



中华人民共和国国家标准

GB/T 20280—2006

20061727

信息安全技术 网络脆弱性扫描产品测试评价方法

Information security technology—
Testing and evaluation approaches for network vulnerability scanners



2006-05-31 发布

2006-12-01 实施

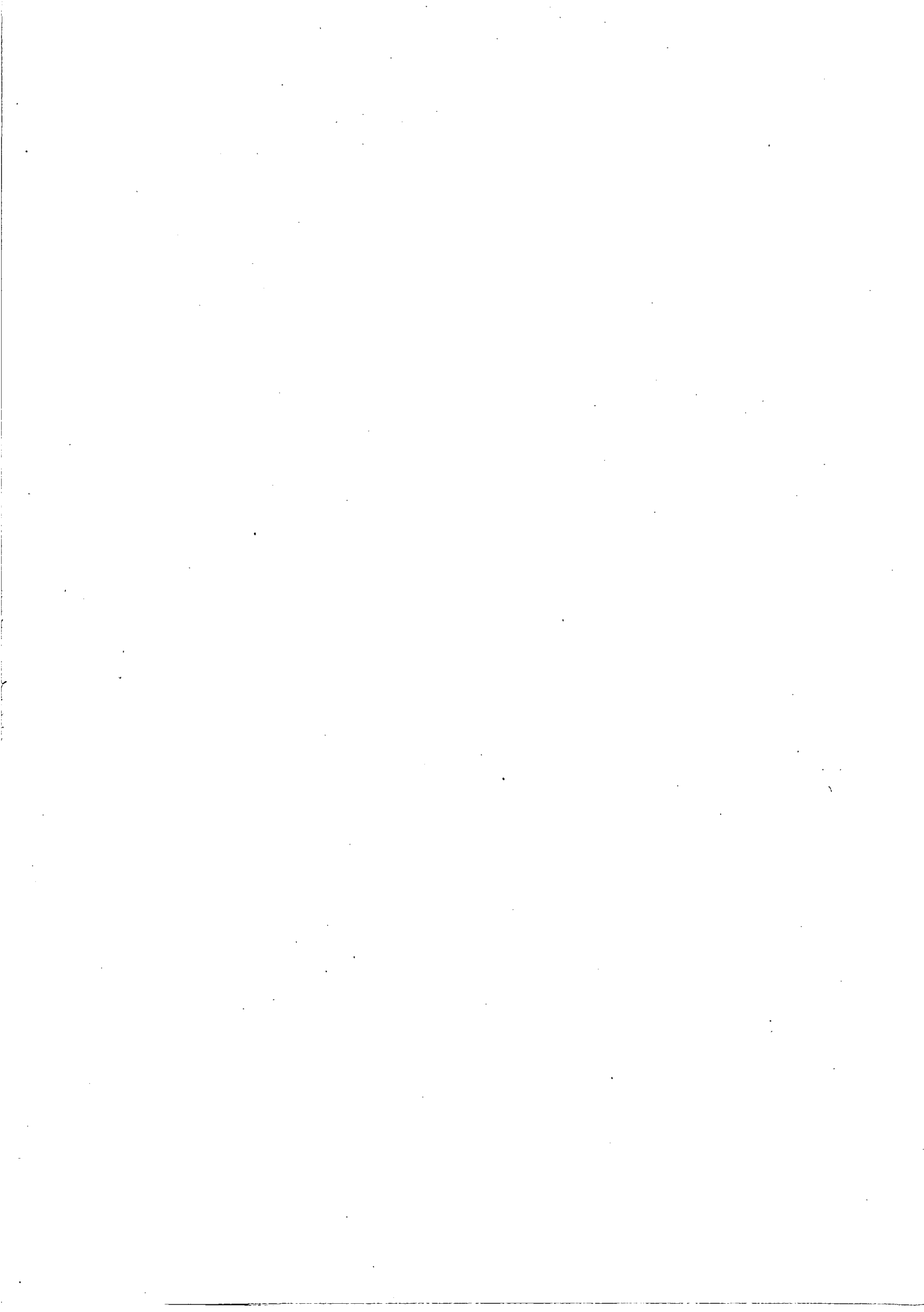
中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会

发布



目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号、缩略语和记法约定	1
4.1 符号和缩略语	1
4.2 记法约定	1
5 网络脆弱性扫描产品概述	2
6 测试环境	2
7 测试评价方法及步骤	3
7.1 基本型	3
7.1.1 基本功能	3
7.1.2 性能要求	7
7.1.3 安全保证要求	8
7.2 增强型	10
7.2.1 基本功能及性能	10
7.2.2 增强功能	10
7.2.3 安全保证要求	12
附录 A (规范性附录) 产品厂商向测试单位提供的测试证据	19
A.1 基本型	19
A.2 增强型	19
参考文献	20
图 1 网络脆弱性扫描产品测试环境拓扑图	2
表 1 环境说明	2



前 言

本标准的附录 A 为规范性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准由北京中科网威信息技术有限公司、公安部十一局负责起草。

本标准主要起草人：肖江、陆驿、杨威、刘伟、刘兵、丁宇征。

引 言

本标准规定了网络脆弱性扫描产品的测评方法,包括网络脆弱性扫描产品测评的内容,测评功能目标及测试环境,给出产品基本功能、增强功能和安全保证要求必须达到的具体目标。

本标准的目的是为网络脆弱性扫描产品的研制、生产和认证提供技术支持和指导。

正确使用符合本标准的评价活动,其结果可以得到确认,检测对象可以对网络进行脆弱性检查,对发现的安全隐患提出解决建议,从而提高了产品的质量。

信息安全技术

网络脆弱性扫描产品测试评价方法

1 范围

本标准规定了对采用传输控制协议和网际协议(TCP/IP)的网络脆弱性扫描产品的测试、评价方法。

本标准适用于对计算机信息系统进行人工或自动的网络脆弱性扫描的安全产品的评测、研发和应用。

本标准不适用于专门对数据库系统进行脆弱性扫描的产品。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 5271.8—2001 信息技术 词汇 第8部分:安全(idt ISO/IEC 2382-8:1998)

GB/T 20278—2006 信息安全技术 网络脆弱性扫描产品安全技术要求

3 术语和定义

GB/T 5271.8—2001 和 GB/T 20278—2006 确立的术语和定义适用于本标准。

4 符号、缩略语和记法约定

CVE

通用脆弱性知识库

Common Vulnerabilities and Exposures

DNS

域名系统

Domain Name System

b) 说明:本标准对网络脆弱性扫描产品测评进行了分级论述。本标准中的规定,凡未特殊说明,均为基本型产品要求,增强型产品的测评项目、测试内容和测试评价结果用斜体字表示。

5 网络脆弱性扫描产品概述

网络脆弱性扫描产品的简介、体系结构及产品分级见 GB/T 20278—2006 的第 5 章和附录 A

6 测试环境

网络脆弱性扫描产品测试环境如图 1,图 1 中各项设备的作用见表 1:

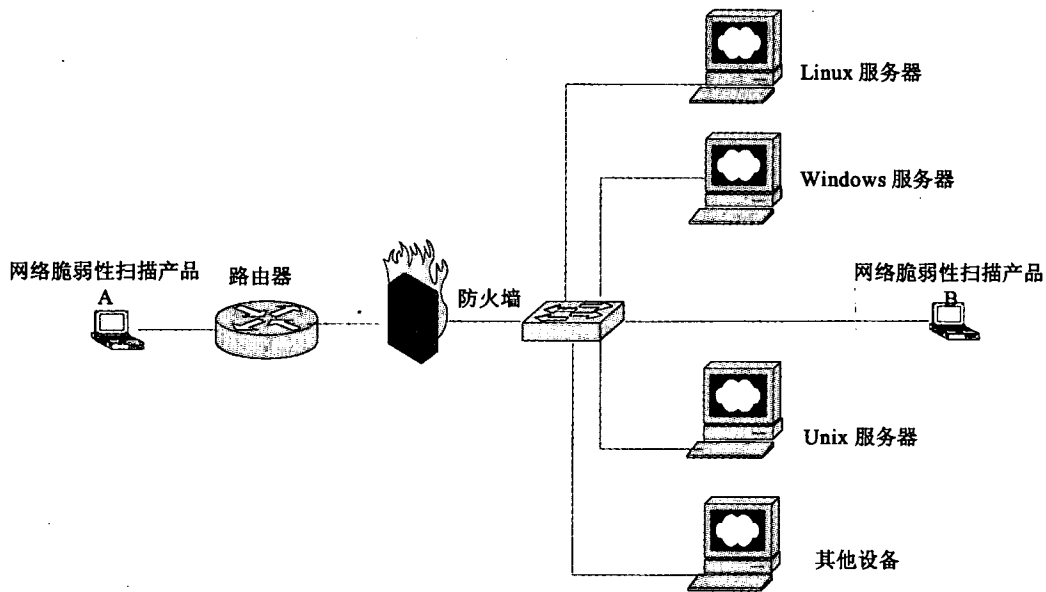


图 1 网络脆弱性扫描产品测试环境拓扑图

表 1 环境说明

名称	作用
脆弱性扫描产品 A	脆弱性扫描产品 A,部署在目标网络之外,进行远程扫描
脆弱性扫描产品 B	脆弱性扫描产品 B,部署在目标网络内部,进行网内扫描
防火墙	隔离网段
Unix 服务器	被扫描机器
Linux 服务器	被扫描机器
Windows 服务器	被扫描机器
其他设备	被扫描机器 包括路由器 交换机 防火墙

7 测试评价方法及步骤

7.1 基本型

7.1.1 基本功能

7.1.1.1 自身安全性要求

1) 根据网络脆弱性扫描产品版本发行说明、管理员手册、配置管理文档等,启动图 1 中网络脆弱性扫描产品 A 和 B;

2) 以授权管理员身份分别登录启动图 1 中网络脆弱性扫描产品 A 和 B,运行创建普通管理员等操作。

c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断。

7.1.1.1.2 适用限制

、评价内容见 GB/T 20280—2006 中 7.1.1.1 的内容

7.1.1.1.6 扫描结果安全

a) 评价内容:见 GB/T 20278—2006 中 7.2.6 的内容。

b) 测试评价方法:

1) 根据网络脆弱性扫描产品版本发行说明、用户手册、管理员手册、高层设计文档、低层设

计文档等,对扫描产品的脆弱性扫描工具和人机交互进行扫描。

7.1.1.2.4 端口和服务扫描

- a) 评价内容:见 GB/T 20278—2006 中 7.3.4 的内容。
- b) 测试评价方法:
 - 1) 根据管理员手册和用户手册等,启动图 1 中网络脆弱性扫描产品 A 和 B,配置产品策略,针对以下端口和服务进行扫描:
 - RPC 端口;
 - TCP 端口;
 - UDP 端口;
 - 端口协议分析;
 - NT 服务。
 - 2) 手工对比扫描结果。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:
 - 1) 获得 RPC 服务及所在的 RPC 端口信息;
 - 2) 应能检查 TCP 端口是否开启;
 - 3) 应能检查 UDP 端口是否开启;
 - 4) 就扫描得到的已开启的 TCP/UDP 端口,能够判断相应端口对应的服务或使用的协议;
 - 5) 获取启动的 NT 服务列表。

7.1.1.3 管理要求

7.1.1.3.1 管理员访问

- a) 评价内容:见 GB/T 20278—2006 中 7.4.1 的内容。
- b) 测试评价方法:
 - 1) 根据安装手册、管理员手册、测试文档等,启动网络脆弱性扫描产品 A 和 B,检测管理员访问功能;
 - 2) 查看授权管理员访问权限,并设置普通管理员权限;
 - 3) 验证普通管理员权限。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:
 - 1) 只有授权管理员才能访问网络脆弱性扫描产品,即只允许授权管理员有配置、使用网络脆弱性扫描产品的能力;
 - 2) 普通管理员部分具有由授权管理员分配的配置或使用网络脆弱性扫描产品的能力。

7.1.1.3.2 扫描结果分析处理

- a) 评价内容:见 GB/T 20278—2006 中 7.4.2 的内容。
- b) 测试评价方法:
 - 1) 根据附录 A 中测试证据及上述测试过程产生的结果,手工比对;
 - 2) 利用网络脆弱性扫描产品软件对扫描结果进行导入、导出、删除、定制报告、输出报告、浏览漏洞数据库等;
 - 3) 仔细查看形成的扫描结果报告。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:
 - 1) 扫描结果写入数据库;
 - 2) 扫描结果可导入导出及彻底删除;
 - 3) 可按照不同的分类定制报告(例如:以时间、用户组分类);
 - 4) 报告可输出成标准格式,包括 HTML、RTF、PDF 等格式;
 - 5) 可提供全面灵活的扫描结果数据库浏览功能;
 - 6) 可提供包括以下内容的扫描结果报告:

- 脆弱性报告,包括各脆弱点的详细信息、补救建议等,补救建议合理并有效;
- 可对目标主机扫描后的信息获取结果生成相应的报告;
- 脆弱性分析报告,包括:
 - 目标的风险等级评估报告;明确将扫描脆弱点分成极度危险漏洞、危险漏洞和轻度危险漏洞;
 - 同一目标多次扫描形成的趋势分析报告;
 - 多个目标扫描后的结果的总体报告;
 - 对关键的网络脆弱性扫描信息可生成摘要报告;
 - 针对主机间进行比较的结果生成报告。

7.1.1.3.3 扫描策略定制

a) 评价内容:见 GB/T 20278—2006 中 7.4.3 的内容。

b) 测试评价方法:

- 1) 根据网络脆弱性扫描产品版本发行说明、安装手册、管理员手册、配置管理文档、测试文档、高层设计文档等,启动图 1 中网络脆弱性扫描产品 A 和 B,确认是否具有定制策略方法;
 - 2) 定制已知账号和口令、扫描项目及属性、定时启动等策略,进行扫描;
 - 3) 查看日志,验证审计功能。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:
- 1) 能使用目标的已知账号和口令对目标进行更有效的扫描;
 - 2) 能定制扫描项目及属性,形成计划任务等策略;
 - 3) 具有完整的日志及审计功能;
 - 4) 提供方便的定制策略的方法。

7.1.1.3.4 扫描对象的安全性

a) 评价内容:见 GB/T 20278—2006 中 7.4.4 的内容。

b) 测试评价方法:

- 1) 查看网络脆弱性扫描产品版本发行说明、安装手册、管理员手册、配置管理文档、测试文档、高层设计文档等,并启动图 1 中网络脆弱性扫描产品 A 和 B;
 - 2) 对报警功能进行验证,观察目标系统网络性能。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:
- 1) 能够在开始扫描前宿主机向目标主机发送一个警告信息,提示该主机将要接受扫描测试;
 - 2) 扫描时对网络的正常工作无明显影响;
 - 3) 使用 DOS 等攻击测试手段时,测试开始前向用户发出的明确提示中,说明了该类测试的危害性,用户可以采取确认与否操作。

7.1.1.3.5 升级能力

a) 评价内容:见 GB/T 20278—2006 中 7.4.5 的内容;

b) 测试评价方法:查看网络脆弱性扫描产品版本发行说明、安装手册、用户手册等,启动图 1 产品

A 和 B,扫描用户手册检查产品是否具有升级更新能力。

- b) 测试评价方法:查看网络脆弱性扫描产品版本发行说明、安装手册、管理员手册、配置管理文档,对网络脆弱性扫描产品进行实际安装、操作。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:
 - 1) 随机文档中对网络脆弱性扫描产品安装、管理、操作的可控性有说明,网络脆弱性扫描产品实行发行许可措施(例如:发行序列号、根据安装计算机信息生成许可等);
 - 2) 网络脆弱性扫描产品扫描过程可随时停止,并且能断点保存,随时恢复;
 - 3) 网络脆弱性扫描产品扫描过程中,能执行键盘锁定功能和屏幕保护功能。

7.1.2 性能要求

7.1.2.1 速度

- a) 评价内容:见 GB/T 20278—2006 中 8.1 的内容。
- b) 测试评价方法:
 - 1) 根据网络脆弱性扫描产品安装手册、管理员手册、测试文档、高层设计文档、产品版本发行说明及产品运行界面(或面板),并启动图 1 中网络脆弱性扫描产品 A 和 B;
 - 2) 检查网络脆弱性扫描产品是否采取了有效的设计或技术手段来提高扫描速度(例如:能提供通过调整线程或者进程数目来调节扫描速度),并实际操作验证其对速度的影响。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:网络脆弱性扫描产品采取了有效的设计或技术手段,能够提高扫描速度。

7.1.2.2 稳定性和容错性

- a) 评价内容:见 GB/T 20278—2006 中 8.2 的内容。
- b) 测试评价方法:
 - 1) 观察上述网络脆弱性扫描产品测试过程,确定产品是否能够避免以下问题出现:
 - 主界面失去响应或非正常退出;
 - 扫描进度停滞不前。
 - 2) 反复试用网络脆弱性扫描产品。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,应符合:无界面失去响应,扫描进度停滞不前或非正常退出现象。

7.1.2.3 漏洞发现能力

- a) 评价内容:见 GB/T 20278—2006 中 8.3 的内容;
- b) 测试评价方法:查看网络脆弱性扫描产品版本发行说明、安装手册、管理员手册、配置管理文档;试用网络脆弱性扫描产品;
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,应符合:网络脆弱性扫描产品的技术文档及产品界面中给出系统能够扫描的漏洞数目,并针对漏洞给出详细描述。

7.1.2.4 误报率

- a) 评价内容:见 GB/T 20278—2006 中 8.4 的内容。
- b) 测试评价方法:查看网络脆弱性扫描产品版本发行说明、安装手册、管理员手册、配置管理文档;试用网络脆弱性扫描产品。

c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,应符合:网络脆弱性扫描产品的技术文档及产品界面中给出系统能够扫描的漏洞数目,并针对漏洞给出详细描述。

脆弱性扫描产品的技术文档标明了该系统的漏报率,并指明所使用的测试方法、测试工具、测试环境和测试步骤。

7.1.3 安全保证要求

7.1.3.1 配置管理

- a) 评价内容:见 GB/T 20278—2006 中 9.1.1 的内容。
- b) 测试评价方法:评价者应审查开发者提供的配置管理支持文件是否包含以下内容:
 - 1) 版本号,要求开发者所使用的版本号与所应表示的网络脆弱性扫描产品样本应完全对应,没有歧义;
 - 2) 授权标识,要求开发者所提供的授权标识与所提供用户的网络脆弱性扫描产品样本完全对应且惟一;

- 1) 评价开发者提供的测试文档,是否包括测试计划、测试过程、预期的测试结果和实际测试结果;
 - 2) 评价测试计划是否标识了要测试的安全功能,是否描述了测试的目标;
 - 3) 评价测试过程是否标识了要执行的测试,是否描述了每个安全功能的测试概况(这些概况包括对其他测试结果的顺序依赖性);
 - 4) 评价期望的测试结果是否表明测试成功后的预期输出;
 - 5) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的五方面。开发者提供的内容应完整。

7.1.3.3.2 覆盖分析

- a) 评价内容:见 GB/T 20278—2006 中 9.1.3.2 的内容;
- b) 测试评价方法:评价者应审查开发者提供的测试覆盖分析结果,是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的;
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,开发者提供的测试文档中所标识的测试与安全功能设计中所描述的安全功能应对应。

7.1.3.4 指导性文档

7.1.3.4.1 管理员指南

- a) 评价内容:见 GB/T 20278—2006 中 9.1.4.1 的内容。
- b) 测试评价方法:
 - 1) 评价者应审查开发者是否提供了供系统管理员使用的管理员指南,并且此管理员指南是否包括如下内容:
 - 网络脆弱性扫描产品可以使用的管理功能和接口;
 - 怎样安全地管理网络脆弱性扫描产品;
 - 在安全处理环境中应进行控制的功能和权限;
 - 所有对与网络脆弱性扫描产品的安全操作有关的用户行为的假设;
 - 所有受管理员控制的安全参数,如果可能,应指明安全值;
 - 每一种与管理功能有关的安全相关事件,包括对安全功能所控制的实体的安全特性进行的改变;
 - 所有与系统管理员有关的 IT 环境的安全要求。
 - 2) 评价者应确认管理员指南是否与为评价而提供的其他所有文件保持一致。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南应完整。

7.1.3.4.2 用户指南

- a) 评价内容:见 GB/T 20278—2006 中 9.1.4.2 的内容。
- b) 测试评价方法:
 - 1) 评价者应审查开发者是否提供了供系统用户使用的用户指南,并且此用户指南是否包括如下内容:
 - 网络脆弱性扫描产品的非管理用户可使用的安全功能和接口;

- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的五方面。开发者提供的用户指南应完整,并与为评价而提供的其他所有文件保持一致。

7.1.3.5 交付与运行

- a) 评价内容:见 GB/T 20278—2006 中 9.1.5 的内容。
- b) 测试评价方法:评价者应审查开发者是否提供了文档说明网络脆弱性扫描产品的安装、生成和启动的过程。用户能够通过此文档了解安装、生成、启动过程。上述过程中不应向非产品使用者提供网络拓扑信息。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断。

7.1.3.6 生命周期支持

- a) 评价内容:见 GB/T 20278—2006 中 9.1.6 的内容。
- b) 测试评价方法:评价者应审查开发者所提供的信息是否满足如下要求。

1) 开发过程的安全管理:开发过程的出入口控制制度和记录,开发环境的温室度要求和记录,开发环境的防火防盗措施和国家有关部门的许可文件,开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料;

2) 开发环境的安全管理:开发地点的出入口控制制度和记录,开发环境的温室度要求和记录,开发环境的防火防盗措施和国家有关部门的许可文件,开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料;

3) 开发设备的安全管理:开发设备的安全管理制度,包括开发主机使用管理和记录,设备的购置、修理、处置的制度和记录,上网管理,计算机病毒管理和记录等;

4) 开发过程和成果的安全管理:对产品代码、文档、样机进行受控管理的制度和记录,若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料。

- 档、产品版本发行说明及 7.1.1.2.1 的扫描结果,逐一手工查对;
- 2) 确认脆弱性描述是否与通用的脆弱性描述方法兼容;
 - 3) 是否针对不同的操作系统类型提出了有针对性的脆弱性修补方法,并确认其有效性;
 - 4) 重新启动图 1 中网络脆弱性扫描产品 A 和 B 进行扫描,比对网络脆弱性扫描产品两次扫描结果,确认是否经过第一次扫描之后,进行了部分脆弱性修复。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,应符合:
- 1) 脆弱性描述与通用的脆弱性描述方法兼容;
 - 2) 针对不同操作系统的确提出了有针对性的有效的修补方法;
 - 3) 部分脆弱性得到修补。

7.2.2.3 智能化

- a) 评价内容:见 GB/T 20278—2006 中 7.7.3 的内容。
- b) 测试评价方法:
- 1) 查看网络脆弱性扫描产品版本发行说明、安装手册、用户手册、管理员手册、配置管理文档、测试文档、高层设计文档、低层设计文档等;
 - 2) 启动图 1 网络脆弱性扫描产品 A 和 B,进行扫描操作;
 - 3) 改变图 1 测试环境某些网络或者系统设置,模拟设置漏洞,再次启动图 1 网络脆弱性扫描产品 A 和 B,进行扫描操作,观察两次扫描结果的变化。
- c) 测试评价结果:记录测试结果并对该结果是否符合测试评价方法要求作出判断,网络脆弱性扫描产品应在使用上部分实现智能化,包括:
- 1) 自动处理结果,并将新出现的危险情况通知管理员;
 - 2) 自动判断目标属性,进行相应扫描。

7.2.2.4 互动接口

- a) 评价内容:见 GB/T 20278—2006 中 7.7.4.1 的内容。
- b) 测试评价方法:
- 1) 查看网络脆弱性扫描产品版本发行说明、安装手册、用户手册、管理员手册、配置管理文档、测试文档、高层设计文档、低层设计文档等;
 - 2) 查询厂商,索要样板程序;
 - 3) 编译并运行样板程序,查看运行结果。

7.2.2.6 与防火墙产品的互动

- a) 评价内容:见 GB/T 20278—2006 中 7.7.4.3 的内容。
- b) 测试评价方法:
 - 1) 根据网络脆弱性扫描产品版本发行说明、管理员手册、配置管理文档、测试文档、高层设计文档、低层设计文档等,检查产品软件安装目录;
 - 2) 在测试环境中,对防火墙产品进行渗透测试。

- 2) 文档应描述配置管理系统是如何跟踪这些配置项的；
 - 3) 文档还应提供足够的信息证明达到所有要求。
- c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者测试和审查内容至少包括测试评价方法中的三方面。

7.2.3.2 安全功能开发过程

7.2.3.2.1 功能设计

- a) 评价内容：见 GB/T 20278—2006 中 9.2.2.1 的内容。
- b) 测试评价方法：
 - 1) 评价者应审查开发者所提供的信息是否满足如下要求：
 - 功能设计应当使用非形式化风格来描述网络脆弱性扫描产品安全功能与其外部接口；
 - 功能设计应当是内在一致的；
 - 功能设计应当描述使用所有外部网络脆弱性扫描产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节；
 - 功能设计应当完整地表示网络脆弱性扫描产品安全功能。
 - 2) 评价者应确认功能设计是否是网络脆弱性扫描产品安全功能要求的精确和完整的示例。
- c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的内容应精确和完整。

7.2.3.2.2 高层设计

- a) 评价内容：见 GB/T 20278—2006 中 9.2.2.2 的内容。
- b) 测试评价方法：

评价者应审查开发者是否提供网络脆弱性扫描产品高层设计，所提供的信息是否满足如下要求：

 - 1) 高层设计应采用非形式化的表示；
 - 2) 高层设计应当是内在一致的；
 - 3) 网络脆弱性扫描产品高层设计应当描述每一个网络脆弱性扫描产品安全功能子系统所提供的安全功能，提供了适当的体系结构来实现网络脆弱性扫描产品安全功能要求；
 - 4) 网络脆弱性扫描产品的高层设计应当以子系统的观点来描述网络脆弱性扫描产品安全功能的结构，定义所有子系统之间的相互关系，并把这些相互关系适当地作为数据流、控制流等的外部接口来表示；
 - 5) 高层设计应当标识网络脆弱性扫描产品安全功能要求的任何基础性的硬件、固件和/或软件，并且通过支持这些硬件、固件或软件所实现的保护机制，来提供网络脆弱性扫描产品安全功能表示。

- c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者审查内容至少包括测试评价方法中的五个方面。开发者提供的高层设计内容应精确和完整。

7.2.3.2.3 低层设计

- a) 评价内容：见 GB/T 20278—2006 中 9.2.2.3 的内容。
- b) 测试评价方法：评价者应审查开发者所提供的网络脆弱性扫描产品安全功能的低层设计是否满足如下要求：
 - 1) 低层设计的表示应当是非形式化的；
 - 2) 低层设计应当是内在一致的；
 - 3) 低层设计应当以模块术语描述网络脆弱性扫描产品安全功能；
 - 4) 低层设计应当描述每一个模块的目的；

- 5) 低层设计应当以所提供的安全功能性和对其他模块的依赖性术语定义模块间的相互关系;
 - 6) 低层设计应当描述如何提供每一个网络脆弱性扫描产品安全策略强化功能;
 - 7) 低层设计应当标识网络脆弱性扫描产品安全功能模块的所有接口;
 - 8) 低层设计应当标识网络脆弱性扫描产品安全功能模块的哪些接口是外部可见的;
 - 9) 低层设计应当描述网络脆弱性扫描产品安全功能模块所有接口的目的与方法,适当时,应提供影响、例外情况和错误信息的细节;
 - 10) 低层设计应当描述如何将网络脆弱性扫描产品分离成网络脆弱性扫描产品安全策略加强模块和其他模块。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的十个方面。开发者提供的低层设计内容应精确和完整。

7.2.3.2.4 表示对应性

- a) 评价内容:见 GB/T 20278—2006 中 9.2.2.4 的内容。
- b) 测试评价方法:评价者应审查开发者是否在网络脆弱性扫描产品安全功能表示的所有相邻对之间提供对应性分析。其中,网络脆弱性扫描产品各种安全功能表示(如网络脆弱性扫描产品功能设计、高层设计、低层设计、实现表示)之间的对应性是所提供的抽象网络脆弱性扫描产品安全功能表示要求的精确而完整的子集。网络脆弱性扫描产品安全功能在功能设计中进行细

化,并且较为抽象的网络脆弱性扫描产品安全功能表示的所有相关安全功能部分,在较具体的网络脆弱性扫描产品安全功能表示中进行细化。

- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括功能设计、高层设计、底层设计、实现表示这四项。开发者提供的内容应精确和完整,并互相对应。

7.2.3.3 测试

7.2.3.3.1 功能测试

评价内容:见 GB/T 20278—2006 中 9.2.3.1 的内容。

盖所有安全功能。

7.2.3.3.3 深度

- a) 评价内容:见 GB/T 20278—2006 中 9.2.3.3 的内容。
- b) 测试评价方法:
 - 1) 评价开发者是否提供测试深度分析;
 - 2) 评价开发者提供的测试深度分析,若能说明测试文档中所标识的对安全功能的测试,就表明该安全功能和高层设计是一致的。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者测试和审查与安全功能相对应的测试,这些测试应能正确保证测试出的安全功能符合高层设计的要求。

7.2.3.3.4 独立性测试

- a) 评价内容:见 GB/T 20278—2006 中 9.2.3.4 的内容。
- b) 测试评价方法:评价者应审查开发者是否提供了网络脆弱性扫描产品经过独立的第三方测试并通过的证据。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,开发者应提供正确的第三方测试证据。

7.2.3.4 指导性文档

7.2.3.4.1 管理员指南

- a) 评价内容:见 GB/T 20278—2006 中 9.2.4.1 的内容。
- b) 测试评价方法:
 - 1) 评价者应审查开发者是否提供了供系统管理员使用的管理员指南,并且此管理员指南是否包括如下内容:
 - 网络脆弱性扫描产品可以使用的管理功能和接口;
 - 怎样安全地管理网络脆弱性扫描产品;
 - 在安全处理环境中应进行控制的功能和权限;
 - 所有对与网络脆弱性扫描产品的安全操作有关的用户行为的假设;
 - 所有受管理员控制的安全参数,如果可能,应指明安全值;
 - 每一种与管理功能有关的安全相关事件,包括对安全功能所控制的实体的安全特性进行的改变;
 - 所有与系统管理员有关的 IT 环境的安全要求。
 - 2) 评价者应确认管理员指南是否与为评价而提供的其他所有文件保持一致。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南应完整。

7.2.3.4.2 用户指南

- a) 评价内容:见 GB/T 20278—2006 中 9.2.4.2 的内容。
- b) 测试评价方法:
 - 1) 评价者应审查开发者是否提供了供系统用户使用的用户指南,并且此用户指南是否包括如下内容:

网络脆弱性扫描产品的非管理用户可用的安全功能和接口

2) 评价者应确认用户指南是否与为评价而提供的其他所有文件保持一致。

- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的五方面。开发者提供的用户指南应完整,并与为评价而提供的其他所有文件保持一致。

7.2.3.5 脆弱性评定

7.2.3.5.1 指南检查

- a) 评价内容:见 GB/T 20278—2006 中 9.2.5.1 的内容。

b) 测试评价方法:

1) 评价者应确认开发提供了指南性文档。

2) 评价者应审查开发者提供的指南性文档,是否满足了以下要求:

——评价指南性文档,是否确定了对网络脆弱性扫描产品的所有可能的操作方式(包括失败和操作失误后的操作),是否确定了它们的后果,以及是否确定了对于保持安全操作的意义;

——评价指南性文档,是否列出了所有可能存在的漏洞以及所有可能的人员操作(包括员

部程序的、物理的或人员的控制)的要求;

——评价指南性文档是否完整、清晰、一致、合理。

- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,开发者提供的评价指南性文档应完整。

7.2.3.5.2 脆弱性分析

- a) 评价内容:见 GB/T 20278—2006 中 9.2.5.2 的内容。

b) 测试评价方法:

1) 评价开发者提供的脆弱性分析文档,是否从用户可能破坏安全策略的明显途径出发,对网络脆弱性扫描产品的各种功能进行了分析;

2) 对被确定的脆弱性,评价开发者是否明确记录了采取的措施;

3) 对每一条脆弱性,评价是否有证据显示在使用网络脆弱性扫描产品的环境中该脆弱性不能被利用;

4) 评价所提供的文档,是否证明经过标记脆弱性的网络脆弱性扫描产品可以抵御明显的容

- b) 测试评价方法:评价者应审查开发者是否提供了文档说明网络脆弱性扫描产品的安装、生成和启动的过程。用户能够通过此文档了解安装、生成、启动过程。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断。

7.2.3.7 生命周期支持

7.2.3.7.1 开发安全

- a) 评价内容:见 GB/T 20278—2006 中 9.2.7.1 的内容。
- b) 测试评价方法:评价者应审查开发者所提供的信息是否满足如下要求:
 - 1) 开发人员的安全管理:开发人员的安全规章制度,开发人员的安全教育培训制度和记录;
 - 2) 开发环境的安全管理:开发地点的出入口控制制度和记录,开发环境的温室度要求和记录,开发环境的防火防盗措施和国家有关部门的许可文件,开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料;
 - 3) 开发设备的安全管理:开发设备的安全管理制度,包括开发主机使用管理和记录,设备的购置、修理、处置的制度和记录,上网管理,计算机病毒管理和记录等;
 - 4) 开发过程和成果的安全管理:对产品代码、文档、样机进行受控管理的制度和记录,若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查内容至少包括测试评价方法中的四方面。开发者提供文档应完整。

7.2.3.7.2 生命周期模型

- a) 评价内容:见 GB/T 20278—2006 中 9.2.7.2 的内容。
- b) 测试评价方法:评价者应审查开发者所提供的生命周期定义文件中是否包含以下内容:
 - 1) 开发者定义的生命周期模型,要求开发者应建立用于开发和维护网络脆弱性扫描产品的生命周期模型。该模型应对网络脆弱性扫描产品开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护网络脆弱性扫描产品的模型。
 - 2) 标准生命周期模型,要求开发者应建立标准化的、用于开发和维护网络脆弱性扫描产品的生命周期模型。该模型应对网络脆弱性扫描产品开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护网络脆弱性扫描产品的模型,解释选择该模型的原因,解释如何用该模型来开发和维护网络脆弱性扫描产品,以及阐明与标准化的生命周期模型的相符性。
 - 3) 可测量的生命周期模型,要求开发者应建立标准化的、可测量的、用于开发和维护网络脆

- 工具的选项,并且开发工具文档应明确定义实现中每个语句的含义,以及明确定义所有基于实现的选项的含义。
- 2) 遵照实现标准—应用部分,除明确定义的开发工具的要求外,要求开发者应描述所应用部分的实现标准。
 - 3) 遵照实现标准—所有部分,除遵照实现标准—应用部分的要求外,要求开发者应描述网络脆弱性扫描产品所有部分的实现标准。
- c) 测试评价结果:记录审查结果并对该结果是否符合测试评价方法要求作出判断,评价者审查文档的可行性,内容至少包括测试评价方法中的三方面。

附录 A

(规范性附录)

产品厂商向测试单位提供的测试证据

A.1 基本型

- a) 产品本身(至少提供两套产品);
- b) 产品版本发行说明;
- c) 安装手册;
- d) 用户手册;
- e) 管理员手册;
- f) 配置管理文档;
- g) 测试文档;
- h) 高层设计文档;
- i) 其他必要的证据。

A.2 增强型

除基本型所需要的产品和资料外,还应提供下列资料:

- a) 底层设计文档;
- b) 根据测试单位要求,提供部分接口源代码或样板程序;
- c) 其他必要的证据。

参 考 文 献

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构
(idt ISO 7498-2:1989)

GB/T 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般
模型(idt ISO/IEC 15408-1:1999)

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要
求(idt ISO/IEC 15408-2:1999)

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要
求(idt ISO/IEC 15408-3:1999)

中华人民共和国
国家标准
信息安全技术
网络脆弱性扫描产品测试评价方法
GB/T 20280—2006

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 1.75 字数 42 千字
2006年10月第一版 2006年10月第一次印刷

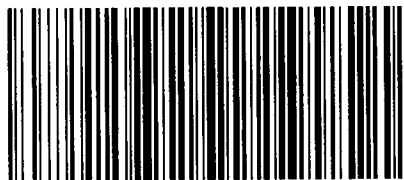
*

书号: 155066·1-28010 定价 15.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533



GB/T 20280-2006