ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20280—2006

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

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

4.1 符号和缩略语

CGI	公共网关接口	Common Gateway Interface
CVE	通用脆弱性知识库	Common Vulnerabilities and Exposures
DNS	域名系统	Domain Name System
DOS	拒绝服务	Denial Of Service
FTP	文件传输协议	File Transfer Protocol
IDS	入侵检测系统	Intrusion Detection System
IP	网际协议	Internet Protocol
NETBIOS	网络基本输入输出系统	NETwork Basic Input Output System
NFS	网络文件系统	Network File System
POP	邮局协议	Post Office Protocol
RPC	远程过程调用	Remote Procedure Call
SMB	服务器消息块协议	Server Message Block Protocol
SNMP	简单网络管理协议	Simple Network Management Protocol
TCP	传输控制协议	Transport Control Protocol
UDP	用户数据报协议	User Datagram Protocol

4.2 记法约定

a) 选择:用于从对某一功能要求的陈述中突出一个或多个选项,用*带下划线的斜体字*表示。

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：

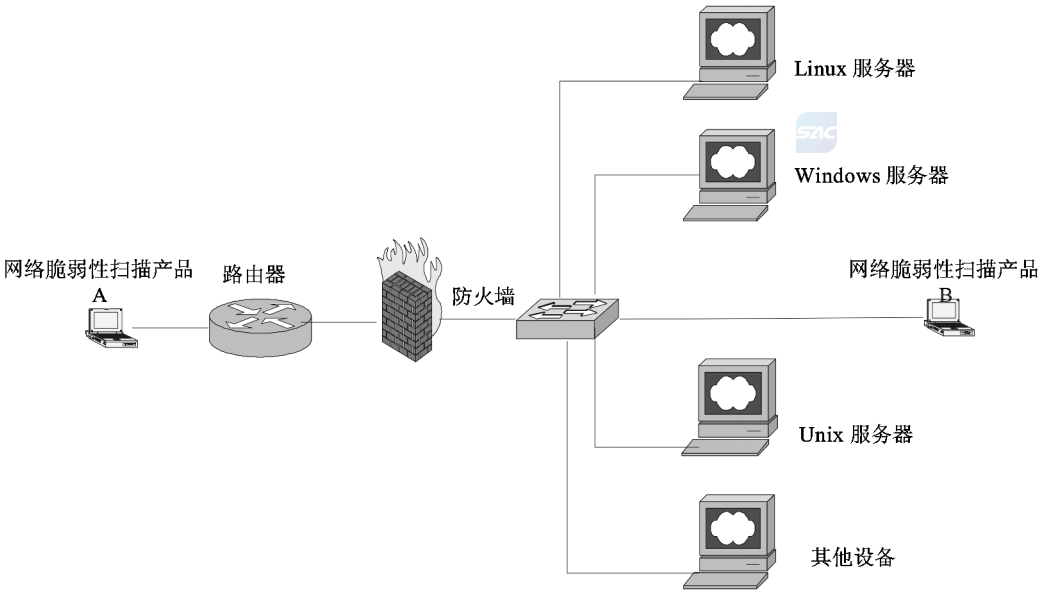

图 1 网络脆弱性扫描产品测试环境拓扑图

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、交换机等等
注：根据情况，“其他设备”的数目和种类可以调整。	

被扫描主机应至少运行如下服务：HTTP、FTP、POP3、SMTP、SQL SERVER、ORACLE、UNIX 和 LINUX 服务器应运行 NFS 服务。

服务器应运行常见木马。

服务器宜运行其他具有脆弱性的服务，宜选择脆弱性较常见和造成危害较严重的服务。

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

7.1.1.1.1 身份鉴别

a) 评价内容:见 GB/T 20278—2006 中 7.2.1 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

a) 评价内容:见 GB/T 20278—2006 中 7.2.2 的内容;

b) 测试评价方法:根据网络脆弱性扫描产品版本发行说明、用户手册、高层设计文档、测试文档等,启动图 1 中网络脆弱性扫描产品 A 和 B,进行管理配置、启动扫描等操作;

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,如网络脆弱性扫描产品是否能够限制产品可扫描的具体 IP 地址。

7.1.1.1.3 敏感信息保护

a) 评价内容:见 GB/T 20278—2006 中 7.2.3 的内容;

b) 测试评价方法根据网络脆弱性扫描产品版本发行说明、用户手册、高层设计文档、测试文档等,启动图 1 中网络脆弱性扫描产品 A 和 B,进行管理配置、启动扫描等操作;

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,如是否对策略信息进行加密、敏感信息规避等。

7.1.1.1.4 软件使用记录

a) 评价内容:见 GB/T 20278—2006 中 7.2.4 的内容。

b) 测试评价方法:根据网络脆弱性扫描产品版本发行说明、用户手册、管理员手册等,启动图 1 中网络脆弱性扫描产品 A 和 B,进行下列操作,观察日志变化:

1) 管理员登录;

2) 扫描操作过程;

3) 扫描结果分析处理;

4) 产品升级;

5) 其他使用。

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。

7.1.1.1.5 扫描数据包标记

a) 评价内容:见 GB/T 20278—2006 中 7.2.5 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,启动图 1 中网络脆弱性扫描产品 A 和 B,执行扫描功能;

2) 通过抓包工具(例如:Tcpdump 等)捕获网络脆弱性扫描产品扫描数据包,并对捕获数据进行分析。

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。

7.1.1.1.6 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，启动图 1 中网络脆弱性扫描产品 A 和 B，执行扫描功能；

2) 直接利用数据库工具查证扫描结果；

3) 对扫描结果进行导入、导出及删除操作。

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。

7.1.1.2 安全功能要求

7.1.1.2.1 脆弱性扫描

a) 评价内容：见 GB/T 20278—2006 中 7.3.1 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、用户手册、管理员手册、配置管理文档、测试文档、高层设计文档等，确定测试对象（产品、扫描对象等），按照 GB/T 20278—2006 中 7.3.1 及其注解给出的细节，分别编写测试用例。

2) 对照测试用例，*目标主机分别安装并启动相应的应用程序。*启动图 1 中网络脆弱性扫描产品 A 和 B，分别对被扫描机器进行扫描，并根据扫描结果，手工对比网络脆弱性扫描产品是否能够正确的发现危险或不合理的配置等安全问题，并能提出相应的安全性建议。

3) 检查扫描结果中详细描述是否准确。

4) 按产品提供的安全性建议进行脆弱性修复后，再次进行测试，检查产品是否报告相应的脆弱性。

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。

7.1.1.2.2 网络旁路检查

a) 评价内容：见 GB/T 20278—2006 中 7.3.2 的内容。

b) 测试评价方法：

1) 在被扫描的网络环境中，配置一个拨号上网或代理服务器或其他网络旁路服务；

2) 根据管理员手册、用户手册等，启动图 1 中网络脆弱性扫描产品 B，查看扫描结果是否能够发现网络旁路服务。

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。

7.1.1.2.3 信息获取

a) 评价内容：见 GB/T 20278—2006 中 7.3.3 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，对以下条目进行扫描：

——操作系统，包括类型、版本号等；

——TCP/IP 服务旗标；

——系统硬件信息；

——系统软件配置信息；

——其他网络配置信息；

——共享目录信息；

——系统运行状态信息等。

2) 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。

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，根据用户手册检查产品是否具备升级更新能力；

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：升级操作方便、自动化，能够进行手工升级和漏洞库增加操作。

7.1.1.4 使用要求

7.1.1.4.1 安装与操作控制

a) 评价内容：见 GB/T 20278—2006 中 7.5 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、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标明了该系统的误报率，并指明所使用的测试方法、测试工具、测试环境和测试步骤。

7.1.2.5 漏报率

a) 评价内容：见 GB/T 20278—2006 中 8.5 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、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给用户的网络脆弱性扫描产品样本完全对应且惟一;

3) 配置项,要求配置项应有惟一的标识,从而对网络脆弱性扫描产品的组成有更清楚的描述。

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:开发者应提供惟一版本号、授权标识和配置项。

7.1.3.2 安全功能开发过程

7.1.3.2.1 功能设计

a) 评价内容:见 GB/T 20278—2006 中 9.1.2.1 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) 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;

2) 功能设计应当是内在一致的;

3) 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;

4) 功能设计应当完整地表示网络脆弱性扫描产品安全功能。

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。

7.1.3.2.2 表示对应性

a) 评价内容:见 GB/T 20278—2006 中 9.1.2.2 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物理网络脆弱性扫描产品安全功能表示要求的精确而完整的示例。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。

7.1.3.3 测试

7.1.3.3.1 功能测试

a) 评价内容:见 GB/T 20278—2006 中 9.1.3.1 的内容。

b) 测试评价方法:

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；

——网络脆弱性扫描产品提供给用户的安全功能和接口的用法；

——用户可获取但应受安全处理环境控制的所有功能和权限；

——网络脆弱性扫描产品安全操作中用户所应承担的职责；

——与用户有关的 IT 环境的所有安全要求。

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。

7.1.3.5 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 增强型

7.2.1 基本功能及性能

按 7.1.1 及 7.1.2 的测试内容进行测试评价。

7.2.2 增强功能

7.2.2.1 身份鉴别

a) 评价内容：见 GB/T 20278—2006 中 7.7.1 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；

3) *要求产品厂商提供更换身份鉴别方式的接口，根据低层设计文档实际验证产品更换身份鉴别方式的能力。*

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) 网络脆弱性扫描产品只有授权管理员才能使用网络脆弱性扫描产品的完整功能。授权管理员、普通管理员采取了身份鉴别措施(例如：用户名和口令)。

2) *网络脆弱性产品提供了可以根据不同用户的需求更换身份鉴别方式的接口。*

7.2.2.2 脆弱性修补

a) 评价内容：见 GB/T 20278—2006 中 7.7.2 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、低层设计文*

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。

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提供或采用一个标准的、开放的接口。遵照该接口规范，可编写相应的程序模块，达到与网络安全漏洞扫描产品进行互动的目的。

7.2.2.5 与 IDS 产品的互动

a） 评价内容：见 GB/T 20278—2006 中 7.7.4.2 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） 在测试环境中安装一个符合通用脆弱性描述的 IDS 环境；

3） 分别启动 IDS 和图 1 中网络脆弱性扫描产品 A 和 B，手工检查比对脆弱性特征描述；

4） 编写测试用例，利用网络脆弱性扫描产品提供的接口及网络脆弱性扫描产品厂商提供的测试程序，启动图 1 中网络脆弱性扫描产品及 IDS 进行测试。

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：产品能够接收 IDS 发出的对某一目标进行指定漏洞扫描请求，并能启动扫描工作。脆弱性描述符合通用脆弱性描述方法（例如：CVE 或 CNCVE 等）。

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) 在图 1 环境中构造一个包括有木马在内的测试环境；

3) 编写测试用例，利用网络脆弱性扫描产品提供的接口及网络脆弱性扫描产品厂商提供的测试程序，启动图 1 中网络脆弱性扫描产品及防火墙进行测试。

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，符合网络脆弱性扫描产品并能将包括木马及绑定的端口信息在内漏洞信息发送给防火墙，使防火墙动态调整自身的过滤规则，封堵相应的端口。

7.2.2.7 与其他应用程序之间的互动

a) 评价内容：见 GB/T 20278—2006 中 7.7.4.4 的内容；

b) 测试评价方法：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，指定并安装某种应用程序（例如：邮件系统等），适当的对图 1 中网络脆弱性扫描产品进行产品配置；

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：在发现危险漏洞以上级别漏洞时，指定应用程序对脆弱性作出响应（例如：邮件通知等）。

7.2.3 安全保证要求

7.2.3.1 配置管理

7.2.3.1.1 授权机制

a) 评价内容：见 GB/T 20278—2006 中 9.2.1.1 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) 开发者应使用配置管理系统并提供配置管理文档，以及为网络脆弱性扫描产品的不同版本提供惟一的标识。

2) 配置管理系统应对所有的配置项作出惟一的标识，并保证只有经过授权才能修改配置项。

3) 配置管理文档应包括配置清单、配置管理计划。配置清单用来描述组成网络脆弱性扫描产品的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

4) 配置管理文档还应描述对配置项给出惟一标识的方法，并提供所有的配置项得到有效地维护的证据。

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，应符合：评价者审查内容至少包括测试评价方法中的四方面。开发者提供的配置管理内容应完整。

7.2.3.1.2 配置管理范围

a) 评价内容：见 GB/T 20278—2006 中 9.2.1.2 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：

网络脆弱性扫描产品配置管理范围，要求将网络脆弱性扫描产品的实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：

1) 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；

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示例。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

a) 评价内容：见 GB/T 20278—2006 中 9.2.3.1 的内容。

b) 测试评价方法：

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。

7.2.3.3.2 覆盖分析

a) 评价内容：见 GB/T 20278—2006 中 9.2.3.2 的内容。

b) 测试评价方法：

1) 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；

2) 评价测试文档中所标识的测试，是否完整。

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，并且标识的测试应覆

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使用的安全功能和接口；

——网络脆弱性扫描产品提供给用户的安全功能和接口的用法；

——用户可获取但应受安全处理环境控制的所有功能和权限；

——网络脆弱性扫描产品安全操作中用户所应承担的职责；

——与用户有关的 IT 环境的所有安全要求。

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，是否列出了所有目标环境的假设以及所有外部安全措施（包括外部程序的、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，是否证明经过标识脆弱性的网络脆弱性扫描产品可以抵御明显的穿透性攻击。

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，*开发者提供的脆弱性分析文档应完整。*

7.2.3.6 交付与运行

7.2.3.6.1 交付

a） 评价内容：见 GB/T 20278—2006 中 9.2.6.1 的内容。

b） 测试评价方法：

1） 评价者应审查开发者是否使用一定的交付程序交付网络脆弱性扫描产品；

2） 使用文档描述交付过程，并且评价者应审查开发者交付的文档是否包含以下内容：在给用户方交付网络脆弱性扫描产品的各版本时，为维护安全所必需的所有程序；

3） 评价者应审查上述过程中是否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，*开发者应提供完整的文档描述所有交付的过程（文档和程序交付）。整个过程不应向非产品使用者提供网络拓扑信息。*

7.2.3.6.2 安装生成

a） 评价内容：见 GB/T 20278—2006 中 9.2.6.2 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。*

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弱性扫描产品的生命周期模型，并用此模型来衡量网络脆弱性扫描产品的开发。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，包括针对该模型衡量网络脆弱性扫描产品开发所需的算术参数和/或度量的细节。生命周期定义文档应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，阐明与标准化的可测量的生命周期模型的相符性，以及提供利用标准化的可测量的生命周期模型来进行网络脆弱性扫描产品开发的测量结果。*

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，评价者审查三模型的可行性，内容至少包括测试评价方法中的三方面。

7.2.3.7.3 工具和技术

a) 评价内容：见 GB/T 20278—2006 中 9.2.7.3 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) *明确定义的开发工具，要求开发者应标识用于开发网络脆弱性扫描产品的工具，并且所有用于实现的开发工具都必须有明确定义。开发者应文档化已选择的依赖实现的开发*

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
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.spc.net.cn
电话:(010)51299090、68522006
2006 年 10 月第一版
*
书号:155066·1-28010

GB/T 20280-2006