

ICS 35.040  
CCS L 80



**NATIONAL STANDARD OF THE  
PEOPLE'S REPUBLIC OF CHINA**

**GB/T 20280-2006**

---

**Information security technology -- Testing and evaluation  
approaches for network vulnerability scanners**

信息安全技术 网络脆弱性扫描产品测试评价方法

**(English Translation)**

**Issued on: May 31, 2006**

**Implemented on: December 1, 2006**

---

**Issued by: General Administration of Quality Supervision, Inspection and  
Quarantine of the People's Republic of China**

## Table of Contents

|                                                       |    |
|-------------------------------------------------------|----|
| Foreword...                                           | 3  |
| Introduction...                                       | 4  |
| 1 Scope...                                            | 5  |
| 2 Normative References...                             | 5  |
| 3 Terms and Definitions...                            | 5  |
| 4 Stipulation of Symbol, Abbreviation and Notation... | 6  |
| 4.1 Symbols and Abbreviations...                      | 6  |
| 4.2 Stipulation of Notation...                        | 6  |
| 5 Overview of Network Vulnerability Scanners...       | 7  |
| 6 Testing Environment...                              | 7  |
| 7 Testing and Evaluation Approaches and Procedure...  | 8  |
| 7.1 Basic-type...                                     | 8  |
| 7.1.1 Basic function...                               | 8  |
| 7.1.3 Security assurance requirements...              | 18 |
| 7.2 Enhanced-type...                                  | 23 |
| 7.2.1 Basic function and performance...               | 23 |
| 7.2.2 Enhancement function...                         | 23 |
| 7.2.3 Security assurance requirements...              | 27 |

### Foreword

Appendix A of this Standard is normative.

This Standard was proposed by and shall be under the jurisdiction of the National Technical Committee on Information Security of Standardization Administration of China.

This Standard is responsibly drafted by Beijing Netpower Technology Ltd. AND Network Security Bureau of the Ministry of Public Security.

Chief drafters of this Standard. Xiao Jiang, Lu Yi, Yang Wei, Liu Wei, Liu Bing and Ding Yuzheng.

## 1 Scope

This Standard specifies the testing and evaluation approaches for network vulnerability scanners that adopt Transmission Control Protocol and Internet Protocol (TCP/IP).

This Standard is applicable to the testing and evaluation, R&D and application of security products for manual or automatic network vulnerability scan on computer information system.

This Standard is not applicable to products specialized for vulnerability scan on database system.

## 2 Normative References

The following standard contains the provisions which, through reference into this document, constitute the provisions of this document. For the dated reference, the subsequent amendments (excluding corrigendum) or revisions of these publications do not apply. However, the parties who reach an agreement according to this Standard are encouraged to study whether the latest edition of these documents can be used. For undated references, their latest editions apply.

GB/T 5271.8-2001 Information Technology - Vocabulary - Part 8.Security (idt ISO/IEC 2382-8.1998)

GB/T 20278-2006 Information Security Technology Technique Requirement for Network Vulnerability Scanners

## 3 Terms and Definitions

For the purpose of this Standard, terms and definitions established in GB/T 5271.8-2001 and GB/T 20278-2006 apply.

### 4.2 Stipulation of Notation

- a) Selection. It is used for emphasizing one or more than one options in the statement of certain functional requirement, represented by underlined italics.
- b) Note. This Standard performs a classified discussion on testing and evaluation

of network vulnerability scanners. The provisions in this Standard, unless stated, are all the requirements of basic products. The testing and evaluation item, testing content and testing and evaluation result of enhanced products shall be represented in italics.

## 5 Overview of Network Vulnerability Scanners

Brief introduction, system structure and product classification of network vulnerability scanners is detailed in Chapter 5 and Appendix A of GB/T 20278-2006.

## 6 Testing Environment

Testing environment for network vulnerability scanners is shown in Figure 1; the function of each equipment in Figure 1 is detailed in Table 1.

### 7.1.1.1.5 Label of scan data pack

- a) Evaluation contents. refer to the contents in 7.2.5 of GB/T 20278-2006.
- b) Testing and evaluation approaches.
  - 1) According to version release statement, user manual, high-level design document, testing document etc. of network vulnerability scanners, start network vulnerability scanners A and B in Figure 1 and perform scan function;
  - 2) Acquire scan data pack of network vulnerability scanners via sniffer (e.g. Tcpdump etc.) and analyze it.
- c) Testing and evaluation result. record testing result and judge whether the result conforms to requirements of testing and evaluation approaches.

### 7.1.1.2.4 Port and service scan

- a) Evaluation contents. refer to the contents in 7.3.4 of GB/T 20278-2006.
- b) Testing and evaluation approaches.

### 7.1.1.3.2 Analysis and processing for scan result

- a) Evaluation contents. refer to the contents in 7.4.2 of GB/T 20278-2006.

b) Testing and evaluation approaches.

#### **7.1.1.3.4 Security of scanning object**

a) Evaluation contents. refer to the contents in 7.4.4 of GB/T 20278-2006.

b) Testing and evaluation approaches.

#### **7.1.1.3.5 Upgrade capability**

a) Evaluation contents. refer to the contents in 7.4.2 of GB/T 20278-2006;

b) Testing and evaluation approaches. check version release statement, instruction manual, user manual etc. of network vulnerability scanners; start product A and B in Figure 1; inspect whether the products are provided with upgrade and update capability according to user manual.

c) Testing and evaluation result. record testing result and judge whether the result conforms to requirements of testing and evaluation approaches; it shall meet such requirements as convenient and automatic upgrade and available manual upgrade and vulnerability database addition.

#### **7.1.1.4.1 Installation and operation control**

a) Evaluation contents. refer to the contents in 7.5 of GB/T 20278-2006.

b) Testing and evaluation approaches. check version release statement, instruction manual, administrator manual, configuration management document of network vulnerability scanners, network vulnerability scanners shall be installed and operated practically.

c) Testing and evaluation result. records testing result and judge whether it conforms to the requirements of testing and evaluation approaches; it shall meet the following requirements.

1) Installation, management, operating controllability of network vulnerability scanners are explained in random documents; network vulnerability scanners execute the measure of issuing license (e.g. issuing serial number; generating license according to installed