ICS 35.040
L80

中华人民共和国国家标准

GB/T 20278—2006

信息安全技术
网络脆弱性扫描产品技术要求

Information security technology-
Technique requirement for network vulnerability scanners

2006-05-13 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

前鋘言

（略）

引鎏言

网络脆弱性扫描是检查网络安全性能的一种重要技术手段，其原理是对目标网络系统及设备可能存在的已知网络脆弱性进行逐项检测，确定存在的安全隐患及危险程度，并提出解决建议。

信息安全技术
网络脆弱性扫描产品技术要求

1 范围

本标准规定了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技术要求，提出网络脆弱性扫描产品实现的安全目标及环境，给出产品基本功能、增强功能和安全保证要求。

本标准适用于通过网络对系统和设备进行脆弱性扫描的安全产品的研制、生产和认证。

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部分的条款。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）或者修订版均不适合于本标准，但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。凡是不注日期的引文，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）

3 术语和定义

GB/T 5271.8-2001 确立的以及下列术语和定义适用于本标准。

3.1

扫描　scan

使用脆弱性扫描产品进行探测，找到网络中的主机系统存在的安全隐患的过程。

3.2

威胁　threat

可能对网络系统和设备或网络所有者造成损害的事故的潜在原因。

3.3

脆弱性　vulnerability

网络系统和设备中能被利用并造成危害的弱点。

3.4

宿主机　local host

运行网络脆弱性扫描产品的计算机。

3.5

目标主机　target host

网络脆弱性扫描产品对其进行风险分析的计算机。

3.6

网络脆弱性扫描　network vulnerability scan

通过网络远程检测目标网络系统安全隐患的探测过程，它对网络系统和设备进行安全脆弱性检测和分析，从而发现可能被入侵者利用的漏洞，并采取一定的防范和补救措施。

3.7

网络脆弱性扫描产品　network vulnerability scanner

能够完成网络脆弱性扫描功能的产品。

3.8

误报　false positives

报告了不存在的脆弱性。

3.9

漏报　false negatives

没有报告出实际存在的脆弱性。

3.10

旗标　banner

由应用程序发送的一段讯息，通常包括欢迎语、应用程序名称和版本等信息。

4　缩略语和记法约定

4.1　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

本标准对网络脆弱性扫描产品进行了分级。本标准中的规定，凡未特殊说明，均为基本型产品要求，对于增强型产品的要求，标准中将进行特殊说明或用斜体表示。

5　网络脆弱性扫描产品分级

5.1　基本型

该级的网络脆弱性扫描产品应具备7.1及9.1中规定的基本功能要求和保证要求。

5.2　增强型

该级的网络脆弱性扫描产品除满足基本型产品各项要求外，还必须符合7.7及9.2中规定的扩展功能和保证要求。

6　使用环境

宿主机与目标主机应处于连通状态，且宿主机应满足网络脆弱性扫描产品的软硬件配置要求。

7 功能要求

7.1 基本型网络脆弱性扫描产品功能组件

基本型网络脆弱性扫描产品的功能组件由表1所列项目组成。

表 1 基本型网络脆弱性扫描产品功能要求

功能分类	功能组件
自身安全要求	身份鉴别
	适用限制
	敏感信息保护
	使用记录
	扫描数据包标记
	扫描结果安全
安全功能要求	脆弱性扫描
	网络旁路检查
	信息获取
	端口和服务扫描
管理要求	管理员访问
	扫描结果分析处理
	扫描策略定制
	扫描对象的安全性
	升级能力
使用要求	安装与操作控制

7.2 自身安全要求

7.2.1 身份鉴别

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，对于授权管理员、普通管理员和审计员至少采用一种身份鉴别方式（例如：用户名和口令）对其进行身份鉴别。

7.2.2 适用限制

网络脆弱性扫描产品应提供对产品扫描范围进行限制的手段，如限制产品可扫描的具体IP地址。

7.2.3 敏感信息保护

策略定制时，一些敏感信息可能被涉及，应采取相应措施来保证敏感信息的机密性和完整性，例如对用户口令进行加密存储。

7.2.4 使用记录

对软件的以下使用应有完整的日志记录，便于审计跟踪和分析：

a) 管理员登录；
b) 扫描操作过程；
c) 扫描结果分析处理；
d) 产品升级；
e) 其他使用。

7.2.5 扫描数据包标记

网络脆弱性扫描产品扫描数据包应具备厂商自身特征，并将特征公开。

7.2.6 扫描结果安全

应采取相应措施来保证扫描结果的机密性和完整性，扫描结果应能够导入、导出及删除。

7.3 安全功能要求

7.3.1 脆弱性扫描

7.3.1.1 浏览器脆弱性

检查和浏览器安全相关的信息和配置，发现危险或不合理的配置，并提出相应的安全性建议。检查项目应包括：

a) 浏览器版本号；
b) 浏览器安全设置，包括：
   1) ActiveX 控件和插件；
   2) Cookies 设置；
   3) Java 权限设置；
   4) 脚本设置；
   5) 下载设置；
   6) 用户登录验证设置；
   7) 其他设置；
c) 其他由于操作系统或软件未升级带来的安全隐患。

7.3.1.2 邮件服务脆弱性

检查使用了POP3、SMTP等电子邮件相关协议的服务程序的安全问题，检查项目应包括：

a) 服务程序旗标、版本号；
b) 服务程序本身的脆弱性：
   1) 设计错误；
   2) 对输入缺乏合法性检查；
   3) 不能正确处理异常情况；
c) 服务器的危险或错误配置：
   1) 是否允许 EXPN 和 VRFY 命令；
   2) 是否允许邮件转发；
   3) 其他安全配置；
d) 其他由于操作系统或软件未升级带来的安全隐患。

7.3.1.3 FTP 服务脆弱性

检查使用了FTP协议的服务程序的安全问题，检查项目应包括：

a) 服务程序旗标、版本号；
b) 服务程序本身的脆弱性：
   1) 设计错误；
   2) 对输入缺乏合法性检查；
   3) 不能正确处理异常情况；
c) 服务器的危险或错误配置：
   1) 是否允许匿名登录；
   2) 是否使用了默认口令；
   3) 是否允许危险命令；
   4) 其他安全配置；
d) 其他由于操作系统或软件未升级带来的安全隐患。

7.3.1.4 Web 服务脆弱性

检查使用了HTTP协议的服务程序的安全问题，检查项目应包括：

a) 服务程序旗标、版本号；

b) 服务程序本身的脆弱性：

1）设计错误；

2）对输入缺乏合法性检查；

3）不能正确处理异常情况；

c) 服务器上运行的脚本及 CGI 程序的脆弱性；

d) 服务器的危险或错误配置：

1）文件属性错误；

2）目录属性错误；

3）其他安全配置；

e) 其他由于操作系统或软件未升级带来的安全隐患。

7.3.1.5 DNS 服务脆弱性

检查DNS服务的安全问题，检查项目应包括：

a) 服务程序旗标、版本号；

b) 服务程序本身的脆弱性:

1）设计错误；

2）对输入缺乏合法性检查；

3）不能正确处理异常情况；

c) 其他由于操作系统或软件未升级带来的安全隐患。

7.3.1.6 其他已知 TCP/IP 服务脆弱性

检查其他使用了TCP/IP协议的服务程序的安全问题，检查项目应包括：

a) 服务程序的旗标、版本号；

b) 服务程序本身的脆弱性：

1）设计错误；

2）对输入缺乏合法性检查；

3）不能正确处理异常情况；

c) 服务程序的错误配置。

7.3.1.7 RPC 服务的脆弱性

检查使用了RPC协议的服务程序的安全问题，检查是否开启了危险的RPC服务。

7.3.1.8 NIS 服务的脆弱性

检查使用了NIS协议的服务程序的安全问题，检查是否开启了危险的NIS服务。

7.3.1.9 SNMP 服务的脆弱性

SNMP服务的脆弱性包括：

a) SNMP 口令脆弱性检查；

b) 检查 SNMP 服务是否导致下列的系统敏感信息泄露：

1）TCP 端口表；

2）UDP 端口表；

3）存储设备信息；

4）服务列表；

5）共享目录；

6）进程列表；

7）路由表；
8）软件安装信息；
9）设备表；
10）网络接口设备表；
11）用户名列表；

c） 其他相关检查。

7.3.1.10 口令脆弱性

检查系统帐户口令的健壮性，检查项目应包括：

a） 系统是否使用了帐户名称经过简单变换后的口令；
b） 系统是否使用了其他易猜口令；
c） 使用字典，检查系统是否使用了易猜测的口令；
d） 有条件使用穷举法猜测口令以验证系统帐户口令的强度，例如：口令长度小于 5，且只采用英文字母或数字等。

7.3.1.11 windows 操作系统用户、组、口令、共享、注册表等等脆弱性

检查Windows操作系统特有的一些脆弱性，检查项目应包括：

a） 安全设置
1）注册表项目访问权限设置；
2）审核策略设置：
—— 审核帐号登录；
—— 审核帐号管理；
—— 审核系统事件；
—— 审核特权使用；
—— 审核目录服务访问；
—— 审核过程追踪；
—— 审核对象访问；
—— 审核登录事件；
—— 审核策略更改；
3）系统口令策略设置：
—— 检查是否允许空连接；
—— 检查“口令字长度最小值”设置；
—— 检查“口令字最长存留期”设置；
—— 检查“口令字最短存留期”设置；
—— 检查“强制密码历史”设置；
—— 账号是否能改变其口令；
—— 账号长时间未登录；
—— 账号失败的登录次数过多；
—— 账号“密码永不过期”；
—— 账号口令长期未改变；
—— 账号禁用；

b） 操作系统版本和补丁安装情况检查；
c） 其他相关检查。

7.3.1.12 木马

检查常见木马使用的默认端口是否开启，并对扫描得到的开启端口进行测试分析，对未知服务和已知木马做出警告。

7.3.1.13 NT 服务

检查Windows操作系统服务开启情况，检查项目应包括：

a) 将当前启动的NT服务列表与用户定义的“已知NT服务列表”相比较，给出“未知NT服务列表”；

b) 检查是否启动了具有一定危险性的NT服务。

7.3.1.14 NFS 服务脆弱性

检查NFS服务相关的脆弱性。

7.3.1.15 路由器、交换机脆弱性

检查路由器、交换机及其开启服务相关的脆弱性。

7.3.1.16 DOS 攻击脆弱性

使用实际攻击手法对目标服务器进行真实的攻击，以检查目标服务器对已知DOS攻击的抵御能力。

7.3.1.17 文件共享

检查使用的NETBIOS或SMB共享，发现危险的设置，检查项目应包括：

a) 重要目录被共享；

b) 共享目录可被匿名用户写入；

c) 是否使用了缺省或过于简单的共享口令；

d) SAMBA服务器软件的版本号。

7.3.1.18 数据库脆弱性

检查网络数据库相关的脆弱性，检查项目应包括：

a) 用户密码是否为空；

b) 服务器的版本号。

7.3.1.19 其他

未归于以上各门类的系统脆弱性。

7.3.2 网络旁路检查

检查目标系统网段中是否存在连通外网网络旁路，如代理服务器，拨号上网等。

7.3.3 信息获取

7.3.3.1 操作系统探测

网络脆弱性扫描产品应能对操作系统类型、版本号进行探测。

7.3.3.2 服务旗标

网络脆弱性扫描产品应能获取已开启的各项TCP/IP服务的旗标。

7.3.3.3 网络其他信息

网络脆弱性扫描产品应能对下列的信息进行探测：

a) 系统硬件信息；

b) 系统软件配置信息；

c) 系统网络配置信息；

d) 共享目录信息；

e) 系统运行状态信息。

7.3.4 端口和服务扫描

7.3.4.1 RPC 端口

获取运行的RPC服务及其所在的RPC端口信息。

7.3.4.2 TCP 端口

扫描所有TCP端口，检查其是否开启。

7.3.4.3 UDP 端口

扫描所有UDP端口，检查其是否开启。

7.3.4.4 端口协议分析

就扫描得到的已开启的TCP/UDP端口，应能判断相应端口对应的服务或使用的协议。

7.3.4.5 NT 服务

获取启动的NT服务列表。

7.4 管理要求

7.4.1 管理员访问

7.4.1.1 授权管理员

网络脆弱性扫描产品应确保只有授权管理员才能使用所有网络脆弱性扫描产品功能，包括对普通管理员的授权。

7.4.1.2 普通管理员

由授权管理员基于角色的管理给予普通管理员最低程序的许可来完成任务，即只允许普通管理员部分具有配置或使用网络脆弱性扫描产品的能力。

7.4.1.3 审计员

由授权管理员基于角色的管理给予审计员最低程序的许可来完成任务，即只允许审计员部分具有查看审计日志的能力。

7.4.2 扫描结果分析处理

a) 从扫描结果数据库形成报告，包括：
   1) 脆弱性报告，包括各脆弱点的详细信息、补救建议等，补救建议应确保其合理性和可用性；
   2) 可对目标主机扫描后的信息获取结果生成相应的报告；
   3) 脆弱性分析报告，包括：
      —— 目标的风险等级评估报告；将扫描脆弱点按严重程度分级，并明确标出；
      —— 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。
b) 扫描结果写入数据库；
c) 扫描结果可导入、导出和删除；
d) 可按照不同的分类定制报告；
e) 报告可输出成标准格式，至少包括 HTML、RTF、PDF 等格式；
f) 提供全面灵活的扫描结果数据库浏览功能。

7.4.3 扫描策略定制

a) 能够使用目标的已知帐号和口令对目标进行更有效的扫描；
b) 定制扫描项目及属性，形成计划任务等策略；
c) 具有完整的日志及审计功能；
d) 提供方便的定制策略的方法（如：定时启动等）。

7.4.4 扫描对象的安全性

7.4.4.1 报警功能

在开始扫描前宿主机应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，以避免网络脆弱性扫描产品被入侵者用作网络入侵工具。

7.4.4.2 对目标系统所在网络性能的影响

扫描应不影响网络的正常工作，允许网络性能的少量降低。

7.4.4.3 对目标系统的影响

网络脆弱性扫描产品应在脆弱性探测的强度和深度上提供一定的控制手段，以避免对被扫描系统造成严重危害。扫描宜避免影响目标系统的正常工作，宜避免使用攻击方法进行测试；在必要时使用DOS等攻击测试手段，测试开始前要给用户明确的提示，说明该类测试的危害并要求用户进行确认。

7.4.5 升级能力

a) 网络脆弱性扫描产品应能根据技术的发展进行升级和更新。产品体系结构的设计应有利于产品的升级操作；

b) 对网络脆弱性扫描产品的升级操作应遵循方便性、及时性和自动化原则。

c) 对网络安全漏洞扫描产品至少可进行手动升级操作，更新漏洞特征库。

7.5 安装与操作控制

a) 安装与操作时应确保对网络脆弱性扫描产品的安装、管理、操作都是安全可控的；

b) 网络脆弱性扫描产品扫描过程应可随时停止，并且能断点保存，随时恢复；

c) 网络脆弱性扫描产品扫描过程中，应提供键盘锁定功能和屏幕保护功能。

7.6 增强型网络脆弱性扫描产品功能组件

增强型网络脆弱性扫描产品的功能要求由表2所列项目组成，其中标记为*斜体*的项目为增强型网络脆弱性扫描产品所应满足的扩展技术要求。

表 2 增强型网络脆弱性扫描产品功能要求

功能分类	功能组件
自身安全要求	*身份鉴别*
	适用限制
	敏感信息保护
	使用记录
安全功能要求	脆弱性扫描
	网络旁路检查
	信息获取
	端口和服务扫描
	脆弱性修补
性能要求	速度
	稳定性和容错性
管理要求	管理员访问
	扫描结果分析处理
	扫描策略定制
	扫描对象的安全性
	升级能力
使用要求	安装与操作控制
	智能化
互动性要求	*互动接口*
	与IDS产品的互动
	与防火墙产品的互动
	与其他应用程序之间的互动

7.7 增强型网络脆弱性扫描产品扩展功能要求

7.7.1 身份鉴别

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，对于授权管理员、普通管理员至少采用一种身份鉴别方式（例如：用户名和口令）对其进行身份鉴别。*且底层设计上应留有接口，方便更换身份鉴别方式。*

7.7.2 脆弱性修补

增强型网络脆弱性扫描产品应能对发现的脆弱性进行修补，脆弱性描述应与通用的脆弱性描述（例如:CVE、CNCVE等）兼容，脆弱性修补应满足下列要求：

a) 应针对不同的操作系统类型提出针对性的脆弱性修补方法；

b) 提供的脆弱性修补方法应确保有效；

7.7.3 智能化

增强型网络脆弱性扫描产品应能在使用上部分实现智能化，包括：

a) 自动处理结果，并将新出现的危险情况通知管理员；

b) 自动判断目标属性，进行相应扫描。

7.7.4 互动性要求

7.7.4.1 互动接口

网络脆弱性扫描产品应提供或采用一个标准的、开放的接口。遵照该接口规范，可为其他类型安全产品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。

7.7.4.2 与 IDS 产品的互动

增强型网络脆弱性扫描产品应满足以下要求：

a) 与符合通用脆弱性描述（例如:CVE、CNCVE 等）的 IDS 产品脆弱性特征描述方法一致；

b) 能接收 IDS 产品发出的指定漏洞扫描请求，并进行相应扫描。

7.7.4.3 与防火墙产品的互动

增强型网络脆弱性扫描产品应能与防火墙产品共享扫描信息，以增强网络的防护能力，例如将扫描得到的木马及其绑定的端口信息通知防火墙，使防火墙动态调整自身的过滤规则，封堵相应的端口。

7.7.4.4 与其他应用程序之间的互动

增强型网络脆弱性扫描产品应能在发现严重脆弱性（例如：病毒等）时操作其他应用程序，对脆弱性做出响应。例如：通过邮件程序通知管理员等。

8 性能要求

8.1 速度

应可通过调整扫描线程或进程数目等技术手段对扫描速度进行调节。

8.2 稳定性和容错性

a) 主界面不应失去响应或非正常退出；

b) 扫描进度不应停滞不前。

8.3 漏洞发现能力

网络脆弱性扫描产品的技术文档应给出系统能够扫描的漏洞数目，并针对漏洞给出详细描述。

8.4 误报率

网络脆弱性扫描产品的技术文档应标明该系统的误报率，并指明所使用的测试方法、测试工具、测试环境和测试步骤。

8.5 漏报率

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

9 保证要求

9.1 基本型

9.1.1 配置管理

a) 开发者应为网络脆弱性扫描产品的不同版本提供唯一的标识；
b) 开发者应针对不同用户提供唯一的授权标识；
c) 要求配置项应有唯一的标识。

9.1.2 安全功能开发过程

9.1.2.1 功能设计

a) 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；
b) 功能设计应当是内在一致的；
c) 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；
d) 功能设计应当完整地表示网络脆弱性扫描产品安全功能。

9.1.2.2 表示对应性

a) 开发者应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；
b) 对于网络脆弱性扫描产品安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完整地细化。

9.1.3 测试

9.1.3.1 功能测试

a) 开发者应测试安全功能，将结果文档化并提供测试文档；
b) 测试文档应包括测试计划、测试规程、测试报告。测试计划应标识要测试的安全功能，并描述测试的目标。测试规程应标识要执行的测试，并描述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。测试报告的内容包括预期的测试结果和实际测试结果。

9.1.3.2 覆盖分析

a) 开发者应提供测试覆盖的分析结果；
b) 测试覆盖的分析结果应表明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。

9.1.4 指导性文档

9.1.4.1 管理员指南

a) 开发者应提供系统管理员使用的管理员指南；
b) 管理员指南应说明以下内容：
   1）网络脆弱性扫描产品可以使用的管理功能和接口；
   2）怎样安全地管理网络脆弱性扫描产品；
   3）在安全处理环境中应进行控制的功能和权限；
   4）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；
   5）所有受管理员控制的安全参数，如果可能，应指明安全值；
   6）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；
   7）所有与系统管理员有关的 IT 环境的安全要求。
c) 管理员指南应与为评估而提供的其他所有文件保持一致。

9.1.4.2 用户指南

a) 开发者应提供用户指南；

b) 用户指南应说明以下内容：
   1）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；
   2）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；
   3）用户可获取但应受安全处理环境控制的所有功能和权限；
   4）网络脆弱性扫描产品安全操作中用户所应承担的职责；
   5）与用户有关的 IT 环境的所有安全要求。
c) 用户指南应与为评估而提供的其他所有文件保持一致。

9.1.5 交付与运行

a) 开发者应提供文档说明网络脆弱性扫描产品的安装、生成和启动的过程；
b) 上述过程中不应向非产品使用者提供网络拓扑信息。

9.1.6 生命周期支持

a) 开发者应提供开发安全文件；
b) 开发安全文件应描述在网络脆弱性扫描产品的开发环境中，为保护网络脆弱性扫描产品设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在网络脆弱性扫描产品的开发和维护过程中执行安全措施的证据。

9.2 增强型

9.2.1 配置管理

9.2.1.1 授权机制

a) 开发者应使用配置管理系统并提供配置管理文档，为网络脆弱性扫描产品的不同版本提供唯一的标识；
b) 配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项；
c) 配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述；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；
d) 配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

9.2.1.2 配置管理范围

a) 开发者应提供配置管理文档；
b) 配置管理文档应说明配置管理系统至少能跟踪：网络脆弱性扫描产品实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档，并描述配置管理系统是如何跟踪配置项的。

9.2.2 安全功能开发过程

9.2.2.1 功能设计

a) 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；
b) 功能设计应当是内在一致的；
c) 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出错信息的细节；
d) 功能设计应当完整地表示网络脆弱性扫描产品安全功能。

9.2.2.2 高层设计

a) 开发者应提供网络脆弱性扫描产品安全功能的高层设计；
b) 高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强网络脆弱性扫描产品安全功能的子系统和其他子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提

供安全功能子系统的作用、例外情况和出错信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

9.2.2.3 低层设计

a) 开发者应提供网络脆弱性扫描产品安全功能的低层设计；

b) 低层设计应是非形式化、内在一致的。在描述网络脆弱性扫描产品安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口的作用、例外情况和错误信息的细节；

c) 低层设计还应包括以下内容：

1) 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

2) 说明如何提供每一个安全策略的强化功能；

3) 说明如何将网络脆弱性扫描产品加强安全策略的模块和其他模块分离开。

9.2.2.4 表示对应性

a) 开发者应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；

b) 对于网络脆弱性扫描产品安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完整地细化。

9.2.3 测试

9.2.3.1 功能测试

a) 开发者应测试安全功能，将结果文档化并提供测试文档；

b) 测试文档应包括测试计划、测试过程、测试报告。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述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。测试报告的内容包括预期的测试结果和实际测试结果。

9.2.3.2 覆盖分析

a) 开发者应提供测试覆盖的分析结果；

b) 测试覆盖的分析结果应表明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，且该对应是完整的。

9.2.3.3 深度

a) 开发者应提供测试深度的分析；

b) 在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

9.2.3.4 独立性测试

开发者应提供证据证明，开发者提供的网络脆弱性扫描产品经过独立的第三方测试并通过。

9.2.4 指导性文档

9.2.4.1 管理员指南

a) 开发者应提供系统管理员使用的管理员指南；

b) 管理员指南应说明以下内容：

1) 网络脆弱性扫描产品管理员可以使用的管理功能和接口；

2) 怎样安全地管理网络脆弱性扫描产品；

3) 在安全处理环境中应进行控制的功能和权限；

4) 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；

5) 所有受管理员控制的安全参数，如果可能，应指明安全值；

6) 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；

7）所有与系统管理员有关的 IT 环境的安全要求。

c） 管理员指南应与为评估而提供的其他所有文件保持一致。

9.2.4.2 用户指南

a） 开发者应提供用户指南；

b） 用户指南应说明以下内容：

1）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；

2）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；

3）用户可获取但应受安全处理环境控制的所有功能和权限；

4）网络脆弱性扫描产品安全操作中用户所应承担的职责；

5）与用户有关的 IT 环境的所有安全要求。

c） 用户指南应与为评估而提供的其他所有文件保持一致。

9.2.5 脆弱性评定

9.2.5.1 指南检查

a） 开发者应提供指南性文档；

b） 在指南性文档中，应确定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）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出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。指南性文档应是完整的、清晰的、一致的、合理的。

9.2.5.2 脆弱性分析

a） 开发者应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分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施；

b） 对每一条脆弱性，应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。在文档中，还需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。

9.2.6 交付与运行

9.2.6.1 交付

a） 开发者应使用一定的交付程序交付网络脆弱性扫描产品，并将交付过程文档化；

b） 交付文档应描述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；

c） 上述过程中不应向非产品使用者提供网络拓扑信息。

9.2.6.2 安装生成

开发者应提供文档说明网络脆弱性扫描产品的安装、生成和启动的过程。

9.2.7 生命周期支持

9.2.7.1 开发安全

a） 开发者应提供开发安全文件；

b） 开发安全文件应描述在网络脆弱性扫描产品的开发环境中，为保护网络脆弱性扫描产品设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在网络脆弱性扫描产品的开发和维护过程中执行安全措施的证据。

9.2.7.2 生命周期模型

a） 开发者应建立生命周期模型并提供生命周期定义文档；

b) 在生命周期定义文档中，应描述用于开发和维护网络脆弱性扫描产品的模型。为了对网络脆弱性扫描产品开发和维护进行必要的控制，该模型应提供相应的支持。

9.2.7.3 工具和技术

a) 开发者应标识用于开发网络脆弱性扫描产品的工具，并对开发工具中已选择的依赖实现的选项文档化；

b) 在开发工具文档中，应明确定义所有用于实现的开发工具和实现中每个语句的含义，以及所有基于实现的选项的含义。

附 录 A
（资料性附录）
网络脆弱性扫描产品介绍

A.1 脆弱性扫描技术

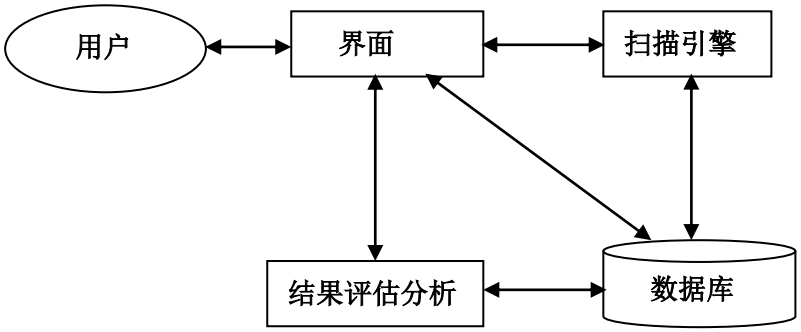
脆弱性扫描技术是一类重要的网络安全技术。脆弱性扫描技术与防火墙、入侵检测等技术互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，评估网络风险等级。网络管理员可以根据扫描的结果修补网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。脆弱性扫描是一种主动的防范措施。

脆弱性扫描技术主要分为两类：主机脆弱性扫描技术和网络脆弱性扫描技术。网络脆弱性扫描技术主要针对网络系统和设备中不合适的设置、脆弱的口令以及其他同安全规则抵触的对象，通过网络进行检查和提出补救方法等；而主机脆弱性扫描技术则是直接在被扫描主机上对主机系统进行扫描并记录系统的反应，从而发现其中的漏洞，并提出补救方法。

本标准针对采用了网络脆弱性扫描技术的产品提出相关技术要求。

A.2 网络脆弱性扫描产品简介

网络脆弱性扫描产品的功能是对计算机系统和网络设备进行安全评估分析，即进行安全相关的检查，发现其漏洞和脆弱性，对系统的安全状况进行评估、风险分析、安全趋势分析，对发现的问题提出解决方案和建议，从而提高网络系统安全性能。



图A1 网络脆弱性扫描产品的系统基本组成

A.3 体系结构

A.3.1 系统组成

系统的基本组成由四个模块构成，模块间的关系如图A1所示。分布式系统由一个以上扫描引擎和其他三个模块组成。

A.3.2 界面

界面部分主要完成以下的功能：

a) 负责接受并处理用户输入、定制扫描策略、开始和终止扫描、定制评估分析报告等；

b) 显示系统工作状态。

A.3.3 扫描引擎

扫描引擎部分主要完成以下的功能：

a） 响应界面指令；

b） 读取扫描策略数据库，并依此制定执行方案；

c） 执行扫描方案，启动扫描进程和线程，并进行调度管理；

d） 将扫描结果存档保存。

A.3.4 结果评估分析

结果评估分析部分主要完成以下的功能：

a） 读取数据库中扫描结果信息；

b） 形成结果报告。

A.3.5 数据库

数据库部分主要完成以下的功能：

a） 存放扫描结果、定制策略内容、脆弱性描述及其解决方法；

b） 提供数据查询、管理功能。

参考文献

GB/T 9387.2-1995 信息系统 开放系统互连 基本参考模型 第2部分：安全体系结构

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）