ICS 35.040
L 80

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

2006-05-31 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 是资料性附录。

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、赵德芳、刘 兵、丁宇征。

引　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)或修订版均不适合于本标准,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)

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。