信息安全产品技术丛书

网络 NETWORK 脆弱性扫描产品原理及应用

丛书主编 顾健

主编 沈亮 陆臻 张艳 宋好好

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息安全产品技术丛书

网络 NETWORK 脆弱性扫描产品原理及应用

丛书主编 顾健

主编 沈亮 陆臻 张艳 宋好好

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书内容共分为 5 章，从脆弱性扫描产品的实现、标准介绍入手，对脆弱性扫描产品的产生需求、实现原理、技术标准、应用场景和典型产品等内容进行了全面翔实的介绍。

本书适合脆弱性扫描产品的使用者（系统集成商、系统管理员）、产品研发人员及测试评价人员作为技术参考，也可以供信息安全专业的学生及其他科研人员作为参考读物。

图书在版编目（CIP）数据

网络脆弱性扫描产品原理及应用 / 沈亮等主编. —北京：电子工业出版社，2013.7
（信息安全产品技术丛书 / 顾健主编）
ISBN 978-7-121-20731-0

I. ①网… II. ①沈… III. ①信息系统—安全技术—研究 IV. ①TP309

中国版本图书馆 CIP 数据核字（2013）第 133072 号

策划编辑：李 洁
责任编辑：刘 凡
印 刷：三河市鑫金马印装有限公司
装 订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：720×1 000 1/16 印张：9.5 字数：197 千字
印 次：2013 年 7 月第 1 次印刷
定 价：42.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

<<<<< PREFACE

现在计算机网络已经成为了人们日常生活中不可缺少的部分，在大多数人生活中的重要性也越来越高。现在可以通过各种途径访问网络，从传统的计算机到时兴的终端，以及未来的物联网中各种千奇百怪的访问结点。人们在享受网络带来便捷的同时，也在越来越多地考虑网络所带来的安全问题。从早期神龙见首不见尾的黑客，到实实在在发生的各种“门”的泄密事件，再到网上银行漏洞被利用所引发的资金被盗的安全事件，网络安全越来越触及每个人的正常生活，人们也对使用网络产生了很多恐惧。

如何来保障网络安全，远离网络安全威胁？面对复杂多层的网络系统，应用简单而又直接的脆弱性扫描产品应运而生。

脆弱性扫描产品是网络使用者的一个重要的安全工具。它能模拟黑客的行为，对网络设备进行攻击测试，以帮助使用者在被黑客攻击之前找出存在的脆弱性漏洞。这些扫描器通过各种形式存在于我们的周围，如可能已经集成到个人防火墙或杀毒软件中的主机型扫描器，也可能早就存在于网络中或者使用它来探测其他安全设备漏洞的网络型扫描器。

脆弱性扫描产品是怎么产生的？其适用标准是如何实现的？本书就是带着这样的问题展开陈述的。

本书是信息安全产品技术丛书之一，就信息安全产品的历史、技术、标准等不同方面进行了全面的介绍。内容力争全面，分析力求深刻。在产品历史、原理、标准、应用等几大方面均有翔实的描述。与此同时，本书力求实用，收集了许多实际数据与案例，期望能够给读者在脆弱性扫描技术上一定的帮助。

本书的主要编写成员均来自公安部信息安全产品检测中心，他们常年从事脆弱性扫描产品的测评工作，对脆弱性扫描产品有深入的研究。本书的作者全程参与了脆弱性扫描产品标准从规范、行标到国标制定/修订的工作。因此，本书具有一定的权威性。

本书第 1 章由沈亮撰写，第 2 章由张艳撰写，第 3 章由陆臻撰写，第 4、5 章由张艳、宋好好、邵东撰写。顾健负责把握全书技术方向，并对各章节的具体编写提供了指导性意见，最后由沈亮完成全书修改和统稿工作。此外，俞优、王志佳、张笑笑、顾健新等同志也参与了本书资料的收集和部分章节的编写工作。由于编写人员水平有

限和时间紧迫，本书不足之处在所难免，恳请各位专家和读者不吝批评指正。

在本书的编写过程中，得到了福建榕基软件股份有限公司、北京神州绿盟信息安全科技股份有限公司、北京中科网威信息技术有限公司、北京天融信公司、北京网御星云信息技术有限公司等单位的大力协助，在此表示衷心的感谢！

编　者

目录

CONTENTS

第1章 综述 / 1

1.1 为什么要脆弱性扫描产品 / 2

1.1.1 网络中的安全问题 / 2

1.1.2 我国的网络安全问题现状 / 5

1.1.3 采用脆弱性扫描产品的必要性 / 7

1.2 怎样实施脆弱性扫描 / 10

1.2.1 脆弱性（漏洞）概述 / 10

1.2.2 脆弱性扫描产品的部署 / 15

1.3 脆弱性扫描产品的发展历程 / 17

第2章 脆弱性扫描产品的实现 / 19

2.1 传统网络面临的安全问题 / 19

2.1.1 面临的威胁 / 19

2.1.2 传统威胁防护方法的优缺点 / 23

2.1.3 脆弱性扫描的必要性 / 26

2.2 脆弱性扫描产品与技术 / 31

2.2.1 脆弱性扫描技术概述 / 31

2.2.2 脆弱性扫描技术分类 / 33

2.2.3 脆弱性扫描产品发展和现状 / 35

2.3 脆弱性扫描产品技术详解 / 41

2.3.1 端口扫描 / 41

2.3.2 漏洞扫描 / 45

2.3.3 规避技术 / 47

2.3.4 指纹技术 / 48

2.4 脆弱性扫描产品技术展望 / 50

2.4.1 技术发展趋势 / 50

2.4.2 产品发展趋势 / 51

第 3 章　脆弱性扫描产品标准 / 54
3.1　标准概述 / 54
3.1.1　脆弱性扫描产品标准简介 / 54
3.1.2　脆弱性扫描产品标准发展 / 55
3.2　标准介绍 / 58
3.2.1　MSTL_JGF_04—017 信息安全技术主机安全漏洞扫描产品检验规范 / 58
3.2.2　GB/T 20278—2006 信息安全技术网络脆弱性扫描产品技术要求 / 63
3.3　标准比较 / 66
3.3.1　GB/T 20278—2006 同 GA/T 404—2002 比较 / 66
3.3.2　MSTL_JGF_04—017 同 GB/T 20278—2006 比较 / 68
3.3.3　MSTL_JGF_04—016 同 GB/T 20278—2006 比较 / 69
3.3.4　等级和保证要求 / 70
3.4　GB/T 20278—2006 标准检测方法 / 70
3.4.1　自身安全要求 / 71
3.4.2　安全功能要求 / 73
3.4.3　管理要求 / 78
3.4.4　使用要求 / 81
3.4.5　性能要求 / 81
3.4.6　互动性要求 / 83

第 4 章　脆弱性扫描产品典型应用 / 85
4.1　产品应用部署 / 85
4.1.1　独立式部署 / 85
4.1.2　分布式部署 / 86
4.2　产品应用场合 / 86
4.2.1　政府行业中脆弱性扫描产品应用介绍 / 87
4.2.2　高校中脆弱性产品应用介绍 / 90
4.2.3　运营商中脆弱性产品应用介绍 / 92
4.2.4　金融行业中脆弱性产品应用介绍 / 93
4.2.5　能源行业中脆弱性产品应用介绍 / 95

第 5 章　脆弱性扫描产品介绍 / 98
5.1　榕基网络隐患扫描系统 / 98
5.1.1　产品简介 / 98

5.1.2 产品实现关键技术 / 99
5.1.3 产品特点 / 101
5.2 绿盟远程安全评估系统 / 104
5.2.1 产品简介 / 104
5.2.2 产品实现关键技术 / 104
5.2.3 产品特点 / 108
5.3 中科网威网络漏洞扫描系统 / 111
5.3.1 产品简介 / 111
5.3.2 产品实现关键技术 / 111
5.3.3 产品特点 / 114
5.4 网络卫士脆弱性扫描与管理系统 / 116
5.4.1 产品简介 / 116
5.4.2 产品实现关键技术 / 116
5.4.3 产品特点 / 117
5.5 网御漏洞扫描系统 / 119
5.5.1 产品简介 / 119
5.5.2 产品实现关键技术 / 119
5.5.3 产品特点 / 120
5.6 漏洞扫描评估系统 TW01 / 123
5.6.1 产品简介 / 123
5.6.2 产品实现关键技术 / 124
5.6.3 产品特点 / 125
5.7 极地网络漏洞扫描系统 / 126
5.7.1 产品简介 / 126
5.7.2 产品实现关键技术 / 126
5.7.3 产品特点 / 127
5.8 铱迅漏洞扫描系统 / 128
5.8.1 产品简介 / 128
5.8.2 产品实现关键技术 / 128
5.8.3 产品特点 / 131
5.9 NeXpose 漏洞管理系统 / 132
5.9.1 产品简介 / 132
5.9.2 产品实现关键技术 / 132
5.9.3 产品特点 / 133
5.10 网络漏洞扫描系统 / 134
5.10.1 产品简介 / 134

5.10.2 产品实现关键技术 / 135
5.10.3 产品特点 / 137
5.11 蓝盾安全扫描系统 / 137
5.11.1 产品简介 / 137
5.11.2 产品实现关键技术 / 138
5.11.3 产品特点 / 138
5.12 其他脆弱性扫描产品 / 140
5.12.1 远望网络脆弱性分析和漏洞扫描系统 v1.0 / 140
5.12.2 天鹰网络隐患扫描系统 TianYing III/v3.0 / 141
5.12.3 中华箭-综合网络安全检测评估增强系统 v3.0 / 141
5.12.4 永达安全漏洞扫描评估系统 v1.0 / 141
参考文献 / 142

Chapter 1

第1章 综 述

现在计算机网络已经变成人们日常生活中不可缺少的部分，在大多数人的生活中其地位的重要性越来越高。现在人们可以通过各种途径访问网络，从传统的电脑到时兴的终端，以及未来的物联网中各种千奇百怪的访问结点，人们在享受网络带来便捷的同时，也在越来越多地考虑网络所带来的安全问题。从早期神龙见首不见尾的黑客，到实实在在发生的各种“门”的泄密事件，以及网上银行漏洞被利用所引发的资金被盗的安全事件，网络安全越来越触及每个人的正常生活，人们也对使用网络产生了很多恐惧。

如何保障网络安全，远离网络安全威胁？这个问题不仅需要网络安全行业生产优良的网络安全防范和防护产品，网络管理人员进行网络安全维护，也需要使用者本人掌握必要的网络安全知识。用户不必精通但应会拿来主义，使用合适的方法和工具，采取基本的自我保护措施。而最简单、最直接的对个人计算环境安全进行评估的方法和工具，就是使用脆弱性扫描器，俗称“Scanner”或“漏洞扫描器”。这些扫描器通过各种形式存在于我们的周围，如可能已经集成到个人防火墙或杀毒软件中的主机型扫描器，也可能早就存在于你的网络中或者你使用它来探测其他安全设备漏洞的网络型扫描器。

面对现在复杂的多层结构网络系统，脆弱性扫描是网络使用者的一个重要安全工具。脆弱性扫描能够模拟黑客的行为，对网络设备进行攻击测试，帮助使用者在被黑客攻击之前找出存在的脆弱性漏洞。这样的工具可以提高本地或远程评估使用者的网络安全级别，并生成评估报告，提供相应的整改措施。选择正确的脆弱性扫描工具，对于提高网络设备和系统的安全性非常重要。

本章将首先对脆弱性扫描器产品存在的必要性进行分析，简要介绍脆弱性扫描器产品的基本原理，并按照主机型和网络型两种模式产品介绍脆弱性扫描器产品的发展历程，从宏观上使读者对脆弱性扫描产品有充分的认识，为后续章节介绍具体的技术细节打下基础。

1.1 为什么要脆弱性扫描产品

1.1.1 网络中的安全问题

随着计算机网络的快速发展，信息共享应用日益普及和重要。但是，信息在共享的通信网络上传输、存储和共享的过程中，会面临大量威胁，包括被非法嗅探、截取、篡改和破坏等。这些安全威胁可能会给网络使用者带来巨大的有形或无形的损失，使得网络使用者丧失对网络安全的信心。尤其是对金融、生产、基础设施、政府或军方等同民生密切相关网络系统，信息在公共网络中传输、存储过程中的可用性、保密性、完整性等网络安全问题更是重中之重。

网络安全的概念正是在这样的背景之下产生的。网络安全是指：网络系统中的硬软件及其系统中的数据受到保护，不因偶然或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全，可以从不同角度对网络安全做出不同的解释。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。一般意义上，网络安全包括信息安全和控制安全两部分。国际标准化组织把信息安全定义为“信息的完整性、可用性、保密性和可靠性”；控制安全则是指身份认证、不可否认性、授权和访问控制。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。研究和发展网络安全的目的，就是为了防范和防御网络攻击。虽然在这方面，各个国家都做了巨大的努力，但是网络安全事件还是层出不穷。

辅助阅读

2011 年国际上网络安全事件大盘点

2011 年，网络安全威胁形势进一步加剧，安全形势并没有好转。黑客集团 Anonymous 有愈发猖獗之势，回顾 2011，攻击事件层出不穷。

谷歌 Android 市场出现恶意软件

2011 年 3 月初，Android 出现一系列的恶意应用软件，这些应用软件可窃取用

户数据和未得到手机主人确认许可便“拨出”电话或发昂贵的短信。由于该问题在技术上没有找到好的解决办法，3 月 4 日谷歌 Android 官方应用商店不得不宣布将 56 款包含木马的手机应用下架。虽然谷歌已经从 Android 市场删除了有问题的应用软件，但公司“未对任何已经被下载的恶意软件采取行动”。用户实际上是希望谷歌能远程禁用这些恶意应用软件。安全专家发出警告，很多 Android 智能手机用户下载了可窃取数据或发送收费短信的恶意软件。随后，谷歌 Android 官方应用商店宣布将 56 款包含木马的手机应用移除。

索尼被黑，黑客借网络入侵炫耀

自从 2011 年 4 月 PlayStation 网络入侵事件导致 1 亿多个用户账户曝光以来，索尼共遭遇到大大小小的黑客攻击 10 余次。索尼影视（SonyPictures）、索尼欧洲（SonyEurope）、索尼希腊 BMG 网站（SonyBMGGreece）、索尼泰国（SonyThailand）、索尼日本音乐（SonyMusicJapan）、索尼爱立信加拿大（SonyEricssonCanada）等，无一不成为黑客攻击的目标。最初发生的 PlayStation 网络入侵事件是索尼迄今为止遭遇到的规模最大的黑客攻击。专家认为，索尼之所以遭遇网络攻击问题，一方面是因为索尼的系统缺乏稳定的安全性，另一方面是因为新崛起的黑客群体更乐意出风头，炫耀他们入侵公司防御系统的能力，至于惩罚索尼倒还在其次。“索尼需要时间来调整其安全方案。”White Hat Security 公司的首席技术官杰里米·格罗斯曼（Jeremiah Grossman）说，“作为一个组织，索尼应该将此危机看做一个机会。从现在起一年或一年以上，他们可能成为整个行业处理安全问题的榜样。”尽管随着其他网络攻击事件见诸报端，攻击索尼的新颖性可能会逐渐降低，但是索尼显然必须加强其安全措施，否则还会遭遇更多的攻击，丧失更多的用户和金钱，并可能导致政府的干预。

RSA 公布被攻击内幕：钓鱼邮件惹祸

EMC 在 2011 年 3 月中旬宣布，旗下安全部门 RSA 遭遇黑客攻击。EMC 报告称，RSA 被一种业内称为“高持续性威胁”（Advanced Persistent Threat）的复杂网络攻击，这是一种“极其复杂”的攻击，会导致一些秘密信息从 RSA 的 SecurID 双因素认证（Two-factor Authentication）产品中提取出来。RSA 客户包括一些大军事机构、政府、各种银行及医疗和医保设备。瑞纳称，在两天的时间内，公司一部分普通员工收到了一些电子邮件，这些邮件带有一个名为“2011 年招聘计划”的 Excel 表格附件。一些员工打开了附件，并在表格空白处填写了内容。而该表格包含一个“零日漏洞”，主要是利用了 Adobe Flash 的漏洞。通过该漏洞，黑客可以在目标计算机上安装任何程序。黑客选择安装的是“Poison Ivy RAT”，这是一个远程控制程序，用某个地方的计算机控制另一个地方的另一台计算机。通过远程访问目标计算机，黑客获得了 RSA 企业网络的进一步访问权，这就好比是带着面罩冒充 RSA 员工在公司内部搜索万能密钥。最初，黑客利用被入侵的低级别账号来收集登录信息，其中包括用户名、密码和域名信息等。之后黑客又将目标瞄向拥有更多访问权的高级账号，一旦成功，他们就可以从 RSA 网络系统中盗取任何需要的信息，之后打包并

通过FTP下载。

美国花旗银行被黑客侵入

美国花旗银行于2011年6月8日证实，该银行系统日前被黑客侵入，21万个北美地区银行卡用户的姓名、账户、电子邮箱等信息可能被泄露。花旗银行的一位发言人说，监管人员在对银行系统进行例行检查时发现，不明黑客侵入银行系统，盗取了大批信用卡持有者的信息。据估计，约1%的信用卡持有者受到入侵事件的影响。这位发言人说，被盗取的信息包括用户的姓名、账号以及电子邮箱地址等联系方式，但用户的出生日期、社会安全号、信用卡过期日及安全密码等信息没有被盗取。这位发言人说，银行正在联系受影响的客户，并加强了安全保护措施。尽管花旗银行坚称此次攻击造成的破坏有限，但专家们还是说这是对美国大型金融机构最大的一次直接攻击，并表示这次事件或将促成银行业数据安全体系的彻底大修。

IMF数据库遭“黑客”攻击

国际货币基金组织（IMF）连遭打击。继前总裁多米尼克·斯特劳斯·卡恩因强奸罪指控锒铛入狱之后，IMF又爆出内部网络系统遭黑客袭击。英国《每日邮报》称，这是一起“经过精心策划的严重攻击”，作为目前国际社会应对金融危机努力中的领导者，IMF掌握着关于各国财政情况的绝密信息，以及各国领导人就国际救市计划进行的秘密协商的有关材料。一旦这些内容泄漏，不仅将对世界经济复苏造成严重的负面影响，更有可能引发一些国家的政治动荡。美国《纽约时报》消息称，此次事件可能只是黑客在试验被入侵系统的性能。此外，也有人认为国际货币基金组织此次遭袭是一起“网络钓鱼”事件：该组织的某位工作人员可能在不知情的情况下误点了某个不安全的链接，或者运行了某个使黑客得以入侵的软件。大多数被黑客攻击的组织或机构都不愿意透露过多的信息，因为他们担心这样做只会带来更多的入侵。

Facebook被黑，暴力色情图片泛滥

据2011年11月15消息，社交网络Facebook已遭到了黑客攻击，部分用户抱怨在其个人资料页面中目睹了大量色情和暴力图片。有人认为，这是黑客组织Anonymous所为。这个问题开始于两三天前，现在已有愈演愈烈之势。该社交网络的部分用户抱怨称，一些暴力或色情的图片在未经他们许可的情况下就出现在了他们的新闻动态信息中；还有些用户则被告知，他们的Facebook好友正在发送点击链接或视频的请求。这类似于我们以前在Facebook上见过的那类垃圾信息。不同的是，它来得要迅猛得多，似乎是提前计划好的。有媒体称，这些垃圾信息中的链接并不是要将用户带到别的什么地方，而是为了“侵入用户的账户，并向该用户的所有好友发送类似的垃圾信息”。在Twitter上搜索“Facebook色情”可以发现，这两个社交网络的用户对此发出了很多抱怨之声。

从以上事件中可以看出，各个国家以及整个互联网网络都面临着巨大的安全威胁，网络犯罪已经成为了国际上普遍的问题。网络犯罪因其具有的专业性、瞬间性、时空跨越性等特点，通常都很难获得犯罪证据，所以激发了网络犯罪的高发率，使

得网络安全事件频发。此外，随着网络攻击预期的危害性不断扩大，各国也希望能够通过利用敌对国网络安全问题在战争时期对对方发动网络战，欲求使用最小的代价获得巨大的胜利。“网络战”这个名词也迅速被人们所接受。

作为全球信息化程度最高的国家，美国拥有世界上最先进和最庞大的信息系统，对信息网络的依赖性和网络安全的认知程度也最高，就是它将国家的网络安全引申到了国际间网络战的高度，当然这也是有历史原因的。“网络战”最早获得关注的事件，始于1988年11月2日。一种不知名的计算机病毒“入侵”了美国国防部战略系统的主控中心和各级指挥中心，导致8500台军用计算机出现各种异常情况，造成上亿美元直接经济损失。调查发现，美国康奈尔大学计算机系23岁学生莫里斯抱着恶作剧的心态，利用病毒操纵计算机程序侵入美国国防部战略C4I系统的计算机主控中心和各级指挥中心，最终导致这起恶性事件的发生。这次事件给美军敲响了警钟：只要有一台计算机接入互联网，就有可能制造比杀伤性武器还要严重的伤害。有得必有失，1991年海湾战争期间，美国向伊拉克派出特工，将伊拉克从法国购买的防空系统使用的打印机芯片换上了含有计算机病毒的芯片。在美国对伊拉克实施战略空袭前，美特工用遥控手段激活了这些芯片中的病毒，致使伊拉克防空指挥中心主计算机系统程序错乱，伊拉克防空C3I系统失灵，从而为美军的袭击提供了便利条件。这次行动也让美军尝到了信息技术的甜头，于是网络安全开始逐渐被提升到战略的高度。事实上，从20世纪90年代起美国军队已开始大量招募网络人才。1995年，五角大楼开始组织第一批“黑客”，在网络空间与敌人展开全面信息对抗。两年后，第一批国家级“网络战士”参加了美国国家安全局组织的秘密演习。到了2002年，美国总统布什签署了“国家安全第16号总统令”，组建美军历史上，也是世界上第一支国家级网络“黑客”部队——“网络战联合功能司令部”(Joint Functional Component Command—Network Warfare)。这支部队由世界顶级电脑专家和“黑客”组成，其人员组成包括美国中央情报局、国家安全局、联邦调查局以及其他部门的专家，甚至还可能包括盟国的顶级电脑天才，所有成员的平均智商都在140分以上，因此也被一些媒体戏称为“140部队”。

随着个人犯罪发展到有组织犯罪，甚至国家网络战，网络安全问题越来越被人们所扩大。各种利用网络安全脆弱性的新型攻击正在被大量发掘和扩散，攻击所造成的影响不断严重，网络系统所面临的安全风险和威胁也日趋严重。

1.1.2 我国的网络安全问题现状

1. 网络安全事件频发

根据中国互联网络信息中心（CNNIC）发布的《第29次中国互联网络发展状况统计报告》显示，截至2011年12月底，中国网民规模突破5亿人，互联网普及率

较2010年提升4个百分点。根据Translated 2011年的T-Index数据，美国在线市场份额（16.8%）将会在2015年低于中国份额（18.8%）。也就是说，预计到2015年中国的网络市场容量将超越美国，成为全球第一。由于我国经济的飞速发展以及本身固有的人口大国的原因，巨大的网络发展规模和网络市场已经将我国网络商业价值推到了前所未有的高度，随之日益突出的网络安全问题也摆在了我们面前。

近期我国的商业、金融和政府等重要网络信息系统频遭攻击，网站被入侵、被篡改和被挂马等安全事件多发。据国家互联网应急中心（CNCERT）监测，2012年1～4月，我国境内被篡改网站数量分别为1888个、1853个、2035个、1957个，其中商业类和政府类网站占多数；据中国国家信息安全漏洞库（CNNVD）监测，2012年1～4月，我国境内被挂马网站分别为5106个、9608个、6683个、3715个，其中商业类网站占多数；2012年1～4月，中国反钓鱼网站联盟认定并处理钓鱼网站8451个，其中支付交易类、金融证券类钓鱼网站占近90%的份额。

在针对我国重要网络信息系统的攻击中，有两个动向值得关注。一是出于政治动机的攻击，针对我国的出于政治动机的黑客活动较频繁。例如，2012年3月以来，名为“匿名者中国”的黑客组织入侵了我国近500多个网站，目的是摧毁“中国的大防火墙”。4月，因黄岩岛之争菲律宾黑客攻击了我国多家网站。二是有针对性的高级可持续性攻击（Advanced Persistent Threat）。2012年3月，趋势科技在中国区监测到一起针对金融行业的高级可持续性攻击，该攻击主要针对证券、基金和银行等金融行业用户，在用户环境中已经存在一年或更长的时间。

当前针对我国网络信息系统中的重要信息，谋取经济利益仍是黑客攻击的主要目标之一。我国电子商务、金融等机构的信息和数据泄露事件多发，引发了社会广泛关注。例如，2011年12月21日上午，有黑客在网上公开CSDN网站的用户数据库，导致600余万个注册邮箱账号和与之对应的明文密码（即用户密码是什么样，网站数据库就存成什么样）泄露之后，22日，网上曝出人人网、天涯社区、开心网、多玩、世纪佳缘、珍爱网、美空网、百合网、178、7K7K等知名网站的用户称密码遭网上公开泄露。最新监测数据发现，目前网上公开暴露的网络账户密码超过1亿个。“泄密门”的爆出将原来潜伏在水面之下的互联网信息安全问题变成公众关注的焦点。今年，京东商城、当当网、1号店等电子商务网站又被曝账户信息泄露，给用户造成了不同程度的损失；中国电信网络被名为Swagg Sec的黑客组织攻破，包括900个网络管理员的用户名和密码信息被窃取。除此之外，还发生了一些内部人员的泄密事件。例如，招商、工商等银行员工低价向第三方出售客户征信报告和银行卡信息，导致客户资金被盗等。

2. 境外攻击增多仍是我国网络安全面临的主要威胁之一

由于我国信息安全业发展较晚，造成了我国网络安全防护能力不足、安全防护意识淡薄等情况产生，在我国境内有大量主机被境外木马或僵尸网络所控制。据

CNCERT 统计，2011 年境外有近 4.7 万个 IP 地址作为木马或僵尸网络控制服务器参与控制我国境内近 890 万个主机；2012 年 1～4 月，境外木马或僵尸网络控制服务器 IP 数量分别为 10287 个、8213 个、10711 个、9005 个。目前，美国、日本和韩国仍然是境外网络攻击的主要来源国。境外网络攻击在使境内主机受害的同时，还通过控制境内主机发动针对其他国家的攻击，从而使我国事实上成为这些攻击的“替罪羊”，对我国危害很大。

3. 信息安全产品漏洞隐患多、被渗透利用的风险高

当前，我国基础信息网络和重要信息系统使用的网络信息和网络安全产品的核心技术很多都受制于国外，这些产品不可避免地存在安全漏洞。据 CNNVD 监测，2012 年 1～5 月，我国新增安全漏洞 2619 个，其中危急和高危漏洞 1071 个，占到漏洞总量的 41%。这些信息和网络安全产品的安全漏洞一旦被利用，将严重威胁我国的信息安全。例如，2012 年 3 月发现的 Google Chrome 任意代码执行漏洞，攻击者可以利用该漏洞执行任意代码；又如，英国研究人员发现在波音 787 和一些军用电子系统中应用的芯片存在严重安全漏洞，黑客可以利用该漏洞侵入我国基于以上技术的信息系统，并对系统进行遥控操纵。

4. 基础信息网络和重要信息系统的安全防护存在不足

当前全球网络安全威胁日益复杂，军事集团和国家级别等政治组织成为网络攻击的主体，类似于网络战，攻击目的很可能就是破坏对方国家的重要关键基础设施。再适逢下一代互联网架构的发展，面对新的、甚至是全新的安全威胁，传统的安全防护措施不能立即发挥有效的作用，因此必须建立基于风险的、动态的防御体系，但我国在网络态势感知等应对新威胁的技术研发上还较落后。再加上当前我国基础信息网络和重要信息系统在安全技术和管理上还是存在着大量不足的地方。例如，多家电子商务网站仍采用明文方式存储密码；中国电信将网络管理员的重要信息存储在不安全的 SQL 服务器上。

以上的这些管理和技术漏洞都很容易被不法分子所利用，成为威胁我国信息安全的重要隐患。这些安全问题给我国信息安全带来了很大的挑战，但同时，也为我国信息安全技术和产业带来了前所未有的发展机遇。强化基础网络安全的建设和管理，大力发展信息安全和网络安全产品，堵截信息安全漏洞都是我国现阶段信息安全建设工作的重要组成部分。而脆弱性扫描技术和产品作为信息安全脆弱性评估的重要工具之一，就是在这一背景之下而大力发展起来的。

1.1.3 采用脆弱性扫描产品的必要性

说到脆弱性扫描产品，就不得不提到风险评估。原先脆弱性扫描产品作为一种

黑客、灰客、红客等各种色彩用户所使用的单个工具，对于信息安全而言，其必要性不言而喻。这时候脆弱性扫描产品的着眼点比较偏重技术，使用目的也比较简单，就是为这些用户直接获得脆弱性信息或者防御攻击而已。近些年，随着风险评估技术的兴起，风险评估则将脆弱性扫描产品的使用上又上升了一个档次。结合资产、威胁、风险计算，使得脆弱性扫描产品能够为巨大的信息系统进行风险分析，从而为信息安全企业管理层面采取安全措施提供直接的指导。这样一来，使得信息系统企业能够较容易接受风险评估，使得脆弱性扫描产品得到了巨大的发展，这就是近些年来采用脆弱性扫描产品的另一个重要原因了。

风险评估是指对信息系统安全进行风险分析，通过归纳、比较、综合，确定系统各个风险因素对信息安全影响的强弱程度，便于决策者将有限人力、物力、财力进行合理分配。其目的是为了确保通过合理的步骤，防止对信息安全构成威胁的事件发生。信息安全受到威胁与信息安全防护措施是交互出现的，不适当的信息安全防护，不仅不能减少信息的安全风险，浪费大量的资金，而且可能招致更大的安全威胁。因此，周密的信息安全风险分析，是制定可靠、有效的安全防护措施的必要前提，也是安全管理的一个重要组成部分。

从网络信息安全风险评估的角度来说，通过识别和分析信息安全风险要素（资产的价值、脆弱性被利用的难易程度、威胁的动机和能力的大小、现有控制措施的效果）及其相互关系，来判断信息安全事件发生的可能性、事件后果的严重性和控制措施的有效性，计算出信息安全风险程度的过程，主要涉及对资产、威胁、脆弱性三个基本要素的分析。

资产是指对组织具有价值的信息或资源，是安全策略保护的对象。

威胁是指任何能够导致对网络系统或组织造成潜在破坏和伤害的外部因素，包括人、对象或者事件。网络安全面临的威胁主要有以下几大类。

1. 非人为造成的安全威胁

1）对实体安全的威胁

自然因素主要侵害实体安全。计算机网络中的各种设备和通信线路容易受到不适当的温度和湿度、灰尘、有害气体、水灾、火灾、雷电、地震、静电和电磁辐射等各种自然因素的干扰和破坏。有时因电子元件自身的质量不好，再加上外界因素影响，也会引起故障，甚至酿成严重的安全问题。由这些原因造成的事故和损失国内外都有所报道。

2）电磁辐射

除影响实体安全外，强烈的电磁辐射也可能破坏软件的数据，干扰系统的运行，引起机器的误动作。电磁辐射主要来源于计算机及其外围设备和通信设备在进行信息处理时产生的电磁泄漏。由于电子器件向外部辐射部分电磁波，导致信息泄漏；各种电源线、电缆和电话线路等通信链路，在传输过程中也会造成信息泄漏。