网络安全态势评估技术

张波云　编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

作者简介

张波云，男，湖南警察学院科研管理处处长，教授，博士，三级警监，全国公安高等教育教学名师，湖南省优秀教师，湖南省公安系统优秀教师，湖南省普通高校学科带头人，研究方向：信息安全。主持国家自然科学基金项目1项，主持省级课题研究12项，发表论文50余篇，主编教材3部。

国家自然科学基金面上项目（编号：61471169）、湖南省科技计划重大专项（编号：2017SK1040）、网络侦查技术湖南省重点实验室开放研究项目和湖南警察学院学术专著出版项目资助出版

网络安全态势评估技术

张波云　编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

网络安全态势评估技术/张波云编著.—武汉：武汉大学出版社，2020.6

ISBN 978-7-307-21271-8

Ⅰ.网… Ⅱ.张… Ⅲ.计算机网络—网络安全—安全评价 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2019)第 238528 号

责任编辑：林 莉 沈继侠 责任校对：李孟潇 版式设计：马 佳

出版发行：**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮箱：cbs22@ whu.edu.cn 网址：www.wdp.whu.edu.cn)

印刷：北京虎彩文化传播有限公司

开本：720×1000 1/16 印张：8 字数：161 千字 插页：1

版次：2020 年 6 月第 1 版 2020 年 6 月第 1 次印刷

ISBN 978-7-307-21271-8 定价：29.00 元

前　言

日益严峻的网络安全形势给传统的网络安全技术带来了挑战。源于战场态势感知领域的威胁与态势评估技术的引入，为从总体上解决认知网络安全的动态变化的难题提供了新的思路。

网络安全态势感知包括觉察（Perception）、理解（Comprehension）和预测（Prediction）三个阶段，通过定性或定量的网络安全评价体系对底层各类安全事件进行归并、关联和融合处理，并将获取的态势感知结果以可视化图形提供给网络安全管理员。网络安全态势评估是态势感知的核心，是对网络安全状态的定性定量描述。本书结合当前国内外网络安全态势感知与评估领域的研究现状，总结学者在态势评估研究领域近年来的成果，描述了网络安全态势评估体系的基本模型，重点介绍了相关的量化评估算法。

全书首先介绍了基于隐马尔可夫模型（Hidden Markov Model，HMM）的态势评估技术。将系统的安全状态、入侵报警事件分别与 HMM 的状态和观察符号相对应，给出了一种基于 HMM 的网络风险评估模型。该模型通过关联分析入侵检测系统产生的报警序列，计算各个主机的风险指数，进而对整个网络系统的风险状态进行定量评价。网络风险指数的计算方法简单且速度快，实验结果表明，该模型能够有效对网络系统的安全状态进行定量评估。

然后用隐半马尔可夫模型（Hidden Semi-Markov Model，HSMM）来模拟网络系统的实际运行，以网络防御系统捕获的报警数据作为研究数据源，实现对网络安全态势的评估。因为实际收集到的观测数据可能在同一个状态上发生无规律的驻留，HSMM 修改了 HMM 模型关于系统在某个状态的驻留时间服从指数分布的假定，更适合于描述网络系统运行的实际情况。我们针对系统驻留时间的不同概率分布情况，分别选取了对数分布、负二项分布、几何分布和泊松分布进行了实验测试。其中系统状态驻留时间呈泊松分布时的安全态势评估结果反映了网络攻击的真实情况，黑客发起攻击前先进行探测，经过一段时间的休战，再进行攻击尝试，在黑客的持续攻击下，系统被攻破，实验结果与实际观测结果相吻合。同时，结合 HSMM 的前向-后向算法，给出了部分观测条件下的 HSMM 系统状态预测算法，将其应用于 Honeynet 网络安全态势评估中，得到了较好的评估效果。实验结果表明，由于 HSMM 可以对系统状态的驻留时间进行建模，非常适合于攻击情况复杂多变的网络

系统的安全评估。

从博弈论（Game Theory）的观点来看，信息安全实际上是信息保护者（防御方）与入侵者（攻击方）之间的博弈。本书从博弈论的视角研究信息安全问题，建立了信息安全攻防博弈模型，提出了一种基于随机博弈模型的网络安全量化评估算法。利用安全管理员对网络设备的重要性评定来确定博弈参数，进行纳什均衡（Nash Equilibrium）分析，求得攻防双方的纳什策略（Nash Policy），从而获知网络处于不同安全状态的概率分布，最后可求出网络安全态势量分评估结果。本书提出的攻防双方的博弈模型，为解决现实中的信息安全问题提供了一种新的思路。

本书的研究工作得到了国家自然科学基金面上项目（编号：61471169）、湖南省科技计划重大专项（编号：2017SK1040）、湖南省重点研发计划项目（2017NK2400）、湖南省社会科学基金项目（编号：12YBB090）、网络侦查技术湖南省重点实验室开放研究基金、网络犯罪侦查湖南省普通高等学校重点实验室开放研究基金，以及湖南警察学院学术专著出版基金的大力资助。课题组成员鄢喜爱博士、张明键博士、罗熹博士和唐德权博士生在项目研究和书稿撰写中付出了大量心血，在此一并致谢。

网络安全态势感知作为一种新兴的安全技术，能够从整体上刻画目标网络的安全状态及其变化趋势，能够为网络安全管理员提供合适的安全加固方案，被越来越多地应用到网络安全的各个领域，成为下一代网络安全技术的焦点，为信息保障起到非常重要的作用。由于网络安全的复杂性，在态势感知与评估方面仍然需要进行大量的研究，加上作者知识和研究水平有限，书中难免会有疏漏或不当之处，恳请专家、学者不吝赐教。

作　者

2019 年 3 月

目　　录

第 1 章　绪论…… 1
1.1　网络安全发展及存在的问题 …… 1
1.1.1　信息安全的发展过程 …… 3
1.1.2　网络安全技术的发展现状 …… 5
1.2　网络安全态势感知中的关键技术…… 13
1.2.1　信息融合技术…… 14
1.2.2　态势评估分析技术…… 15
1.2.3　信息可视化技术…… 16
1.2.4　事件过滤技术…… 17
1.3　网络安全态势感知研究现状…… 18
1.4　研究背景…… 24
1.5　研究内容和组织结构…… 25

第 2 章　网络安全态势感知基础知识 …… 28
2.1　网络安全态势感知相关概念…… 28
2.2　网络安全态势感知体系结构…… 31
2.2.1　JDL 模型 …… 31
2.2.2　网络安全态势感知层次结构…… 31
2.3　网络安全态势感知基本研究内容…… 33
2.3.1　网络安全态势理解…… 35
2.3.2　网络安全态势评估…… 37
2.3.3　网络安全态势预测…… 37
2.4　网络安全态势感知与入侵检测系统…… 38
2.5　网络安全态势感知的评价指标…… 39
2.5.1　安全态势的定量评价指标体系 …… 39
2.5.2　安全态势的定性评价指标体系 …… 40
2.6　本章小结…… 41

第 3 章　基于隐马尔可夫模型的网络安全态势评估 …… 42
3.1　隐马尔可夫模型 …… 43
3.1.1　马尔可夫模型 …… 43
3.1.2　隐马尔可夫模型 …… 44
3.1.3　Forward-Backword 算法 …… 45
3.2　基于 HMM 的安全态势评估模型 …… 48
3.3　实验测试与结果 …… 51
3.3.1　实验数据集描述 …… 51
3.3.2　HMM 参数的设置 …… 57
3.3.3　实验结果 …… 58
3.3.4　讨论 …… 63
3.4　本章小结 …… 64

第 4 章　基于隐半马尔可夫模型的网络安全态势评估 …… 65
4.1　HSMM 理论基础 …… 65
4.1.1　HSMM 定义 …… 65
4.1.2　通用的 Forward-Backward 算法 …… 67
4.1.3　改进的 Forward-Backward 算法 …… 68
4.1.4　改进的 Forward-Backward 算法复杂度分析 …… 70
4.1.5　改进的 Viterbi 算法 …… 70
4.1.6　改进的 Baum-Welch 算法 …… 71
4.1.7　HSMM 核心算法实现 …… 72
4.2　基于 HSMM 的网络安全态势评估算法 …… 75
4.2.1　系统模型框架 …… 75
4.2.2　HSMM 中状态驻留时间讨论 …… 76
4.2.3　基于 HSMM 模型的系统状态预测算法 …… 79
4.3　实验测试与讨论 …… 80
4.3.1　HoneyNet 数据集 …… 80
4.3.2　实验步骤与结果 …… 81
4.4　本章小结 …… 89

第 5 章　基于随机博弈模型的网络安全态势评估 …… 90
5.1　博弈论基础 …… 92
5.1.1　博弈模型要素和基本概念 …… 92
5.1.2　博弈的分类 …… 95

5.1.3　博弈论的经典案例——囚徒困境 …… 96
5.2　基于随机博弈模型的网络安全态势评估 …… 97
5.2.1　攻防博弈的一般模型 …… 97
5.2.2　网络安全态势中的随机博弈模型 …… 99
5.3　实验测试与讨论 …… 103
5.3.1　HoneyNet 数据集描述 …… 103
5.3.2　HoneyNet 数据集中的随机博弈安全态势元素 …… 104
5.3.3　实验结果与讨论 …… 105
5.4　本章小结 …… 109

第 6 章　结语 …… 110
6.1　工作小结 …… 110
6.2　研究展望 …… 111

参考文献 …… 113

第1章 绪 论

1.1 网络安全发展及存在的问题

Internet 改变了人们生活方式和工作方式，改变了全球的经济结构、社会结构，Internet 越来越成为人类物质社会的最重要组成部分，成为 20 世纪最杰出的研究成果。但是，在互联网高速发展的同时，网络安全问题也日益严重①②③。

据 CERT/CC（Computer Emergency Response Team/Coordination Center，CERT）报道④，自 1998 年以来，Internet 安全威胁事件逐年上升，近年来的增长态势变得尤为迅猛，从 1998 年到 2003 年，平均年增长幅度达 50%左右，1988 年 CERT 接收的安全事件仅 8 起，到了 2003 年竟达到了 137529 起。国家计算机网络应急技术处理协调中心（CNCERT/CC）发布的《2018 年中国互联网网络安全报告》中指出，2018 年 CNCERT/CC 共接收中国境内外报告的网络安全事件 106700 起，较 2017 年上升了 3.2%。2018 年 CNCERT/CC 网络安全事件接收数量按月统计情况如图 1.1 所示。

导致这些安全事件的主要因素是系统和网络安全的脆弱性（Vulnerability）层出不穷，从 1995 年到 2003 年 CERT 各年度接到的脆弱性报告数逐年增多，例如 1995 年仅接收 171 起，到了 2003 年接收量就达到了 3784 起。近年来我国国家信息安全漏洞共享平台收录的安全漏洞数量增加得也很快，2016 年以来收录的漏洞数量超过了 10000 个，到 2018 年已达 14000 多个，如图 1.2 所示。这些安全威胁事件给 Internet 带来了巨大的经济损失。由于攻击数量如此之多，因此无法仅从安全

---

① Chen L C, Carley K M. The Impact of Countermeasure Propagation, on the Prevalence of Computer Viruses [J]. IEEE Transactions on Systems Man and Cybernetics Part B- Cybernetics, 2004, 34 (2): 823-833 .

② 陈秀真, 郑庆华, 管晓宏, 林晨光 . 层次化网络安全威胁态势量化评估方法 [J]. 软件学报, 2006, 17 (4): 885-897.

③ Hariri S, Qu G Z, Dharmagadda T, et al. Impact Analysis of Faults and Attacks in Large Scale Networks [J]. IEEE Security & Privacy, 2003, 1 (5): 49-54.

④ CERT. http://www.cert.org. 2011-3-1.

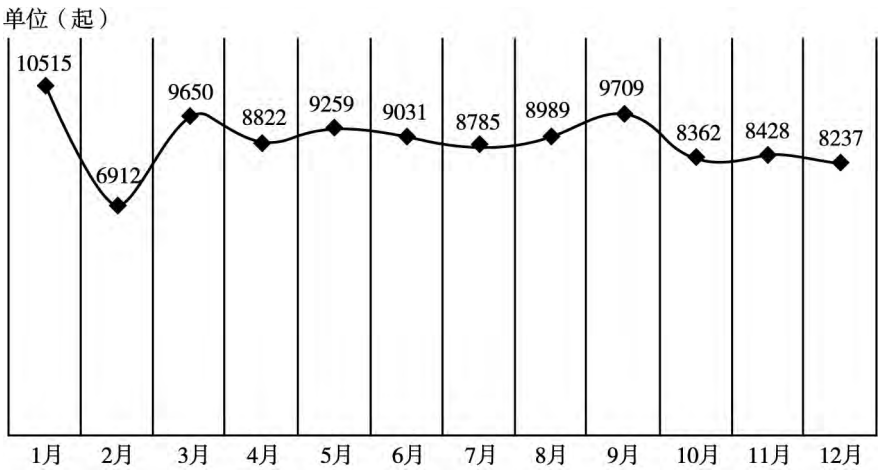

图 1.1　2018 年 CNCERT/CC 网络安全事件接收数量按月统计（来源：CNCERT/CC）

事件的数量中得到有关攻击范围和影响的更为有效的信息，从 2004 年开始，CERT/CC 更为重视专门的安全事件报告①。

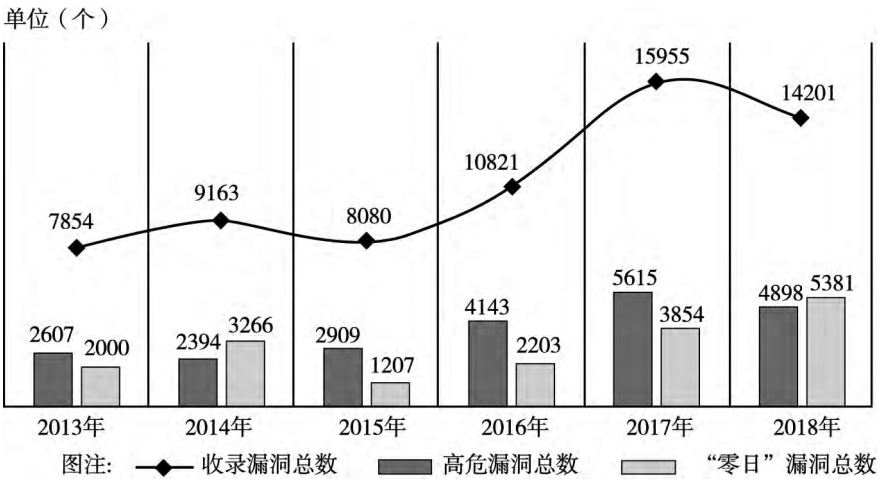

图 1.2　2013—2018 年 CNVD（国家信息安全漏洞共享平台）收录安全漏洞数量年度统计（来源：CNCERT/CC）

① Symantec Corporation. Symantec Internet Security Threat Report, Volume IX, 2006. http://eval. symantec. com /mktginfo/enterprise/white_papers/ent_white paper _ symantec_ internet_ security_ threat _ report_ix. pdf.

随着社会信息化的发展，网络信息安全问题也日益突出。诸多信息系统尤其是大型计算机网络系统的可靠性关系到经济、政治利益乃至国家安全，这些分布式网络具有空间分布广、实时性要求高、攻防对抗性强且多为异构系统等显著特点，它们对网络安全防护技术的需求十分迫切。

为了从全局角度认知网络安全的动态变化，提高网络系统的应急响应能力，缓解网络攻击所造成的危害，发现潜在恶意的入侵行为，提高系统的反击能力，本书所开展的网络安全态势研究逐渐成为了网络安全领域的研究热点之一，作为信息安全研究领域内一个前沿性课题，此方面的研究在国内刚刚起步。

1.1.1 信息安全的发展过程

对信息的安全、可靠和保障方面的考虑从自动化系统问世以来就有了。人们对信息安全的认识，经历了一个由浅入深、由片面到全面、由离散到整体的历史过程，这是在人们的实践中逐步完善的，并且与信息技术的发展相伴，受到不同历史阶段应用需求的驱动。通常认为，信息安全的发展经过了四个历史发展阶段：通信保密阶段（又称通信安全，COMSEC）、计算机安全（COMPUSEC）、信息安全（INFOSEC）、信息保障（IA）①，如图 1.3 所示。在每一个阶段，信息安全都有着不同的内涵。

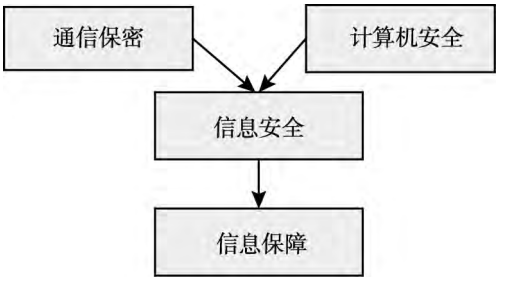

图 1.3 信息安全的发展阶段

（1）通信保密阶段。通信保密阶段开始于 20 世纪 40 年代，其时代标志是 1949 年香农发表的《保密系统的信息理论》，该理论首次将密码学的研究纳入了科学的轨道。在这个阶段所面临的主要安全威胁是搭线窃听和密码分析，其主要保护措施是数据加密。该阶段人们关心的只是通信安全，而且关心的对象主要是军方和政府机构。由于当时计算机速度和性能比较落后，使用范围有限，因此通信保密阶段重点是通过密码技术解决通信保密问题的，保证数据的机密性和完整性。

① 沈昌祥．信息安全工程导论［M］．北京：电子工业出版社，2003：23-28.

（2）计算机安全阶段。进入到 20 世纪 70 年代，通信保密阶段转变到计算机安全阶段。这一时代的标志是 1977 年美国国家标准局公布的《国家数据加密标准》（DES）和 1985 年美国国防部公布的《可信计算机系统评估准则》（TCSEC）。这些标准的提出意味着信息安全问题的研究和应用跨入了一个新的高度。此阶段主要在密码算法及其应用和信息系统安全模型及评价两个方面取得了很大的进展。

（3）信息安全阶段。20 世纪 90 年代以来，通信和计算机技术相互依存，Internet 发展成为一项通用技术平台，安全的需求不断地向社会各个阶段扩展，人们关注的对象已经逐步从计算机转向更具本质性的信息本身，信息安全的概念随之产生。人们需要保护信息在存储、处理或传输过程中的安全，于是除保密性、完整性和可用性之外，人们对安全有了新的需求：可控性和不可否认性。

（4）信息安全保障阶段。从信息安全的发展过程中可以看出，随着信息技术本身的发展和信息技术应用的发展，信息安全的内涵和外延都在不断地加深和扩大，包含的内容已从初期的数据加密演化到后来的数据恢复、信息纵深防御等。人们已经意识到安全不再局限于信息的保护，而是需要对整个信息和信息系统的保护和防御；同时安全已应用的结合更加紧密，追求适度安全已成为共识，安全不再单纯以功能或机制的强度作为评价指标，而是结合了应用环境和应用需求，强调安全是一种信心的度量，使信息系统的使用者确信其预期的安全目标已获满足。

1996 年美国国防部（DoD）在国防部令 S-3600.1 对信息保障作了如下定义："保护和防御信息及信息系统，确保其可用性、完整性、保密性、可认证性、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。"如图 1.4 所示。

图 1.4　P2DR 模型示意图

上述定义表明当前看待信息安全问题的视角已经不再局限于单个维度，而是将信息安全问题抽象为一个由信息系统、信息内容、信息系统的所有者和运营者、信息安全规则等多个因素构成的一个多维问题空间。这些变化均反映了人们对信息安全的意义内容、实现方法等一直在不断地思索和实践。

1.1.2 网络安全技术的发展现状

1.1.2.1 脆弱性检测技术

网络诸多安全问题的根源是网络系统本身存在脆弱性，脆弱性是网络存在安全损害的内因，如果能够设计出不存在任何脆弱性的系统，那么一切安全问题都能迎刃而解，消除系统的脆弱性作为系统安全的最原始的防线很早就被研究。在计算机技术出现之初，系统设计者们采用了各种技术上和管理上的措施，都是旨在设计安全的系统，但是实践证明，不可能设计出绝对安全的系统，任何人工的系统都不可避免地存在各种薄弱环节，但是如果能够检测到系统的脆弱性，及时进行修补，那么可以减少各种安全危害。脆弱性检测技术的目的就是在发现系统本身的安全漏洞和薄弱环节，帮助网络管理员在故障出现之前及时修复，减少潜在的威胁。脆弱性检测主要从技术上和管理上两个方面进行，技术层面涉及检测物理环境、网络环境、网络协议、软件漏洞等方面的脆弱性，管理层面包括检测技术管理和组织管理两方面脆弱性。

脆弱性检测技术所采用的方法主要有问卷调查和工具检测，其中工具检测是最为重要的一种手段，脆弱性检测技术的发展在很大程度上是对脆弱性检测工具的改进。脆弱性检测工具又称为脆弱性扫描器，脆弱性扫描器通过两种技术手段检测目标主机是否存在漏洞，其一是通过端口扫描技术，得到网络中每个主机开放的端口和提供的服务，进而将这些数据匹配脆弱性特征库，确定满足匹配条件的脆弱性；另一种是通过渗透测试技术，模拟黑客的入侵过程，根据入侵成功与否确定系统的脆弱性。端口扫描技术的优点是检测速度快，检测面广，但是只能检测脆弱性规则库中存在的脆弱性，对于未披露的脆弱性却无能为力；渗透测试技术的优点是能检测一些未知的脆弱性，但是检测速度慢，检测面较窄。

第一个脆弱性扫描器出现在 1992 年，Chris 等人编写了一个能远程检测 Unix 系统脆弱性的工具 ISS（Internet Security System）①，该工具能检测 Unix 系统几十种常见的脆弱性。1993 年，Wietse 和 Dan 开发了一个类似的检测工具 SATAN

① ISS. Internet Security System [EB/OL]. http://www.iss.net. 2011.

(Security Administrator Tool for Analyzing Networks)①，该工具本质上与ISS相同，但是它能识别网络相关的脆弱性，但是同ISS一样，它只对脆弱性做上标记而不提出解决的方法，对每一个检测到的脆弱性，SATAN提供一个文档介绍该脆弱性，并给出该脆弱性的潜在影响，同时对该脆弱性进行分类。随后，脆弱性扫描技术得到了长足发展，出现了一系列的脆弱性扫描器，到目前为止市面上大概有几十种脆弱性扫描器，它们的基本原理是相同的，都是通过扫描获得目标主机开放的端口和提供的服务，并将这些数据与漏洞规则库进行匹配，从而判断脆性是否存在。

目前常用的脆弱性扫描器有Nmap、Nessus和X-scan，它们都能检测操作系统的脆弱性和网络结构，Nmap是GNU（General Public License）旗下发布的②，可以免费下载和使用，能够对大规模的网络进行扫描，可以得到网络中开放的主机及其提供的网络服务，支持TCP、UDP和ICMP扫描技术。Nessus是Renaud Derasion开发的开源风险评估工具③，能够支持各种主流的操作系统，功能十分强大，能完成超过1200项安全检查，拥有友好的界面，并支持多种格式的安全报告输出。X-Scan是国内非常有名的一款免费的通用的脆弱性扫描器④，支持多种插件，采用多线程的方式对指定的IP地址段进行漏洞检测，并提供图形的操作界面。能够探测远程主机的操作系统版本及其提供的服务、SNMP信息、CGI漏洞、RPC漏洞、IIS漏洞、SSL漏洞、注册表信息等。

渗透测试技术是脆弱性检测的另一种技术，它通过模拟黑客的攻击行为，来检测系统的脆弱性，从攻击者的角度检测系统是否安全有效⑤。渗透测试包括侦查、入侵、攻击和安全分析四个阶段，渗透测试对网络中节点设备，包括主机、路由器、交换机等的网络协议、操作系统、数据库系统和应用软件系统及网络应用服务分析研究的基础上，通过发现、利用软件系统在机理、设计和配置上存在的缺陷与漏洞，在不影响网络正常运行的前提下，实现对目标网络的植入控制，进而检测目标网络的脆弱性。

脆弱性检测技术的发展对提高系统的安全性起了非常大的作用，利用脆弱性检测的结果，网络管理员可以有针对性地对网络的薄弱环节进行修复和加固，抑制安全事件的发生，从而预防了网络的潜在安全威胁，提高了网络的安全性。

但是脆弱性检测技术本身存在很多不足，首先，脆弱性检测技术只能检测一定

① SATAN. Security Administrator Tool for Analyzing Networks [EB/OL]. http://www.procupine.org/satan. 2011.

② Nmap [EB/OL]. http://nmap.org. 2011.

③ Nessus [EB/OL]. http://www.nessus.org/nessus/. 2011.

④ X-Scan [EB/OL]. http://www.xfocus.net/tools/200507/1057.html. 2011.

⑤ 周晓俊. 网络渗透测试系统研究 [A] //第十六届全国抗恶劣环境计算机学术年会论文集 [C]. 2006：283-288.

的脆弱性，尤其是脆弱性扫描器，只能检测大部分已经公布的脆弱性，不能识别未知脆弱性；其次，渗透测试虽能识别未知的脆弱性，但是应用范围窄，实现起来复杂，只能对一些特定的脆弱性做渗透测试；最后，各种脆弱性检测工具本身的局限性很大，它们有各自的适用范围和优缺点，很难全面地对系统进行检测。因此，脆弱性检测技术对提高网络的安全性的作用有限。

1.1.2.2 恶意代码检测技术

恶意代码指对网络系统有恶意目的的程序，它危害系统运行，并能自行复制和传播。恶意代码从类型上分为病毒、蠕虫、特洛伊木马、后门、逻辑炸弹、间谍软件、僵尸网络客户端等①。恶意代码一般利用系统的软硬件漏洞和欺骗用户的方式进行传播和破坏，如果系统中存在脆弱性而不存在利用该脆弱性的恶意代码，那么系统只是存在潜在的安全风险，并未出现安全损害，恶意代码是对系统造成安全损害的外因。恶意代码检测通过各种检测技术，识别出目标系统存在的恶意代码的特征和位置，包括基于特征码的静态检测技术、启发式扫描技术和基于虚拟机的行为检测技术。

基于特征码的静态分析技术是最基本、最常用的技术，目前主流的防毒软件的查毒引擎大部分采用这种技术，它首先对已存在的恶意代码样本进行分析，提取恶意代码的特征码，并写入相应的特征码库，然后对目标系统的文件进行扫描，若发现目标文件中有与特征码库相符的特征，则认为该文件含有恶意代码②。基于特征码的检测技术具有实现简单、误报率低、查毒效率高的优点，但是检测结果依赖恶意代码的特征库，对已经存在的恶意代码能很好地检测，对未知、加壳变形和特征码难以描述的恶意代码不能很好地检测，造成该技术存在大量的漏报现象。针对这种情况，目前的主流杀毒软件都提供实时的更新技术，及时更新病毒的特征库，并且采用广义特征码技术，能应对一些简单加壳和变形的恶意代码，但是在较为复杂的加壳加密的恶意代码面前，其显得力不从心。

启发式扫描技术是对静态特征码扫描技术的一种改进，对恶意代码的特性进行分析，分析恶意代码指令出现的顺序和特定的指令组合，获得统计上的启发知识，在对文件扫描时，一旦发现目标文件中存在可疑的指令或指令组合，则认为目标文件含有恶意代码③。该技术能够检测出未知的和变形后的恶意代码，但是在实现上

① 文伟平．恶意代码机理与防范技术研究［D］．中国科学院软件研究所博士学位论文，2004：17.

② Cohen F. A Short Course on Compter Viruses［M］. New York：John Wiley & Sons，1994：18-26.

③ Symantec. Plymorphic Virus Detection Module［M］. United States Patent，2004：44.

非常复杂，尤其是恶意代码的启发知识很难精确获取，因此误报率较高。

基于虚拟机的行为检测技术是在系统中虚拟 CPU 环境，在虚拟的环境中将恶意代码激活，根据其行为特征判断是否是恶意代码①。该技术对未知的、加壳和变形后的恶意代码能有效地检测，并且不需要构建庞大的病毒特征库，能在一定程度上保证原系统的安全，因此，该技术是目前杀毒软件升级的一个趋势。

但是基于虚拟机的行为检测技术存在两个缺点，其一是在系统中虚拟计算环境需要占用系统资源，对系统的性能产生影响；其二是激活恶意代码并分析其行为特征需要较长的时间，影响查毒效率。实现该技术难点是如何识别恶意代码的行为特征并构建行为特征库，需要确定哪些行为类型适合作为恶意代码的判断对象。

如果能有效地检测并及时清除系统中存在的恶意代码，可以减少系统受到的安全损害。但是恶意代码检测技术一般都是在系统存在恶意代码之后才能进行检测和清除的，此时恶意代码可能已经造成损害了，因此该技术并不能在第一时间阻止安全事件的发生，并且目前存在的恶意代码检测技术在检测的广度和精度上都不够，存在很多的漏报和误报。因此，恶意代码检测技术对提高网络的安全性作用有限。

1.1.2.3　防火墙技术

防火墙是在已授权和未授权通信实体之间作出判断的软件和硬件的设备组合，防止对重要信息的未授权的访问和修改②。防火墙作为网络安全的第一道防线，常常部署在内外网之间，通过筑高墙的方法，强化网络安全策略，对网络存取和访问进行监控和审计，防止内部私密信息外泄。防火墙从实现方式上分为硬件防火墙和软件防火墙，它们在原理和技术上类似，是为了适应不同的应用背景的需求而设计的。

防火墙所采用的技术分为五类，根据出现的时间先后秩序，依次为包过滤防火墙、应用级网关防火墙、电路级网关防火墙、状态包检查防火墙和自适应代理防火墙。包过滤防火墙是最早出现的防火墙，一般是依附在路由器之上的，可以称为包过滤器或者分组过滤器③。它工作在通信协议的网络层和传输层，根据预先建立的

---

① Arnold W, Tesauro G. Automatically Generated Win32 Heuristic Virus Detection [J]. Proceedings of the 2000 International Virus Bulletin Conference, 2000: 484-495.

② Gordon L A, Loeb M P, Lucyshyn W, Rchardson R. 2006 CSI/FBI Computer Crime and Security Survery [R]. Computer Security Institute Publications, 2005.

③ Keith E. Strassberb, Richard J. Gondex, Gary Rollie. 防火墙技术大全 [M]. 北京：机械工业出版社，2003：162-182.