ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20278—2013
代替 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

Information security technology—
Security technical requirements for network vulnerability scanners

2013-12-31 发布　　2014-07-15 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20278—2006《信息安全技术　网络脆弱性扫描产品技术要求》，本标准与 GB/T 20278—2006 的主要差异如下：

——标准名称修改为《信息安全技术　网络脆弱性扫描产品安全技术要求》；

——修改了“网络脆弱性扫描”的定义（见 3.3）；

——删除了“NIS 服务的脆弱性”（见 2006 版的 7.3.1.8）；

——删除了“数据库脆弱性”（见 2006 版的 7.3.1.18）；

——删除了“RPC 端口”（见 2006 版的 7.3.4.1）；

——删除了“NT 服务”（见 2006 版的 7.3.4.5）；

——删除了“报警功能”（见 2006 版的 7.4.4.1）；

——删除了“安装与操作控制”（见 2006 版的 7.5）；

——删除了“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”（见 2006 版的 7.7.4.2、7.7.4.3、7.7.4.4 和 8）；

——删除了“性能要求”；

——新增了在产品升级过程中升级安全措施要求；

——新增了扫描结果的比对分析功能；

——在产品自身安全要求中新增了鉴别数据保护、鉴别失败处理、超时锁定或注销、远程管理等功能；

——调整了标准的整体结构，按照产品安全功能要求、自身安全要求和安全保证要求三部分描述，同时，细化了产品自身安全的要求项，明确了审计功能要求的内容。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、启明星辰信息技术有限公司、北京中科网威信息技术有限公司。

本标准主要起草人：顾建新、陆臻、俞优、顾健、赵婷、王志佳、王红虹、明旭。

信息安全技术
网络脆弱性扫描产品安全技术要求

1 范围

本标准规定了网络脆弱性扫描产品的安全功能要求、自身安全要求和安全保证要求，并根据安全技术要求的不同对网络脆弱性扫描产品进行了分级。

本标准适用于网络脆弱性扫描产品的研制、生产和检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.3—2008 信息技术 信息技术安全性评估准则 第3部分：安全保证要求

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999 和 GB/T 25069—2010 中界定的以及下列术语和定义适用于本文件。

3.1

扫描 scan

使用技术工具对目标系统进行探测，查找目标系统中存在的安全隐患的过程。

3.2

脆弱性 vulnerability

网络系统中可能被利用并造成危害的弱点。

3.3

网络脆弱性扫描 network vulnerability scan

通过网络对目标系统安全隐患进行远程探测，检查和分析其安全脆弱性，从而发现可能被入侵者利用的漏洞，并提出一定的防范和补救措施建议。

3.4

旗标 banner

由应用程序发送的一段信息，通常包括欢迎语、应用程序名称和版本等信息。

4 缩略语

下列缩略语适用于本文件。

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:文件传送协议(File Transfer Protocol)
IP:网间协议(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)
POP3:邮局协议第三版(Post Office Protocol 3)
RPC:远程过程调用(Remote Procedure Call)
SMB:服务器消息块(Server Message Block)
SMTP:简单邮件传送协议(Simple Mail Transfer Protocol)
SNMP:简单网络管理协议(Simple Network Management Protocol)
TCP:传输控制协议(Transmission Control Protocol)
UDP:用户数据报协议(User Datagram Protocol)

5 网络脆弱性扫描产品等级划分

5.1 等级划分说明

5.1.1 基本级

本级规定了网络脆弱性扫描产品的基本功能要求,通过一定的用户标识和身份鉴别限制对产品功能的使用和数据访问的控制,使产品具备自主安全保护的能力,保证网络脆弱性扫描产品的正常运行,具备审计功能要求,使得管理员的各项操作行为和扫描事件都是可追踪的。通过扫描信息的获取,针对扫描结果提供基本的分析处理能力,并生成报告。其自身安全要求依据 GB 17859—1999 中系统审计保护级的相关要求,安全保证要求依据 GB/T 18336.3—2008 中规定的 EAL2 级要求。

5.1.2 增强级

本级的网络脆弱性扫描产品除具备上述基本级要求的全部内容以外,对管理员进一步划分了不同的安全管理角色,以细化对产品管理权限的控制,同时,还增加了扫描结果的导入导出,扫描结果的比对、已知账号/口令下的扫描、升级安全措施、扫描 IP 地址限制、互动性要求、审计存储安全等内容,使得产品具备的功能要求更加全面,使用更加方便。产品自身安全要求依据 GB 17859—1999 中安全标记保护级的相关要求,产品的安全保证要求覆盖了产品从开发到使用的全部阶段,依据 GB/T 18336.3—2008 中规定的 EAL4 级要求,并在此基础上,将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

5.2 等级划分

网络脆弱性扫描产品的等级划分如表 1、表 2 和表 3 所示。对网络脆弱性扫描产品的等级评定是依据这三个表格综合评定得出的,符合基本级的网络脆弱性扫描产品应满足表 1、表 2 和表 3 中所标明的基本级产品应满足的所有项目;符合增强级的网络脆弱性扫描产品应满足表 1、表 2 和表 3 所标明的增强级产品应满足的所有项目。

表 1　安全功能要求等级划分表

安全功能要求			基本级	增强级
信息获取	端口扫描	TCP 端口	*	*
		UDP 端口	*	*
		端口协议分析	*	*
	操作系统探测		*	*
	服务旗标		*	*
	其他信息		*	*
脆弱性扫描内容	浏览器脆弱性		*	*
	邮件服务脆弱性		*	*
	FTP 服务脆弱性		*	*
	Web 服务脆弱性		*	*
	DNS 服务脆弱性		*	*
	其他已知 TCP/IP 服务脆弱性		*	*
	RPC 服务的脆弱性		*	*
	SNMP 服务的脆弱性		*	*
	弱口令		*	*
	Windows 操作系统用户、组、口令、共享、注册表等脆弱性		*	*
	木马		*	*
	NFS 服务脆弱性		*	*
	路由器/交换机脆弱性		*	*
	DoS 攻击脆弱性		*	*
	文件共享		*	*
扫描结果分析处理	结果入库		*	*
	结果导入导出		—	*
	报告生成		*	*
	报告定制		—	*
	报告输出		*	*
	结果浏览		*	*
	脆弱性修补建议		*	*
	结果比对		—	*

表 1（续）

安全功能要求		基本级	增强级
扫描配置	扫描策略	*	*
	计划任务	*	*
	已知账号/口令扫描	—	*
扫描对象的安全性	对目标系统所在网络性能的影响	*	*
	对目标系统的影响	*	*
升级能力		*	* *
扫描速度		*	*
扫描 IP 地址限制		—	*
互动性要求		—	*
注：“*”表示具有该要求；“—”表示不具有该要求；“**”表示增强级较基本级有更高的要求。本标准中将基本级和增强级的具体要求分别进行描述，其中“**加粗宋体字**”表示增强级较基本级中增加的内容。			

表 2　自身安全要求等级划分表

自身安全要求			基本级	增强级
标识与鉴别	用户标识	属性定义	*	*
		属性初始化	*	*
		唯一性标识	*	*
	身份鉴别	基本鉴别	*	*
		鉴别数据保护	*	*
		鉴别失败处理	—	*
		超时锁定或注销	—	*
安全管理	安全管理功能		*	*
	易用性		*	*
	角色管理		—	*
	远程管理		—	有则适用
审计日志	审计日志生成		*	*
	审计日志保存		*	*
	审计日志管理		*	* *
	审计存储安全		—	*
注：“*”表示具有该要求；“—”表示不具有该要求；“**”表示增强级较基本级有更高的要求。本标准中将基本级和增强级的具体要求分别进行描述，其中“**加粗宋体字**”表示增强级较基本级中增加的内容。				

表 3　安全保证要求等级划分表

安全保证要求			基本级	增强级
配置管理	部分配置管理自动化		—	*
	配置管理能力	版本号	*	*
		配置项	*	*
		授权控制	—	*
		产生支持和接受程序	—	*
	配置管理范围	配置管理覆盖	—	*
		问题跟踪配置管理覆盖	—	*
交付与运行	交付程序		*	*
	修改检测		—	*
	安装、生成和启动程序		*	*
开发	功能规范	非形式化功能规范	*	*
		充分定义的外部接口	—	*
	高层设计	描述性高层设计	*	*
		安全加强的高层设计	—	*
	安全功能实现的子集		—	*
	描述性低层设计		—	*
	非形式化对应性证实		*	*
	非形式化产品安全策略模型		—	*
指导性文档	管理员指南		*	*
	用户指南		*	*
生命周期支持	安全措施标识		—	*
	开发者定义的生命周期模型		—	*
	明确定义的开发工具		—	*
测试	测试覆盖	覆盖证据	*	*
		覆盖分析	—	*
	测试：高层设计		—	*
	功能测试		*	*
	独立测试	一致性	*	*
		抽样	*	*

表 3（续）

安全保证要求			基本级	增强级
脆弱性评定	误用	指南审查	—	*
		分析确认	—	*
	产品安全功能强度评估		*	*
	脆弱性分析	开发者脆弱性分析	*	*
		独立的脆弱性分析	—	*
		中级抵抗力	—	*
注："*"表示具有该要求；"—"表示不具有该要求。本标准中将基本级和增强级的具体要求分别进行描述，其中**"加粗宋体字"**表示增强级较基本级中增加的内容。				

6 使用环境

网络脆弱性扫描产品与被扫描系统的各网络设备或者主机应处于连通状态，中途无其他网络安全设备的防护。

7 基本级安全技术要求

7.1 安全功能要求

7.1.1 信息获取

7.1.1.1 端口扫描

7.1.1.1.1 TCP 端口

网络脆弱性扫描产品应能扫描所有 TCP 端口，检查其是否开启。

7.1.1.1.2 UDP 端口

网络脆弱性扫描产品应能扫描所有 UDP 端口，检查其是否开启。

7.1.1.1.3 端口协议分析

就扫描得到的已开启的 TCP/UDP 端口，网络脆弱性扫描产品应能判断相应端口对应的通用服务或使用的协议。

7.1.1.2 操作系统探测

网络脆弱性扫描产品应能对操作系统类型和版本号进行探测。

7.1.1.3 服务旗标

网络脆弱性扫描产品应能获取已开启的各项常用服务的旗标。

7.1.1.4 其他信息

网络脆弱性扫描产品应能对其他信息进行探测，例如网络配置信息、运行状态信息等。

7.1.2 脆弱性扫描内容

7.1.2.1 浏览器脆弱性

网络脆弱性扫描产品应能检查与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；
c) 浏览器自身脆弱性；
d) 其他安全隐患。

7.1.2.2 邮件服务脆弱性

网络脆弱性扫描产品应能检查使用了 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) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
   ——对输入缺乏合法性检查；
   ——不能正确处理异常情况。
c) 服务器的危险或错误配置，包括：
   ——允许 EXPN 和 VRFY 命令；
   ——允许邮件转发；
   ——其他不安全配置。
d) 其他安全隐患。

7.1.2.3 FTP 服务脆弱性

网络脆弱性扫描产品应能检查使用了 FTP 协议的服务程序的安全问题，检查项目应包括：

a) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
   ——对输入缺乏合法性检查；
   ——不能正确处理异常情况。
c) 服务器的危险或错误配置，包括：
   ——允许匿名登录；
   ——使用了默认口令；
   ——允许危险命令；
   ——其他不安全配置。
d) 其他安全隐患。

7.1.2.4 Web 服务脆弱性

网络脆弱性扫描产品应能检查提供 Web 服务程序的安全问题，检查项目应包括：

a) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
   ——对输入缺乏合法性检查；
   ——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，包括：

——文件属性错误；

——目录属性错误；

——其他不安全配置。

e) 其他安全隐患。

7.1.2.5 DNS服务脆弱性

网络脆弱性扫描产品应能检查DNS服务的安全问题，检查项目应包括：

a) 服务程序旗标和版本号。

b) 服务程序本身的脆弱性，包括：

——对输入缺乏合法性检查；

——不能正确处理异常情况。

c) 其他安全隐患。

7.1.2.6 其他已知TCP/IP服务脆弱性

网络脆弱性扫描产品应能检查其他使用了TCP/IP协议的服务程序的安全问题，检查项目应包括：

a) 服务程序旗标和版本号。

b) 服务程序本身的脆弱性，包括：

——对输入缺乏合法性检查；

——不能正确处理异常情况。

c) 服务程序的错误配置。

7.1.2.7 RPC服务的脆弱性

网络脆弱性扫描产品应能检查使用了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。

7.1.2.8 SNMP服务的脆弱性

网络脆弱性扫描产品应能检查使用了SNMP协议的服务程序的安全问题，检查项目应包括：

a) SNMP口令脆弱性检查。

b) 检查SNMP服务是否会暴露下列系统敏感信息，包括：

——TCP端口表；

——UDP端口表；

——服务列表；

——进程列表；

——路由表；

——网络接口设备表。

7.1.2.9 弱口令

网络脆弱性扫描产品应能采用字典或穷举等方法检查系统用户口令的健壮性，检查项目应包括：

——系统是否使用了用户名称经过简单变换后的口令；

——系统是否使用了易猜测口令。

7.1.2.10 Windows 操作系统用户、组、口令、共享、注册表等脆弱性

网络脆弱性扫描产品应能检查 Windows 操作系统特有的一些脆弱性，检查项目应包括：

a) 系统安全设置，包括：
   ——注册表项目访问权限设置；
   ——审核策略设置；
   ——系统口令策略设置。
b) 操作系统版本和补丁安装情况检查。
c) 其他相关检查。

7.1.2.11 木马

网络脆弱性扫描产品应能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。

7.1.2.12 NFS 服务脆弱性

网络脆弱性扫描产品应能检查 NFS 服务相关的脆弱性。

7.1.2.13 路由器/交换机脆弱性

网络脆弱性扫描产品应能检查路由器、交换机及其开启服务相关的脆弱性。

7.1.2.14 DoS 攻击脆弱性

网络脆弱性扫描产品应能使用实际攻击手法对目标主机进行真实的攻击，以检查目标主机对已知 DoS 攻击的抵御能力。

7.1.2.15 文件共享

网络脆弱性扫描产品应能检查使用的 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。

7.1.3 扫描结果分析处理

7.1.3.1 结果入库

扫描结果应能写入结果数据库。

7.1.3.2 报告生成

网络脆弱性扫描产品应能根据扫描结果生成相应的报告，报告具备要求包括如下内容：

a) 各脆弱点的 CVE 号、详细信息、补救建议等；
b) 目标的风险等级评估，将扫描脆弱点按风险严重程度分级，并明确标出；
c) 多个目标扫描后的结果的总体报告；
d) 对关键的脆弱性扫描信息可生成摘要报告。

7.1.3.3 报告输出

报告应可输出为通用的文档格式，例如 PDF、DOC、HTML 等。

7.1.3.4 结果浏览

网络脆弱性扫描产品应提供扫描结果浏览功能。

7.1.3.5 脆弱性修补建议

网络脆弱性扫描产品应能对发现的脆弱性提出修补建议，脆弱性修补建议应满足下列要求：

a) 对不同的操作系统类型提出针对性的脆弱性修补方法；

b) 脆弱性描述应详细，提供的脆弱性修补方法应确保其合理性和可用性。

7.1.4 扫描配置

7.1.4.1 扫描策略

网络脆弱性扫描产品应提供方便的定制策略的方法，可以指定扫描地址范围、端口范围、脆弱性类型等。

7.1.4.2 计划任务

网络脆弱性扫描产品应能定制扫描计划，可以定时启动或者按周期执行扫描任务。

7.1.5 扫描对象的安全性

7.1.5.1 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。

7.1.5.2 对目标系统的影响

扫描应不影响目标系统的正常工作，避免使用攻击方法进行测试；在使用某些可能对目标系统产生不良后果的扫描手段时（如使用 DoS 攻击等测试手段），网络脆弱性扫描产品应在测试开始前给目标系统或者目标系统管理员明确的提示。

7.1.6 升级能力

网络脆弱性扫描产品应能够对脆弱性特征库进行更新：

a) 产品体系结构的设计应有利于产品的升级，方便升级操作；

b) 支持手动或者自动升级操作。

7.1.7 扫描速度

网络脆弱性扫描产品应提供合理的扫描速度，可通过调整扫描线程或进程数目等方法对扫描速度进行调节。

7.2 自身安全要求

7.2.1 标识与鉴别

7.2.1.1 用户标识

7.2.1.1.1 属性定义

网络脆弱性扫描产品应为每个管理角色规定与之相关的安全属性，例如管理角色标识、鉴别信息、隶属组、权限等。

7.2.1.1.2 属性初始化

网络脆弱性扫描产品应提供使用默认值对创建的每个管理角色的属性进行初始化的能力。

7.2.1.1.3 唯一性标识

网络脆弱性扫描产品应为用户提供唯一标识，同时将用户的身份标识与该用户的所有可审计能力相关联。

7.2.1.2 身份鉴别

7.2.1.2.1 基本鉴别

网络脆弱性扫描产品应在执行任何与管理员相关功能之前鉴别用户的身份。

7.2.1.2.2 鉴别数据保护

网络脆弱性扫描产品应保证鉴别数据不被未授权查阅或修改。

7.2.2 安全管理

7.2.2.1 安全管理功能

网络脆弱性扫描产品应保证授权管理员具备以下管理权限：

a) 查看安全属性；
b) 修改安全属性；
c) 启动、关闭全部或部分安全功能；
d) 制定和修改各种安全策略。

7.2.2.2 易用性

网络脆弱性扫描产品应能够稳定的运行，并提供方便易用的管理界面：

a) 提供准确、直观的扫描进度显示，便于用户了解扫描过程；
b) 扫描任务应能随时暂停或者终止。

7.2.3 审计日志

7.2.3.1 审计日志生成

网络脆弱性扫描产品应能对以下事件生成日志：

a) 管理员的登录成功和失败；
b) 对安全策略进行更改的操作；
c) 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；
d) 对管理员、管理角色进行增加、删除和属性修改的操作；
e) 对审计记录的备份和删除操作；
f) 扫描任务的启动、暂停和停止等操作；
g) 管理员的其他操作。

每一条审计日志中至少应包括事件主体、事件发生的时间日期、事件描述和结果。若采用远程登录方式对产品进行管理还应记录管理主机的地址。

7.2.3.2 审计日志保存

网络脆弱性扫描产品的审计日志应能存储于永久性存储介质中。

7.2.3.3 审计日志管理

应提供下列审计日志管理功能：

a) 只允许授权管理员访问审计日志；

b) 提供对审计日志的查询功能；

c) 授权管理员应能保存、删除和清空审计日志。

7.3 安全保证要求

7.3.1 配置管理

7.3.1.1 版本号

开发者应为产品的不同版本提供唯一的标识。

7.3.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，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维护的证据。

7.3.2 交付与运行

7.3.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

7.3.2.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

7.3.3 开发

7.3.3.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；

b) 是内在一致的；

c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；

d) 完备地表示产品安全功能。

7.3.3.2 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 表示应是非形式化的；

b) 是内在一致的；

c) 按子系统描述安全功能的结构；

d) 描述每个安全功能子系统所提供的安全功能性；

e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；

f) 标识安全功能子系统的所有接口；

g) 标识安全功能子系统的哪些接口是外部可见的。

7.3.3.3 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间的对应性分析。

对于产品安全功能所表示的每个相邻对，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且完备地细化。

7.3.4 指导性文档

7.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；

b) 怎样安全地管理产品；

c) 在安全处理环境中应被控制的功能和权限；

d) 所有对与产品的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 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实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

7.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但应受安全处理环境所控制的所有功能和权限；

d) 产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

7.3.5 测试

7.3.5.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

7.3.5.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 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，这些概况应包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，应表明测试成功后的预期输出；

d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

7.3.5.3 独立测试

7.3.5.3.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

7.3.5.3.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

7.3.6 脆弱性评定

7.3.6.1 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

7.3.6.2 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对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。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。

8 增强级安全技术要求

8.1 安全功能要求

8.1.1 信息获取

8.1.1.1 端口扫描

8.1.1.1.1 TCP 端口

网络脆弱性扫描产品应能扫描所有 TCP 端口，检查其是否开启。

8.1.1.1.2 UDP 端口

网络脆弱性扫描产品应能扫描所有 UDP 端口，检查其是否开启。

8.1.1.1.3 端口协议分析

就扫描得到的已开启的 TCP/UDP 端口，网络脆弱性扫描产品应能判断相应端口对应的通用服务或使用的协议。

8.1.1.2 操作系统探测

网络脆弱性扫描产品应能对操作系统类型和版本号进行探测。

8.1.1.3 服务旗标

网络脆弱性扫描产品应能获取已开启的各项常用服务的旗标。

8.1.1.4 其他信息

网络脆弱性扫描产品应能对其他信息进行探测，例如网络配置信息、运行状态信息等。

8.1.2 脆弱性扫描内容

8.1.2.1 浏览器脆弱性

网络脆弱性扫描产品应能检查与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；
c) 浏览器自身脆弱性；
d) 其他安全隐患。

8.1.2.2 邮件服务脆弱性

网络脆弱性扫描产品应能检查使用 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) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
   ——对输入缺乏合法性检查；
   ——不能正确处理异常情况。
c) 服务器的危险或错误配置，包括：
   ——允许 EXPN 和 VRFY 命令；
   ——允许邮件转发；
   ——其他不安全配置。
d) 其他安全隐患。

8.1.2.3 FTP 服务脆弱性

网络脆弱性扫描产品应能检查使用了 FTP 协议的服务程序的安全问题，检查项目应包括：

a) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
   ——对输入缺乏合法性检查；
   ——不能正确处理异常情况。
c) 服务器的危险或错误配置，包括：
   ——允许匿名登录；
   ——使用了默认口令；
   ——允许危险命令；
   ——其他不安全配置。
d) 其他安全隐患。

8.1.2.4 Web 服务脆弱性

网络脆弱性扫描产品应能检查提供 Web 服务程序的安全问题，检查项目应包括：

a) 服务程序旗标和版本号。

b) 服务程序本身的脆弱性，包括：
——对输入缺乏合法性检查；
——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，包括：
——文件属性错误；
——目录属性错误；
——其他安全配置。
e) 其他安全隐患。

8.1.2.5 DNS 服务脆弱性

网络脆弱性扫描产品应能检查 DNS 服务的安全问题，检查项目应包括：
a) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
——对输入缺乏合法性检查；
——不能正确处理异常情况。
c) 其他安全隐患。

8.1.2.6 其他已知 TCP/IP 服务脆弱性

网络脆弱性扫描产品应能检查其他使用了 TCP/IP 协议的服务程序的安全问题，检查项目应包括：
a) 服务程序旗标和版本号。
b) 服务程序本身的脆弱性，包括：
——对输入缺乏合法性检查；
——不能正确处理异常情况。
c) 服务程序的错误配置。

8.1.2.7 RPC 服务的脆弱性

网络脆弱性扫描产品应能检查使用了 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。

8.1.2.8 SNMP 服务的脆弱性

网络脆弱性扫描产品应能检查使用了 SNMP 协议的服务程序的安全问题，检查项目应包括：
a) SNMP 口令脆弱性检查。
b) 检查 SNMP 服务是否会暴露下列系统敏感信息，包括：
——TCP 端口表；
——UDP 端口表；
——服务列表；
——进程列表；
——路由表；
——网络接口设备表。

8.1.2.9 弱口令

网络脆弱性扫描产品应能采用字典或穷举等方法检查系统用户口令的健壮性，检查项目应包括：

a) 系统是否使用了用户名称经过简单变换后的口令；
b) 系统是否使用了易猜测口令。

8.1.2.10 Windows 操作系统用户、组、口令、共享、注册表等脆弱性

网络脆弱性扫描产品应能检查 Windows 操作系统特有的一些脆弱性，检查项目应包括：

a) 系统安全设置，包括：
   ——注册表项目访问权限设置；
   ——审核策略设置；
   ——系统口令策略设置。
b) 操作系统版本和补丁安装情况检查。
c) 其他相关检查。

8.1.2.11 木马

网络脆弱性扫描产品应能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。

8.1.2.12 NFS 服务脆弱性

网络脆弱性扫描产品应能检查 NFS 服务相关的脆弱性。

8.1.2.13 路由器/交换机脆弱性

网络脆弱性扫描产品应能检查路由器、交换机及其开启服务相关的脆弱性。

8.1.2.14 DoS 攻击脆弱性

网络脆弱性扫描产品应能使用实际攻击手法对目标主机进行真实的攻击，以检查目标主机对已知 DoS 攻击的抵御能力。

8.1.2.15 文件共享

网络脆弱性扫描产品应能检查使用的 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。

8.1.3 扫描结果分析处理

8.1.3.1 结果入库

扫描结果应能写入结果数据库。

8.1.3.2 结果导入导出

可对扫描结果数据执行导入导出操作。

8.1.3.3 报告生成

网络脆弱性扫描产品应能根据扫描结果生成相应的报告，报告具备要求包括如下内容：

a) 各脆弱点的 CVE 号、详细信息、补救建议等；
b) 目标的风险等级评估，将扫描脆弱点按风险严重程度分级，并明确标出；
c) 多个目标扫描后的结果的总体报告；
d) 对关键的脆弱性扫描信息可生成摘要报告。

8.1.3.4 报告定制

报告内容应能根据用户要求进行定制生成。

8.1.3.5 报告输出

报告应可输出为通用的文档格式，例如 PDF、DOC、HTML 等。

8.1.3.6 结果浏览

网络脆弱性扫描产品应提供扫描结果浏览功能。

8.1.3.7 脆弱性修补建议

网络脆弱性扫描产品应能对发现的脆弱性提出修补建议，脆弱性修补建议应满足下列要求：
a) 对不同的操作系统类型提出针对性的脆弱性修补方法；
b) 脆弱性描述应详细，提供的脆弱性修补方法应确保其合理性和可用性。

8.1.3.8 结果比对

网络脆弱性扫描产品应提供对同一目标多次扫描结果或者不同主机间扫描结果的比对功能，并能根据比对结果生成比对报告。

8.1.4 扫描配置

8.1.4.1 扫描策略

网络脆弱性扫描产品应提供方便的定制策略的方法，可以指定扫描地址范围、端口范围、脆弱性类型等。

8.1.4.2 计划任务

网络脆弱性扫描产品应能定制扫描计划，可以定时启动或者按周期执行扫描任务。

8.1.4.3 已知账号/口令扫描

网络脆弱性扫描产品应能使用目标系统的已知账号/口令对其进行更有效的扫描。

8.1.5 扫描对象的安全性

8.1.5.1 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。

8.1.5.2 对目标系统的影响

扫描应不影响目标系统的正常工作，避免使用攻击方法进行测试；在使用某些可能对目标系统产生不良后果的扫描手段时（如使用 DoS 攻击等测试手段），网络脆弱性扫描产品在测试开始前给目标系统或者目标系统管理员明确的提示。

8.1.6 升级能力

网络脆弱性扫描产品应能够对脆弱性特征库进行更新：

a) 产品体系结构的设计应有利于产品的升级，方便升级操作；

b) 支持手动或者自动升级操作；

c) **具备升级安全措施，以防止得到错误的或伪造的产品升级包。例如采取身份验证、数字签名以及数据传输加密等手段。**

8.1.7 扫描速度

网络脆弱性扫描产品应提供合理的扫描速度，可通过调整扫描线程或进程数目等方法对扫描速度进行调节。

8.1.8 扫描 IP 地址限制

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。

8.1.9 互动性要求

网络脆弱性扫描产品应具备或采用一个标准的、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，达到与网络脆弱性扫描产品进行互动的目的。

8.2 自身安全要求

8.2.1 标识与鉴别

8.2.1.1 用户标识

8.2.1.1.1 属性定义

网络脆弱性扫描产品应为每个管理角色规定与之相关的安全属性，例如管理角色标识、鉴别信息、隶属组、权限等。

8.2.1.1.2 属性初始化

网络脆弱性扫描产品应提供使用默认值对创建的每个管理角色的属性进行初始化的能力。

8.2.1.1.3 唯一性标识

网络脆弱性扫描产品应为用户提供唯一标识，同时将用户的身份标识与该用户的所有可审计能力相关联。

8.2.1.2 身份鉴别

8.2.1.2.1 基本鉴别

网络脆弱性扫描产品应在执行任何与管理员相关功能之前鉴别用户的身份。

8.2.1.2.2 鉴别数据保护

网络脆弱性扫描产品应保证鉴别数据不被未授权查阅或修改。

8.2.1.2.3 鉴别失败处理

网络脆弱性扫描产品应提供一定的鉴别失败处理措施(如设置最大登录失败次数等),防止暴力猜测密码。

8.2.1.2.4 超时锁定或注销

网络脆弱性扫描产品应具有登录超时锁定或注销功能,在设定的时间段内没有任何操作的情况下,能锁定或终止会话,需要再次进行身份鉴别才能重新操作,最大超时时间仅由授权管理员设定。

8.2.2 安全管理

8.2.2.1 安全管理功能

网络脆弱性扫描产品应保证授权管理员具备以下管理权限:

a) 查看安全属性;
b) 修改安全属性;
c) 启动、关闭全部或部分安全功能;
d) 制定和修改各种安全策略。

8.2.2.2 易用性

网络脆弱性扫描产品应能够稳定的运行,并提供方便易用的管理界面:

a) 提供准确、直观的扫描进度显示,便于用户了解扫描过程;
b) 扫描任务应能随时暂停或者终止。

8.2.2.3 角色管理

网络脆弱性扫描产品应能对管理员角色进行区分:

a) 具有至少两种不同权限的管理员角色,如操作员、安全员、审计员等;
b) 应根据不同的功能模块,自定义各种不同权限角色,并可对管理员分配角色。

8.2.2.4 远程管理

若网络脆弱性扫描产品的控制台提供远程管理功能,应能对可远程管理的主机地址进行限制。

8.2.3 审计日志

8.2.3.1 审计日志生成

网络脆弱性扫描产品应能对以下事件生成日志:

a) 管理员的登录成功和失败;
b) 对安全策略进行更改的操作;
c) 因鉴别尝试不成功的次数超出了设定的限值,导致的会话连接终止;
d) 对管理员、管理角色进行增加、删除和属性修改的操作;
e) 对审计记录的备份和删除操作;
f) 扫描任务的启动、暂停和停止等操作;
g) 管理员的其他操作。

每一条审计日志中至少应包括事件主体、事件发生的时间日期、事件描述和结果。若采用远程登录方式对产品进行管理还应记录管理主机的地址。

8.2.3.2 审计日志保存

网络脆弱性扫描产品的审计日志应能存储于永久性存储介质中。

8.2.3.3 审计日志管理

应提供下列审计日志管理功能：

a) 只允许授权管理员访问审计日志；

b) 提供对审计日志的查询功能；

c) 授权管理员应能保存、删除和清空审计日志；

d) 提供对审计日志的按条件查询和排序功能。

8.2.3.4 审计存储安全

网络脆弱性扫描产品应提供数据存储空间耗尽处理功能，至少包括以下一种方式：

a) 当剩余存储空间达到阈值时，提供告警功能；

b) 在存储空间耗尽前，能够采用自动转储等方式将数据备份到其他存储空间；

c) 其他处理方式。

8.3 安全保证要求

8.3.1 配置管理

8.3.1.1 部分配置管理自动化

配置管理系统应提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。

配置管理计划应描述在配置管理系统中所使用的自动工具，并描述在配置管理系统中如何使用自动工具。

8.3.1.2 配置管理能力

8.3.1.2.1 版本号

开发者应为产品的不同版本提供唯一的标识。

8.3.1.2.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，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维护的证据。

8.3.1.2.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

8.3.1.2.4 产生支持和接受程序

开发者提供的配置管理文档应包括一个接受计划，接受计划应描述用来接受修改过的或新建的作

为产品组成部分的配置项的程序。

配置管理系统应支持产品的生成。

8.3.1.3 配置管理范围

8.3.1.3.1 配置管理覆盖

配置管理范围至少应包括产品实现表示、设计文档、测试文档、指导性文档、配置管理文档，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。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

8.3.1.3.2 问题跟踪配置管理覆盖

配置管理范围应包括安全缺陷，确保安全缺陷置于配置管理系统之下。

8.3.2 交付与运行

8.3.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

8.3.2.2 修改检测

交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异。还应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

8.3.2.3 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

8.3.3 开发

8.3.3.1 功能规范

8.3.3.1.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；

b) 是内在一致的；

c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；

d) 完备地表示产品安全功能。

8.3.3.1.2 充分定义的外部接口

功能规范应包括安全功能是完备地表示的合理性。

8.3.3.2 高层设计

8.3.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 表示应是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

8.3.3.2.2 安全加强的高层设计

开发者提供的安全加强的高层设计应满足以下要求：
a) 描述产品的功能子系统所有接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
b) 把产品分成安全策略实施和其他子系统来描述。

8.3.3.3 安全功能实现的子集

开发者应为选定的安全功能子集提供实现表示。实现表示应当无歧义而且详细地定义安全功能，使得无须进一步设计就能生成安全功能。实现表示应是内在一致的。

8.3.3.4 描述性低层设计

开发者应提供产品安全功能的低层设计，低层设计应满足以下要求：
a) 表示应是非形式化的；
b) 是内在一致的；
c) 按模块描述安全功能；
d) 描述每个模块的用途；
e) 根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；
f) 描述每个安全策略实施功能是如何被提供的；
g) 标识安全功能模块的所有接口；
h) 标识安全功能模块的哪些接口是外部可见的；
i) 描述安全功能模块所有接口的用途和用法，适当时应提供效果、例外情况和错误消息的细节；
j) 把产品分为安全策略实施模块和其他模块来描述。

8.3.3.5 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间的对应性分析。

对于产品安全功能所表示的每个相邻对，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且完备地细化。

8.3.3.6 非形式化产品安全策略模型

开发者应提供安全策略模型，安全策略模型应满足以下要求：
a) 表示应是非形式化的；
b) 描述所有能被模型化的安全策略的规则与特征；
c) 应包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；
d) 应阐明安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，而且是完备的。

8.3.4 指导性文档

8.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；

b) 怎样安全地管理产品；

c) 在安全处理环境中应被控制的功能和权限；

d) 所有对与产品的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 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实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

8.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但应受安全处理环境所控制的所有功能和权限；

d) 产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

8.3.5 生命周期支持

8.3.5.1 安全措施标识

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

8.3.5.2 开发者定义的生命周期模型

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

8.3.5.3 明确定义的开发工具

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

8.3.6 测试

8.3.6.1 测试覆盖

8.3.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

8.3.6.1.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

8.3.6.2 测试：高层设计

开发者应提供测试深度的分析。

深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

8.3.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 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，这些概况应包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，应表明测试成功后的预期输出；

d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

8.3.6.4 独立测试

8.3.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

8.3.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

8.3.7 脆弱性评定

8.3.7.1 误用

8.3.7.1.1 指南审查

开发者应提供指导性文档，指导性文档应满足以下要求：

a) **标识所有可能的产品运行模式(包括失败或操作失误后的运行)、它们的后果以及对于保持安全运行的意义；**

b) **是完备的、清晰的、一致的、合理的；**

c) **列出关于预期使用环境的所有假设；**

d) **列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。**

8.3.7.1.2 分析确认

开发者应提供分析文档论证指导性文档是完备的。

8.3.7.2 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

8.3.7.3 脆弱性分析

8.3.7.3.1 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对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。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。

8.3.7.3.2 独立的脆弱性分析

开发者应提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

8.3.7.3.3 中级抵抗力

开发者应提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

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安全技术要求
GB/T 20278—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
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 2 字数 54 千字
2014年5月第一版 2014年5月第一次印刷
*
书号:155066·1-49158 定价 30.00 元

GB/T 20278-2013

打印日期:2014年6月7日 F009A