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。