent Information Processing，Dalian University，Dalian，Liaoning 116622，China

Abstract

Sophisticated network attacks are well disguised，durative and multi-stage；it can not be detected effectively by current intrusion detection technology.The native properties of sophisticated network attacks have been analyzed thoroughly in this paper，and then a detection model of sophisticated network attacks based on HMM is built.According to properties of sophisticated network attacks，lots of alarm sequences used by HMM are produced from different monitors distributed in real network.Experiments show that this model is effective in detecting sophisticated network attacks.

Key words intrusion detection Hidden Markov Models（HMM） network attacks alarm sequences

DOI:

通讯作者 陶龙明 vilon888@163.com