# 中国移动网络扫描器产品
# 测试总结报告(评审稿)

中国移动通信集团公司研发中心

2004 年 9 月

# 目 录

# 1 前言

1. 随着中国移动网络规模的不断扩大，网络安全在网络的建设和运营中的地位也日益凸现其重要性。为了更好地建设中国移动通信网络，保证网络的安全、可靠，遵循国际国内安全标准规范，制定中国移动企业的标准规范并根据规范来进行相关安全产品测试以满足网络建设中的设备招标选型、工程验收等需求是十分必要的。
2. 为了保证网络的安全，中国移动在网络建设的过程中使用了大量的网络扫描器产品。保障网络安全中非常重要的一项措施就是消除信息系统中已知的安全脆弱性，信息系统安全扫描产品就是指用于对指定信息系统实施测试，判断该系统是否存在已知安全脆弱性的产品。
3. 网络扫描器检测参加测试的厂家有安氏、冠群金辰、启明星辰、赛门铁克、亿阳信通、中联绿盟、中软国际&ISS（按拼音字母顺序）。
4. 本测试中功能和性能的测试参考《中国移动网络扫描器产品测试规范》。
5. 本报告的解释权为中国移动通信集团公司。

# 2 参考标准

GB 17859-1999 计算机信息系统安全保护等级划分准则
GB/T 18336 信息安全-安全技术-IT 安全评估准则
GA/T 404-2002 网络安全漏洞扫描产品技术要求（报批稿）

# 3 扫描器使用需求的调研及评分规则的制定

## 3.1 扫描器使用需求的调研

为了使测试结果能够更好地指导中国移动对于网络扫描器产品的选择工作，测试组向集团公司网络部以及北京、广州、江苏、湖南、福建 5 个省公司网络部和信息化办公室发送了调研函以征集现网对于网络扫描产品的使用需求。调研的内容及反馈结果汇总如下。

### 3.1.1 现网使用操作系统的情况

表 1 操作系统所占的比例

| 反馈单位 | Windows | Linux | Solaris | HP-Unix | BSD | Other |
|---|---|---|---|---|---|---|
| 北京移动 | 90% | 1% | 2% | 5% | 1% | 1% |
| 广东移动 | 47% | 0.9% | 48% | 4% | 0.1% | 0% |
| 江苏移动 | 80% | 0% | 8% | 8% | 0% | 4% |
| 网络部 | 50% | 1% | 20% | 2% | 2% | 25% |
| 北京信息化 | 90% | 1% | 3% | 4% | 2% | 0% |
| 福建信息化 | 50% | 10% | 40% | 0% | 0% | 0% |
| 广东信息化 | 20% | 0% | 70% | 0% | 10% | 0% |
| 湖南信息化 | 88% | 0% | 0% | 0% | 0% | 12% |
| 平均 | 64.375% | 1.7375% | 23.875% | 2.875% | 1.8875% | 5.25% |

通过对表 1 的分析我们得出如下结果：Windows 操作系统和 Solaris 操作系统在现网上的使用情况大致占 64.375%和 23.875%，远远高于其他的操作系统。此外，计费中心也向测试组反馈 HP-Unix 在现网也有大量的应用。我们在实验中设置的环境涵盖了 Windows、Linux、Solaris、HP-Unix、BSD 涵盖的范围占目前中国移动现有的操作系统使用范围的 94.75%，因此此可以看出本次测试所选用的操作系统类型基本覆盖了现有的范围，达到了测试的目的。

通过上述分析，可以得出以下结论：评分中应适当提高 Windows、solaris 和 HP-Unix 操作系统的权重，以满足现网的实际状况。

### 3.1.2 现网所关注的安全隐患

表 2 安全隐患分类

| 反馈单位 | 远程进入系统 | 拒绝服务攻击 | 嵌入恶意代码 | Web 数据类型 | 其他 |
|---|---|---|---|---|---|
| 北京移动 | 1 | 4 | 3 | 2 | 5 |
| 广东移动 | 1 | 2 | 3 | 4 | 5 |
| 江苏移动 | 1 | 2 | 3 | 4 | 5 |
| 网络部 | 2 | 1 | 3 | 4 | 5 |
| 北京信息化 | 5 | 3 | 2 | 4 | 1 |
| 福建信息化 | 4 | 1 | 3 | 2 | 5 |
| 广东信息化 | 1 | 3 | 4 | 2 | 5 |
| 湖南信息化 | 1 | 2 | 4 | 3 | 5 |
| 综合 | 16 | 18 | 25 | 25 | 36 |
| 重要程度 | 1 | 1 | 2 | 2 | 3 |

从以上的结果中可以分析出，目前的安全隐患主要存在于在远程进入系统和拒绝服务服务攻击，应给予较高的权重。嵌入恶意代码和 Web 数据类型重要程度相同，而其他的入侵类型几乎不会发生，权重相对较低。

### 3.1.3 现网数据库的使用类型

表 3 对数据库使用情况的调查结果

| 反馈单位 | SQL Server | Oracle | 其它 |
|---|---|---|---|
| 北京移动 | 2 | 1 | 3 |
| 广东移动 | 1 | 1 | 3 |
| 江苏移动 | 1 | 1 | 3 |
| 网络部 | 1 | 1 | 3 |
| 北京信息化 | 2 | 1 | 3 |
| 福建信息化 | 1 | 1 | 3 |
| 广东信息化 | 3 | 2 | 1 |
| 湖南信息化 | 1 | 2 | 3 |
| 综合 | 12 | 10 | 22 |
| 重要程度 | 1 | 1 | 2 |

在本次扫描器测试环境中，设置了 2 台装有 SQL Server 2000 的机器，其中一台未打补丁，而另一台打上 sp3a；还有 2 台装有 oracle 的机器，使用的版本分别是 8.1.7 和 9.0.1。可见基本满足了反馈的结果要求。鉴于反馈结果中两种数据库在使用上没有太大的差异，故二者采用相同的权重。

### 3.1.4 现网应用服务器的使用情况

表 4 对于服务器使用情况的调查结果

| 反馈单位 | IIS | Apache | Lotus | Exchange | 其它 |
|---|---|---|---|---|---|
| 北京移动 | 1 | 3 | 4 | 2 | 5 |
| 广东移动 | 1 | 2 | 3 | 4 | 5 |
| 江苏移动 | 2 | 1 | 3 | 4 | 5 |
| 网络部 | 2 | 3 | 5 | 5 | *1 |
| 北京信息化 | 2 | 4 | 5 | 3 | 1 |
| 福建信息化 | 5 | 2 | 1 | 5 | *3 |
| 广东信息化 | 1 | 4 | 1 | 3 | 5 |
| 湖南信息化 | 1 | 3 | 4 | 2 | 5 |
| 综合 | 15 | 22 | 26 | 28 | 30 |
| 重要程度 | 1 | 2 | 3 | 3 | 3 |

对于上述的表格所显示的内容，我们在最终评分中也进行了充分的考虑。由于中国移动网上所开展的服务十分复杂，而对于每一种服务而言，都具有不同程度的漏洞，因此面对复杂的网络环境和复杂的应用环境，我们只能平权对待。从上表可知，对于 WEB 服务而言不论 IIS 还是 Apache 都是需要特别关注的，因此在评分的权重上有关 WEB 服务的项目适当的提高了权重。

### 3.1.5 对扫描器输出结果详细程度的需求

表 5 对扫描结果的详细程度的需求分析

| 反馈单位 | 指出漏洞 | 提供分析图表 | 提出解决方案 | 其它 |
|---|---|---|---|---|
| 北京移动 | 1 | 2 | 3 | 无 |
| 广东移动 | 1 | 2 | 3 | 风险级别 |
| 江苏移动 | 1 | 3 | 2 | 无 |
| 网络部 | 1 | 3 | 2 | 无 |
| 北京信息化 | 2 | 3 | 1 | 无 |
| 福建信息化 | 1 | 3 | 2 | 无 |
| 广东信息化 | 2 | 3 | 1 | 无 |
| 湖南信息化 | 2 | 3 | 1 | * |
| 综合 | 15 | 22 | 15 | ** |
| 重要程度 | 1 | 2 | 1 | *** |

注：*要求结果中文化，解决方案可操作性强，能够扫描系统的开放端口和服务

**此处无法综合

***重要度为 2

通过上述表格分析得到以下结论：各级的安全管理人员对于能否

正确地判断漏洞和详尽地给出切实可靠的解决方案很重视。同时在表格的第五列我们发现中文化、风险级别的标定、解决方案的可操作性、对端口和开放服务的鉴别能力都具有比较重要的地位，因此评分时将将适当提高它们的权重。

### 3.1.6 对扫描器日志和审计功能的需求

表 6 对于日志和审计功能的需求分析

| 反馈单位 | 日志功能 | 审计功能 | 对审计对象的需求 |
|---|---|---|---|
| 北京移动 | 是 | 是 | 对操作 |
| 广东移动 | 是 | 无 | 无 |
| 江苏移动 | 是（不高） | 是 | * |
| 网络部 | 是 | 是 | 对登陆者，时间 |
| 北京信息化 | 是 | 是 | 日志，安全状况 |
| 福建信息化 | 是 | 是 | 所有细节 |
| 广东信息化 | 是 | 是 | 登陆、进程、配置 |
| 湖南信息化 | 是 | 无 | 无 |
| 综合 | 是 | 基本是 | ** |
| **重要程度** | 重要 | 一般 | *** |

注：*系统账号口令　SNMP　数据库账号口令　　中间件　　系统服务审计

**无法综合

***视具体选项而定

通过分析上述表格，可以得到如下结果：

1. 所有单位均十分看重日志功能，所以对有关日志部分功能打分的时候将适当提高权重。
2. 对于审计功能大多数肯定了其必要性，从安全的角度上，这一项也是比较重要的，故可将其权重设为略低于日志功能。
3. 对于审计的要求，各单位给出了不完全相同的侧重点，相似的地方是对于登陆及其配置动作的审计都比较重视。因此将在审计功能项的诸多测试项中提高这两项的权重。

### 3.1.7 对于扫描器自身的安全需求分析

表 7 对于扫描器自身的安全需求分析

| 反馈单位 | 本身的安全 |
|---|---|
| 北京移动 | 认证、扫描范围限制 |
| 广东移动 | 无 |
| 江苏移动 | 扫描范围、强度、攻击类型的控制 |
| 网络部 | 扫描范围、登陆认证 |

| | |
|---|---|
| 北京信息化 | *扫描的攻击及应用类型，扫描的范围 |
| 福建信息化 | 安全扫描，密码保护、认证、扫描范围 |
| 广东信息化 | 密码保护，认证，扫描范围 |
| 湖南信息化 | 用户管理，扫描范围、扫描强度 |
| 综合 | 扫描范围和认证 |
| 重要程度 | ** |

注：*由原文归纳出的结果

**重要度顺序：范围限定、认证、攻击类型和强度限制、密码保护、安全扫描、用户管理。

经过分析可知各单位一致认为对扫描范围的限制是最重要的，其余的顺序如**所示。权重的设定将与此一致。

### 3.1.8 对扫描器使用频率的需求

表 8 扫描器的使用频率

| 反馈单位 | 使用频率 |
|---|---|
| 北京移动 | 一周数次 |
| 广东移动 | 两周一次 |
| 江苏移动 | 一周一次 |
| 网络部 | 一周 2-3 次 |
| 北京信息化 | 两周一次 |
| 福建信息化 | 四周一次 |
| 广东信息化 | 一周七次 |
| 湖南信息化 | 一周一次 |
| 平均 | 每周一次左右 |

由于各单位的扫描器使用频率不统一，所以按每周至少一次的扫描频率考虑问题比较合理，这就要求扫描器的漏洞库更新速度至少是每周一次。相对而言，更新速度较快、性能较高的扫描器应略有优势；能够对于新发现的漏洞提供及时通知的扫描器产品较优（这部分将体现为主观评判）。

对于共享媒体的使用情况就不一一列举结果了，总之目前仍有部分单位使用共享媒体设备。由于扫描器的身份验证信息需要通过以太网进行传输，所以要求扫描起做好认证信息的保护工作，对于单机版的不向外发送认证信息的产品或者只进行本地认证的扫描器产品，应对本地密码文件作合理的保密性、完整性检验。此部分的权重略有提高。

江苏移动认为扫描器输出格式应该标准化或者是开放的，便于以后与安全资产系统、安全管理系统集成。同时漏洞信息应尽量统一，如果有 CVE 号首先应提供 CVE 号。

集团公司网络部认为扫描器最重要的几点特征包括：

- 扫描地址的可管理性，这样下达扫描任务就可根据业务系统直接下达；
- 扫描结果的可管理性，能否将相同业务系统不同时间的扫描结果进行比较；
- 扫描器用户的可管理性，能否给用户分配不同的权限，扫描地址范围等；
- 漏洞解决方案的可读性，漏洞解决方案是否对系统管理员清晰可读并且有比较好的可操作性；
- 漏洞更新的及时性，厂家是否维护自己的漏洞库，以保证能够及时更新；
- 扫描参数的配置灵活性，是否可以自由配置各种参数，定制例如线程数、漏洞模板，扫描时间等等。

北京信息化希望扫描器能提供自动在线更新功能。

福建信息化认为扫描器进行扫描时不能对网络性能及应用程序产生明显的影响，而且扫描后产生的漏洞报表必须包含可操作的修复建议。

湖南信息化认为好的产品应该能提供远程网上升级功能并占用较少得系统资源，可以多线程扫描且可以制定计划任务进行定期扫描。

## 3.2 扫描器测试的评分规则

根据上一节对调研函反馈结果的分析，我们得出了本次测试的评分规则。请详细参见附录 B。

# 4 测试平台

## 4.1 网络扫描器测试平台拓扑结构

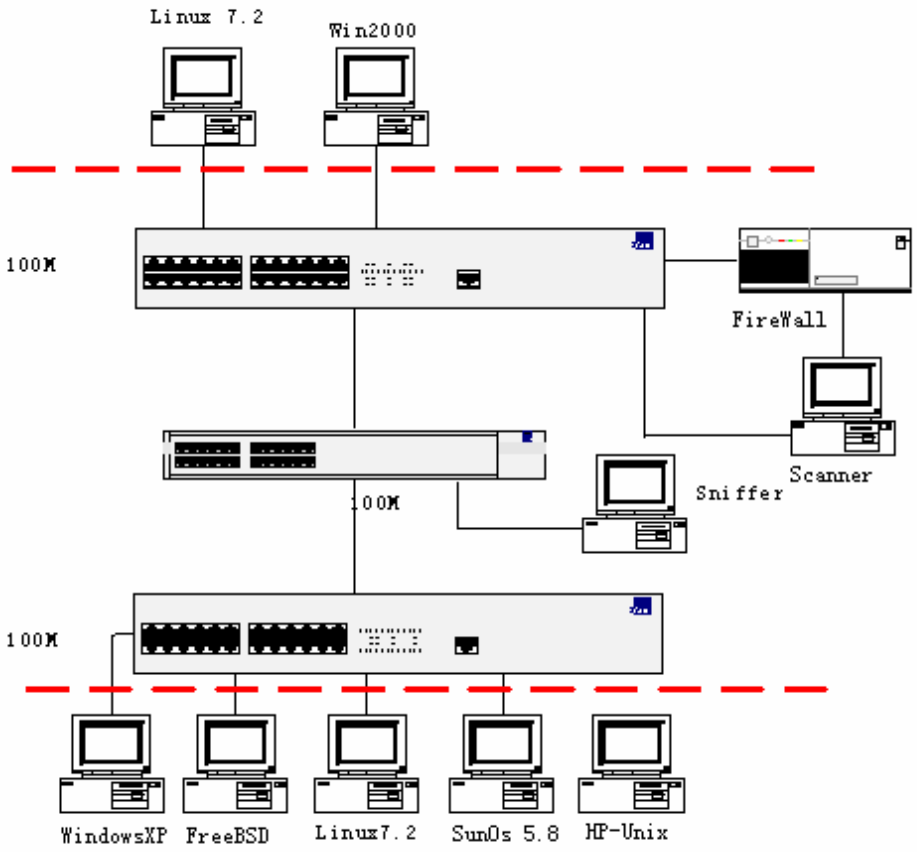


图1 测试平台拓扑图

## 4.2 网络扫描器测试平台硬件配置

**主机配置：**

1、PC 机：

a）IBM 台式机 4 台 P4-3.2G 内存 512M 硬盘 60G 网卡 10/1000M

b）IBM 台式机 4 台 P4-2.6G 内存 256M 硬盘 60G 网卡 10/1000M

c）IBM ThinkPad T30 笔记本

2、SUN 工作站： 1 台 双硬盘

3、HP 工作站： 1 台 双硬盘

**网络配置：**

1、交换机：

a）Cisco Catalyst 2950 1 台
b）3Com 交换机 1 台

2、防火墙：
远东防火墙 2000 系列 One-Up 1 台

## 4.3 网络扫描器测试平台软件配置

在测试中涉及到的操作系统包括：

| | |
|---|---|
| 1、Windows 2k Server | standard |
| | sp3 |
| | sp4 |
| 2、Windows XP | sp1 |
| 3、SunOS 5.8 | 有补丁 |
| | 无补丁 |
| 4、HP-Unix 11.11 | 有补丁 |
| | 无补丁 |
| 5、FreeBSD 5.2.1 | |
| 6、Linux 2.4.7-10(redhat 7.2) | 有补丁 |
| | 无补丁 |

在测试中涉及到的应用程序包括：
如：OpenSSH,Finger,IIS,Apache,Lotus Domino,SQL Server,Oracle 等

# 5 网络扫描器参测产品

| 序号 | 公司名称 | 产品名称 | 产品型号 | 版本号 |
|---|---|---|---|---|
| 1 | 安氏 | 领信网络扫描器（LinkTrust Network Scanner） | S-N-idsbox2.0 | 1.5 |
| 2 | 冠群金辰 | 承影漏洞扫描器 | NetworkDefender-100 | 1.5 |
| 3 | 亿阳信通 | 亿阳网警 Scanner | IDS4235,IDS4250 | 1.5 |
| 4 | 赛门铁克 | Symantec NetRecon | V2.0.0.15 | 3.6 |
| 5 | 中联绿盟 | Aurora－3 | GJ-MIDS-A | 3.0 |
| 6 | 启明星辰 | 天镜脆弱性扫描与管理系统 | V2.5 100M | 6.0 |

| | | | | |
|---|---|---|---|---|
| 7 | 中软国际 | ISS Internet Scanner | N500 | 7.0 |

# 6 功能特性测试

本项测试旨在评估扫描产品的各项具体功能，考察产品结构，部署方式，事件处理能力，数据管理能力，报表详细程度，与其他系统的互动性以及安装手册和用户手册的可读性等。具体包括下列内容：

## 6.1 部署和管理能力的测试

本项测试旨在评估测试系统安装过程是否简易，是否需要安装第三方软件，安装后是否对原系统造成不良影响以及其基本构成是否与厂家提供的说明信息一致。测试结果参见附表 A1。

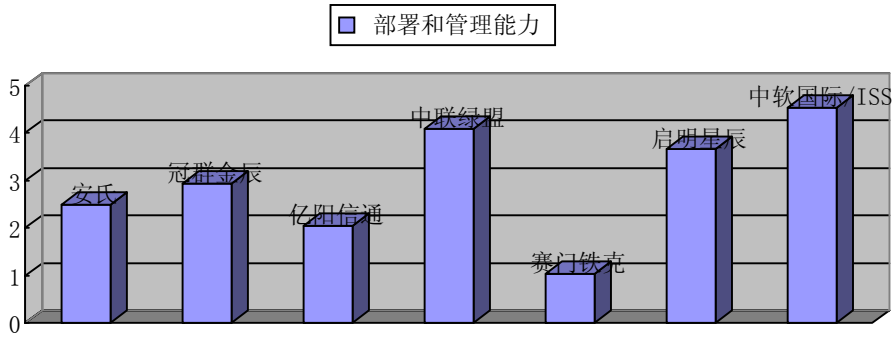


图2 各个受测产品本项测试结果得分对比

## 6.2 系统升级能力测试

随着系统漏洞的不断被发现，扫描系统也必须保持足够的升级和更新能力。主要包括软件版本的升级和特征库的更新，尤其特征库的及时更新非常重要。本项测试旨在评估测试系统升级的方式及手段是否方便、多样、系统是否支持在线升级，升级过程过程是否安全（是否实现身份认证，是否进行加密，升级过程中是否可能安装其它应用程序）。测试结果参见附表 A2。

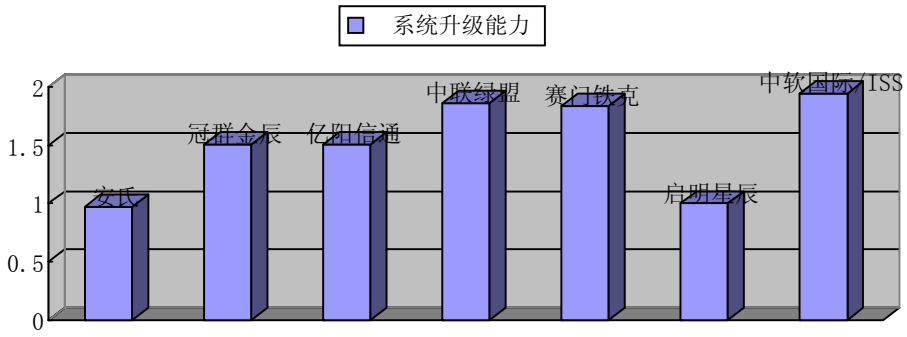


图3 各个受测产品本项测试结果得分对比

## 6.3 系统配置测试

针对不同的扫描目标以及不同的测试目的，用户需要对系统按照自己的需求进行配置，本测试的目的是判断该扫描系统是否能够为用户提供适当的配置选择能力。部分配置功能，比如扫描策略的配置、文档模版的配置在其它测试项目中测试。测试结果参见附表 A3。

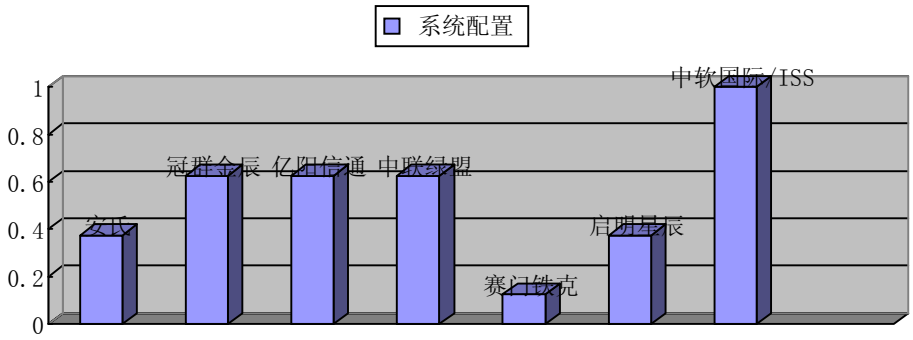


图4 各个受测产品本项测试结果得分对比

## 6.4 扫描策略定制能力测试

扫描策略的定制是指用户能够根据需要自主选择要测试的安全漏洞，并能够将所需测试的漏洞列表保存成某种形式的扫描策略，以后只需选择该扫描策略就可以扫描该策略指定的所有漏洞。本测试的目的是比较各个受测试的扫描系统是否提供定制扫描策略的功能，扫描策略的定制是否方便，分类是否足够详细。测试结果参见附表 A4。

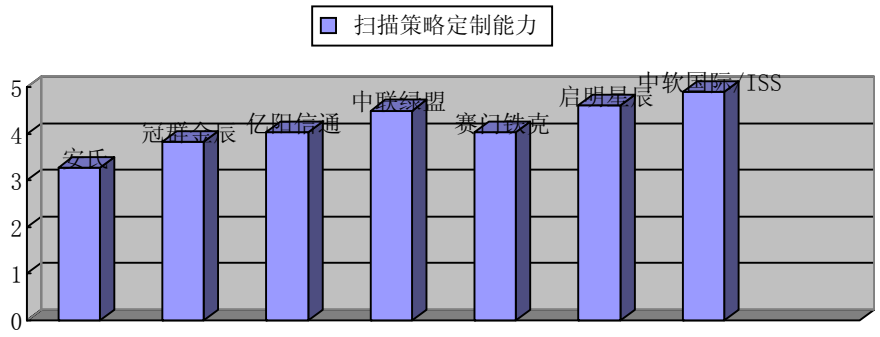


图5 各个受测产品本项测试结果得分对比

## 6.5 信息收集能力测试

收集目标主机信息是扫描系统必须具备的一项基础功能，系统在实施扫描时可以根据获得的信息实现职能化的扫描。比如系统必须能够收集目标主机的名称、IP 地址、打开的端口、过滤的端口、端口上提供的服务、SNMP 协议提供的信息、是否能够 PING 通、路由信息等等，这些信息一方面有助于管理人员充分了解系统的概貌，也有助于扫描系统实现快速的扫描。本项测试旨在评估扫描器产品的信息收集能力，测试结果参见附表 A5。

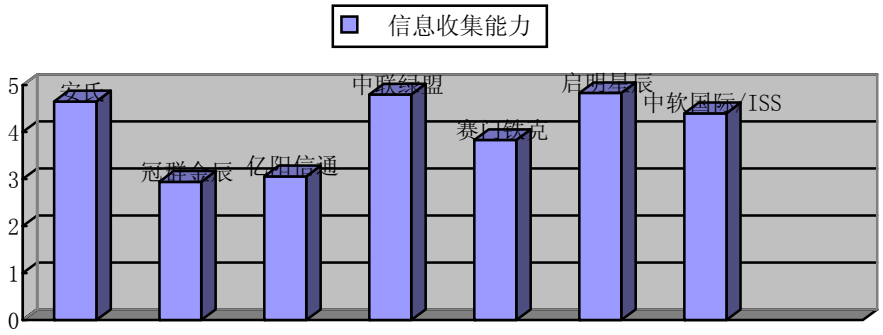


图6 各个受测产品本项测试结果得分对比

## 6.6 扫描文档和报表

对扫描结果进行分析之后提供的扫描报告，是一个扫描产品与用户之间交互的最为重要的接口。一个扫描产品是否能够正确的、有效的生成详细的、易于理解的报告是衡量一个扫描产品是否合格、是否具有友好用户

接口的重要技术指标。本测试规范从以下几个角度衡量扫描产品的这一指标：

- 报告的详细程度。测试扫描结果的报告是否包括详细的漏洞描述、修复漏洞的方法、漏洞的风险程度等等。
- 综合分析的能力。测试扫描结果报告是否具有综合分析能力，是否提供合格的统计分析报告，是否能够以图表方式直观地显示整个网络系统的安全概貌，是否能够分析不同系统安全问题之间的关联性。
- 分析的正确性。测试其分析结果是否正确。

### 6.6.1 生成扫描文档、报表的灵活程度测试

在扫描结束后，用户是否能够灵活地组织其希望生成的报告。测试结果参见附表 A6.1。

### 6.6.2 报表信息完善程度和正确性测试

评估扫描文档和报表信息的完善程度和正确程度。测试结果参见附表 A6.2。

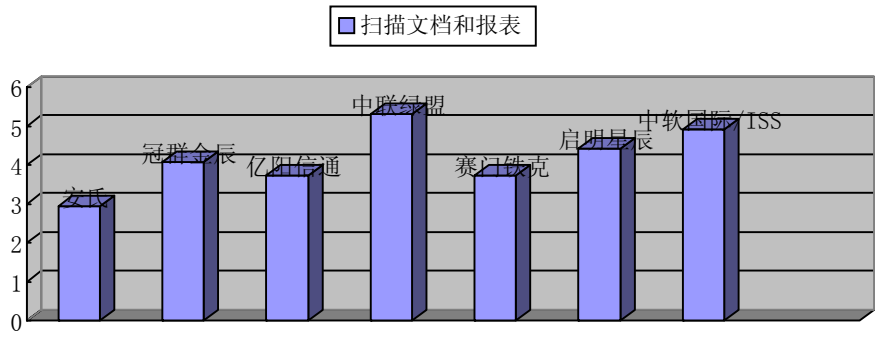


图7 各个受测产品本项测试结果得分对比

## 6.7 系统日志、审计功能与系统的安全策略

网络安全漏洞扫描产品应为下列事件生成审计记录：

- 审计功能的开启和关闭；
- 任何读取、修改和破坏审计数据的尝试；
- 任何鉴别机制的启用；
- 所有启用鉴别机制的请求；
- 任何对系统配置参数的修改（设置和更新），无论成功与否。

网络安全漏洞扫描产品应确保只有被授权的管理员才能读取、修改或

删除审计数据。

当审计记录占用的存储空间达到规定的存储空间阈值时，应能自动删除部分旧的日志记录，以保证审计功能的正常运行。

### 6.7.1 系统的日志、审计功能

应该对产品使用者的动作（包括登录、扫描分析等）产生并提供详尽的系统日志和审计记录，以方便用户对系统进行审计分析。这些文档应该尽量全面和友好。测试结果参见附表 A7.1。

### 6.7.2 系统的安全策略

扫描系统自身的安全策略十分重要，保护扫描器不被未经授权用户使用和不能扫描未经授权的目标是对产品的一个基本的要求。测试结果参见附表 A7.2。

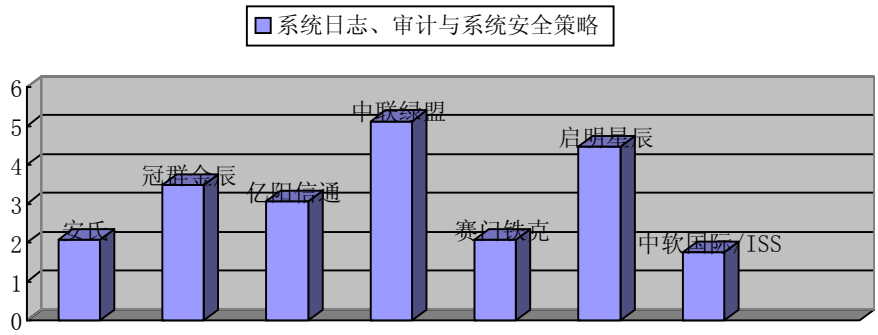


图8 各个受测产品本项测试结果得分对比

## 6.8 系统的互动性

网络安全漏洞扫描产品应能与防火墙产品通过标准的接口共享扫描信息，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。

网络安全漏洞扫描产品应能与防病毒产品以标准的接口共享扫描结果数据，以增强网络的防病毒能力。增强级网络安全漏洞扫描产品应可将扫描得到的病毒信息通知防病毒产品，使防病毒产品立即启动相应的杀毒程序进行查杀病毒操作。

网络安全漏洞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，可为其它类型安全产品开发相应的模块，达到与网络安全漏洞扫描产品进行互动的目的。对该项测试得到的结果参见附表A8。

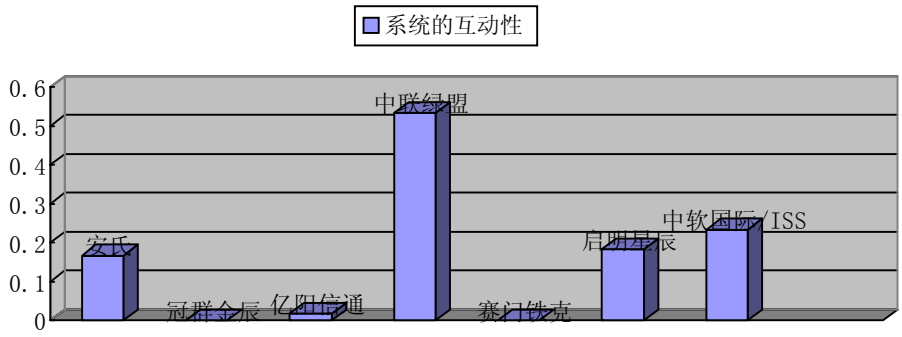


图9 各个受测产品本项测试结果得分对比

## 6.9 文档和手册

为了正确地部署扫描器系统以及正确地使用和维护，一个合格的扫描器产品应该提供详尽的文档。对该项测试得到的结果参见附表 A9。

## 6.10 功能特性测试汇总

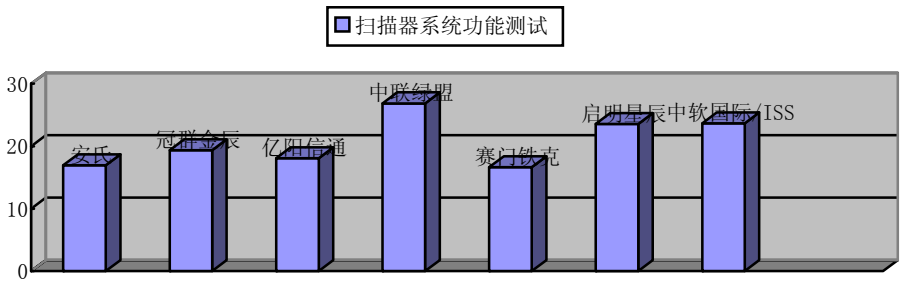


图 10 扫描器系统功能测试汇总

# 7 漏洞扫描能力测试

本项测试旨在评估扫描产品的扫描漏洞能力，考察产品可信性，对目标机脆弱性的扫描能力以及扫描器的智能化等。具体包括下列内容：

## 7.1 漏报率测试

这项测试的目标主要是评测扫描器产品扫描结果的全面性，即评估扫描器扫描出的漏洞集合相对于目标系统已知漏洞集合的覆盖能力，通过测试能够判断受测产品所能扫描出的操作系统类型、网络设备类型。首先对预先设计的网络环境和系统环境进行分析，然后比对受测产品的扫描结果，得出扫描产品的漏报率。

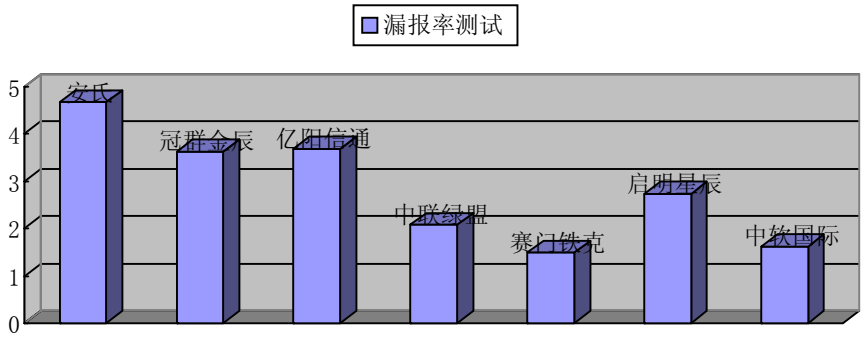


图11 各个受测产品本项测试结果得分对比

## 7.2 误报率测试

产品设计、开发以及不恰当操作等原因都可能导致扫描器对测试环境中并不存在的漏洞给出错误报警。这种虚假报警不仅增大了分析人员的工作量，而且对评估系统安全造成误导，因此对产品进行误报率测试是非常有必要的。对预先已经安装了安全补丁的系统实施扫描，通过分析扫描结果，可以判断该安全扫描产品是否会产生误报，并可以计算出误报率。

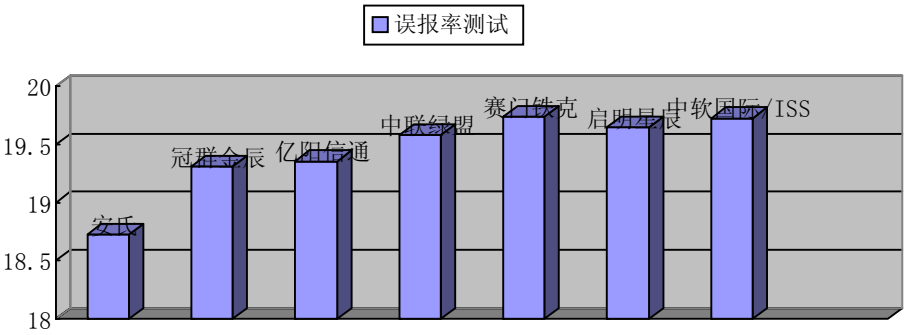


图12 各个受测产品本项测试结果得分对比

## 7.3 系统脆弱性发现能力测试

系统脆弱性测试是为了测试扫描系统是否能发现系统配置上的弱点（如弱口令、配置错误、危险配置等），以及是否能提出相关安全建议。测试结果参见附表 A10。

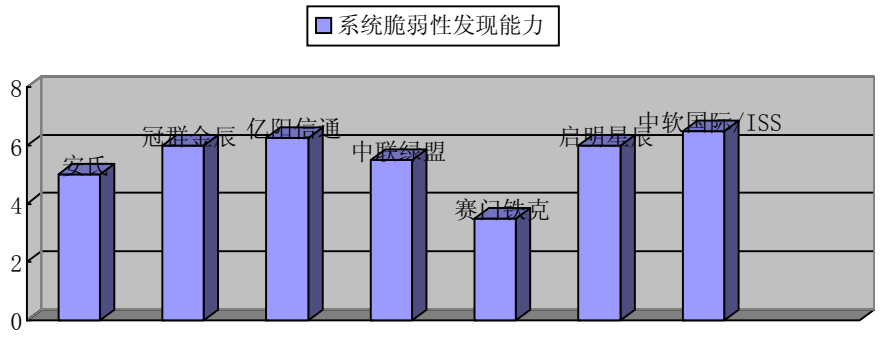


图13 各个受测产品本项测试结果得分对比

## 7.4 系统智能化程度测试

扫描系统的智能化程度测试是为了测试扫描系统是否能够利用已获得的信息智能缩小扫描的范围、是否能够对获得的信息进行综合分析等。事实上，一个扫描系统的智能化程度从一定程度上影响着该扫描系统的其它指标（包括扫描速度、误报率和漏报率等）。对该项目的测试结果参见附表 A11。

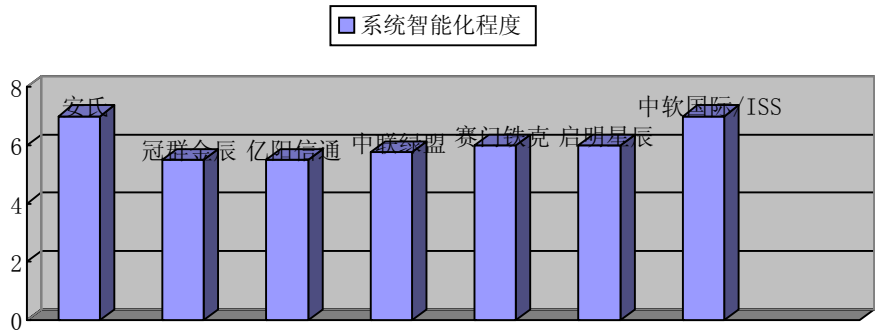


图14 各个受测产品本项测试结果得分对比

## 7.5 漏洞扫描能力测试汇总

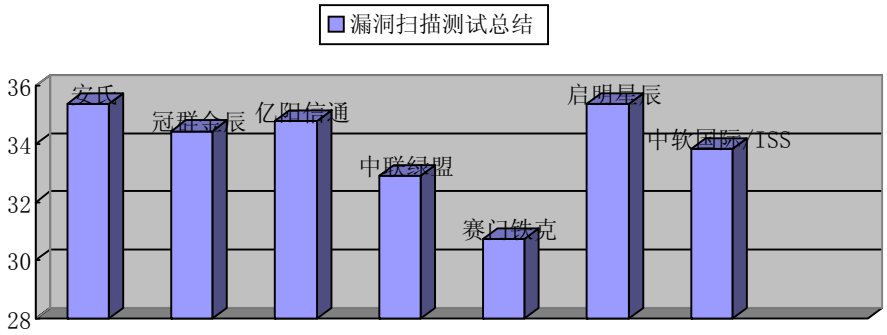


图15　扫描器扫描能力测试汇总

# 8　性能测试

本项测试旨在评估扫描产品的各项性能，考察产品扫描速度、占用带宽及其本身的稳定性等。具体包括下列内容：

## 8.1 扫描速度测试

这一测试的目的，是以量化的方式比较不同扫描系统的扫描速度。为了能够以一种公平的方式比较不同系统的扫描速度，就必须保证在测试过程中对各个受测扫描系统所做的操作是一致的；而且还必须要求扫描达到的效果也基本一致，比如要求两个扫描系统扫描 1 至 65535 号端口，如果一个扫描系统使用了多种扫描技术探测得到较好的扫描结果，那么它可能会花费大量的时间，而另一种扫描系统只是做了最为简单的探测，因此它可能花费的时间较少，但效果较差。

因此，在对扫描系统的扫描速度进行测试时，一方面要求测试环境必须一致如扫描的目标、漏洞数目、端口数目等等，另一方面在评估测试结果的时候还必须要把受测产品采用何种实现技术考虑在内。测试结果参见附表 A12。

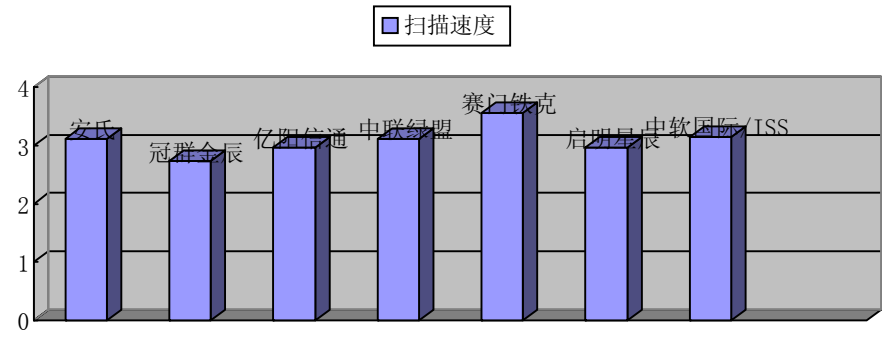


图16 各个受测产品本项测试结果得分对比

## 8.2 扫描系统资源开销

在各厂家技术人员对扫描器做出性能最好、扫描结果最佳的前提下执行该测试项，评定扫描系统运行所需要的资源开销，包括发起扫描主机的CPU、内存和网络带宽占用情况。测试结果参见附表 A13。

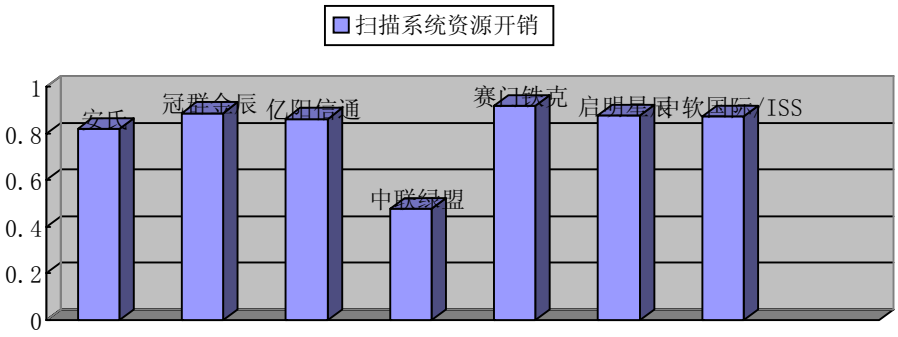


图17 各个受测产品本项测试结果得分对比

## 8.3 稳定性测试

这一测试项的目的是测试扫描系统自身运行是否稳定、错误处理机制是否完善、是否能够正确处理资源耗尽问题。测试结果参见附表 A14。

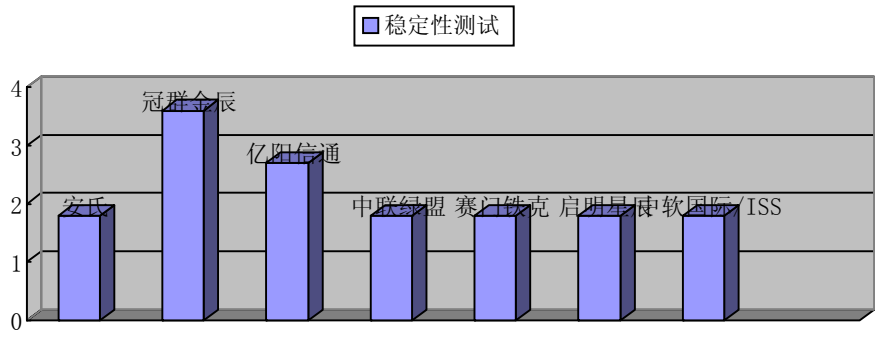


图18 各个受测产品本项测试结果得分对比

## 8.4 性能测试汇总

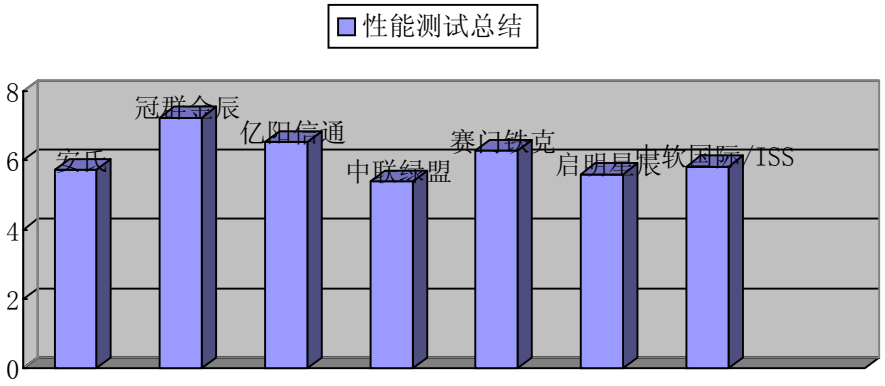


图19 扫描器性能测试汇总

# 9 其它测试项目

## 9.1 增补的客观测试项目

该测试项旨在对扫描系统工作过程中是否引起目标主机的宕机，扫描产品的管理器与扫描引擎之间通信是否稳定做出测评。测评结果见附表A15.1。

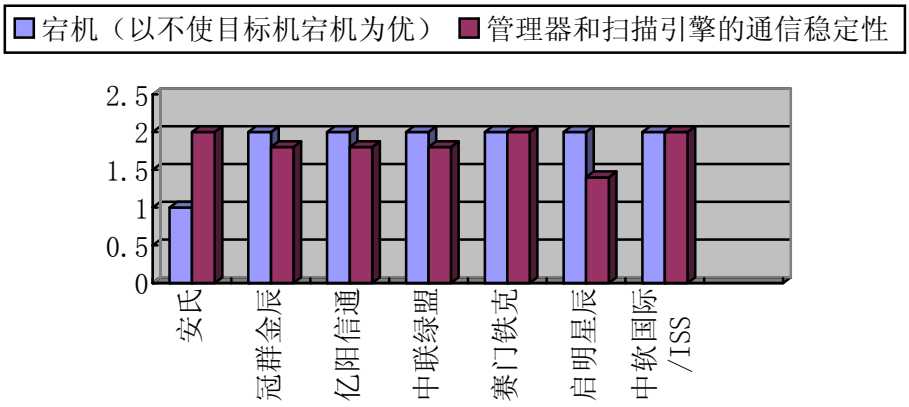


图20　增补客观项目评测结果

## 9.2 增补的主观测试项目

该测试项的主要目的是为了评测厂家技术支持人员对送测设备的操作是否熟悉，对相关技术问题是否能够正确解答，以及是否能够及时、正确地响应测试中的突发故障做出评估；另外，受测厂家技术人员对测试的认真程度也将影响评测结果。测评结果见附表 A15.2。

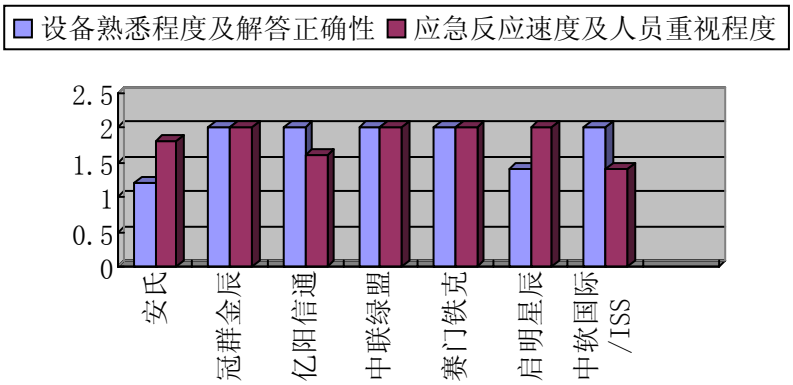


图21　增补主观项目评测结果

# 10 各项评分汇总

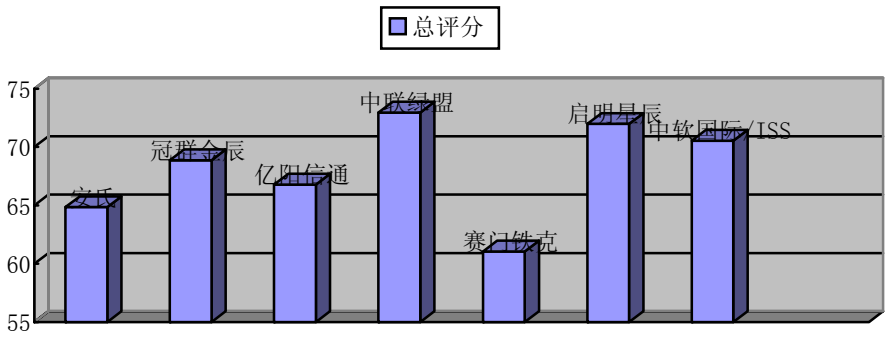


图22 扫描器各项评分汇总

# 附录 A 测试结果数据附表

附表 A1 部署和管理测试结果

| 测试项目 | Nessus | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|---|
| 是否为中文界面 | 否 | 是 | 是 | 是 | 是 | 否 | 是 | 否 | 1 |
| 安装过程中是否需要用户安装第三方软件 | 否 | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 安装的第三方软件名 | | winpcap | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 管理器和扫描组件是否可以分离 | 是 | 是 | 否 | 否 | 是 | 否 | 是 | 是 | 1 |
| 是否需要在测试目标系统上安装软件 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 各组件是否可以单独安装在不同机器上 | 是 | 否 | 是 | 否 | 是 | 否 | 是 | 是 | 1 |
| 一个管理器是否可以控制多个扫描组件 | 是 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 如果支持多个组件，是否可以在管理器上正确显示所有扫描组件 | | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 1 |
| 一个扫描引擎是否可以同时被多个管理器管理 | | 否 | 否 | 否 | 否 | 是 | 否 | 是 | 是 | 1 |
| 如果被管理器可以多个管理器管理，主、辅管理器对各组件控制的能力是否有明确的区别 | | 否 | 否 | 否 | 否 | 是 | 否 | 是 | 是 | 1 |
| 扫描器更新是否通过管理器 | | 是 | 是 | 否 | 是 | 是 | 是 | 否 | 是 | 1 |
| 系统支持是否管理员认证 | | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 2 |
| 采用的认证方式 | 用户名/口令 | 是 | 否 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| | 证书 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| | 其它 | 否 | 1 | 否 | 否 | 否 | 1 | 1 | 1 | 0.5 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 系统是否支持多用户管理 | 否 | 否 | 是 | 否 | 是 | 否 | 是 | 是 | 2 |
| 用户权限可以分级 | 否 | 否 | 是 | 是 | 是 | 否 | 是 | 是 | 2 |
| 用户权限是否更改可以实时生效 | 否 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 1 |

附表 A2 系统升级能力测试结果

| 测试项目 | | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|---|
| 是否支持在线升级 | | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 1.5 |
| 是否支持自动升级 | | 否 | 是 | 是 | 是 | 是 | 否 | 是 | 1.5 |
| 是否支持非在线升级 | | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 升级过程是否加密 | | 否(数字签名) | 否 | 否 | 是 | 是 | 是 | 是 | 2 |
| 所采用的加密算法 | 算法名称 | 否 | 否 | 否 | RC4<br>RSA | AES | RSA<br>RC6 | AES | 1 |
| | 密钥长度 | 否 | 否 | 否 | 128<br>128 | 256 | 1024/128 | 256 | 1 |
| 扫描系统是否提供对升级网站的实施身份认证 | | 否 | 是 | 是 | 是 | 是 | 否 | 是 | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 扫描系统是否对提供的升级文件进行数字签名鉴别 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 2 |
| 升级完成后能否按照先前的策略运行 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 升级后是否能够发现最新公布的安全漏洞 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 升级过程中是否植入了新的应用程序 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 平均升级间隔时间（天） | 0.8 | 0.9 | 0.9 | 0.8 | 0.6 | 0.5 | 0.8 | 1 |
| 平均每次更新漏洞数 | 0.95 | 0.9 | 0.9 | 不祥 | 0.95 | 不祥 | 0.7 | 1 |

附表 A3 系统配置能力测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 是否允许配置只扫描能够 PING 通的网站 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否允许配置扫描线（进）程数 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 是否允许配置扫描项间隔时间 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 是否允许配置网络超时时间 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 是否支持扫描预通知功能 | 否 | 是 | 是 | 是 | 否 | 否 | 是 | 1 |
| 是否可关闭扫描预通知 | 否 | 是 | 是 | 是 | 否 | 否 | 是 | 1 |
| 是否允许对扫描预通知设置 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 1 |
| 是否可设置通知内容 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 1 |

附表 A4 扫描策略定制能力测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 扫描特征库是否分类 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否能显示扫描特征的数量 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否对每个特征有注释说明 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | |
| 是否容易关闭一个特征 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否容易启用一个特征 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否可以对特征参数进行调节 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 特征参数是否可以容易地恢复为缺省值 | 是 | 否 | 否 | 是 | 否 | 否 | 否 | 1 |
| 是否支持定制扫描策略 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 缺省的扫描策略有哪几种 | 0.5 | 0.25 | 0.25 | 0.25 | 0.25 | 0.5 | 0.5 | 1 |
| 是否支持漏洞筛选 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 用于风险筛选程度 | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 1 |
| 漏洞操作的条件有系统类型 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 哪几种 | 应用类型 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | 入侵技术类型 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | 端口列表号 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 1 |
| | 其它 | 0 | 0.5 | 否 | 否 | 否 | 0.1 | 0.2 | 1 |
| 是否种定略 | 能用多组合策条件扫描制 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否独漏洞 | 能够单选择扫描列表 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否描合 | 支持扫策略的组 | 否 | 否 | 否 | 是 | 是 | 是 | 是 | 1 |
| 支持扫策略的组合条件 | 与 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 1 |
| | 或 | 否 | 否 | 否 | 否 | 是 | 是 | 是 | 1 |
| | 非 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| | 其它 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 策略组的选参数 | 扫描目标 | 否 | 否 | 否 | 是 | 否 | 是 | 否 | 1 |
| | 扫描策略 | 否 | 否 | 否 | 是 | 是 | 是 | 否 | 1 |
| | 其它 | 否 | 否 | 否 | 否 | 否 | 否 | 1 | 1 |
| 是否描出和 | 支持扫策略的导入 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 1 |
| 扫否允扫 | 描策略指定许描目标 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 能够指定 | 指定IP地址 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 指定扫描目标的参数 | 指定IP网段 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | 指定多个IP网段 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | 指定多个IP网段和地址关相掩码 | 是 | 是 | 是 | 是 | 是 | 否 | 否 | 1 |
| | 指定多 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 个IP网段中的特定地址 | | | | | | | |
| | 指定端口 | 是 | 否 | 否 | 是 | 是 | 是 | 是 | 1 |
| | 指定端口范围 | 是 | 否 | 否 | 是 | 否 | 是 | 是 | 1 |
| | 其它 | 否 | 1 | 1 | 1 | 1 | 否 | 1 | 1 |
| 是否提供目标地址管理功能 | | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 是否支持在指定时间自动启动扫描 | | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1.5 |
| 是否支持间隔一定时间自动扫描 | | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1.5 |
| 是否能使用目标系统的已知账号/口令对其进行更有效的扫描 | | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 使用对话框输入用户名/口令 | | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 使用用户名/口令文件 | | 否 | 否 | 是 | 否 | 是 | 是 | 是 | 1 |
| 使用用户名/口令数据库 | | 否 | 否 | 是 | 否 | 否 | 否 | 是 | 1 |
| 可使用多少个用户名/口令组合 | | 0.1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 1 |

附表 A5 信息收集能力测试结果

| 测试项目 | | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|---|
| 正确分析出目标系统的操作系统类型 | Windows 2000 Server | 是 | 是 | 是 | 0.8 | 是 | 是 | 否 | 1.5 |
| | Windows XP | | | | | 否 | 是 | 是 | 1.5 |
| | redhat Linux | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | Solaris | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | HP-UX | | | | | | | | 1 |
| | FreeBSD | | | | 是 | 是 | 是 | 是 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 正确分析出目标系统的操作系统版本 | windows 2000 Server | 是 | 否 | 否 | 否 | 是 | 是 | 是 | 1.5 |
| | Win XP | | | | | 否 | 是 | 是 | 1.5 |
| | redhat Linux | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 1 |
| | Solaris | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | HP-UX | | | | | | | | 1 |
| | FreeBSD | | | | 否 | 否 | 否 | 否 | 1 |
| 是否能够正确地探测目标系统是否能够PING通 | | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否能够正确探测目标系统上所有打开的TCP端口 | | 是 | 否 | 是 | 是 | 否 | 是 | 是 | 1 |
| 未探测到的TCP端口 | | 否 | 1 | 否 | 否 | 0.1 | 否 | 否 | -1 |
| 是否能够正确探测目标系统上所有打开的UDP端口 | | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 1 |
| 未探测到的UDP端口 | | 0.9 | 1 | 1 | 否 | 0.1 | 0.3 | 0.1 | 1 |
| 是否能够发现被防火墙过滤的端口 | | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 未发现的被过滤的端口 | | 0.3 | 否 | 否 | 否 | 否 | 否 | 否 | -1 |
| 是否能够正确探测出各个端口上运行的服务器名称，比如对于WEB服务是否能够探测出该WEB服务器是IIS还是APACHE。 | | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 收集到的SNMP提供的信息是否包含Solarwind扫描得到的所有信息 | | 是 | 否 | 否 | 是 | 否 | 否 | 否 | 1 |
| 未探测到但Solarwind包含的信息 | | | 0.5 | 0.5 | 无 | 0.2 | 否 | 0.5 | -1 |
| 收集到的RPC服务名称、端口、版本号是否正确 | | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 未收集到的RPC服务信息 | | 0 | 0 | 0 | 0 | 0 | 0.5 | 0.5 | -2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 是否能够正确分析出网络的拓扑结构和路由表 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 是否能够获得nbtscan获得的所有netbios信息 | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 1 |
| 未能获取的netbios信息 | 否 | 0.25 | 0.75 | 否 | 否 | 否 | 否 | -1 |
| 是否能够正确获得各个IP地址对应的MAC地址 | 是 | 否 | 否 | 是 | 是 | 否 | 否 | 1 |
| 未获取到的MAC地址信息 | 否 | 否 | 否 | 否 | 否 | 否 | 0.5 | -1 |
| 是否能够正确探测出www.somesite.com的域名 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 是否能够探测出与该www.somesite.com相关的DNS记录（MX记录等） | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 2 |
| 是否能够探测出ftp.somesite.com和pop3.somesite.com这两个域名 | 是 | 是 | 是 | 否 | 是 | 否 | 是 | -2 |
| 是否能够利用探测到的用户名和口令从WINDOWS的LDAP服务中扫描获得信息，获得的信息与用ldp获得的信息是否一样多。 | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 是否能够利用finger服务获得目标主机上的用户信息 | 是 | 是 | 是 | 是 | 0.5 | 是 | 是 | 1 |

附表 A6.1 扫描文档、报表的生产灵活程度测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 扫描结果能否写入数据库 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 可对结果数据库执行导入操作 | 否 | 是 | 是 | 否 | 否 | 是 | 否 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 可以对结果数据库执行导出操作 | 否 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 是否支持不同的用户类型 | 否 | 否 | 否 | 是 | 是 | 是 | 是 | 1 |
| 根据设定的条件生成不同的报告 | 否 | 否 | 否 | 是 | 是 | 否 | 是 | 1 |
| | 否 | 否 | 否 | 是 | 是 | 是 | 是 | 1 |
| 是否可以自由控制在报告中包含哪些内容 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 可以自由控制在报告中包含哪些内容 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 1 |
| | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 1 |
| | 否 | 是 | 是 | 是 | 是 | 否 | 是 | 1 |
| | 否 | 是 | 是 | 是 | 是 | 否 | 是 | 1 |
| | 0 | 0.2 | 0.1 | 1 | 0 | 0 | 0.1 | 1 |
| 是否可以组合多种条件决定在生成的报告中包含哪些漏洞 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 允许漏洞风险 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 组合使用的漏洞条件 | 操作系统相关的漏洞 | 否 | 是 | 否 | 是 | 否 | 否 | 是 | 1 |
| | 漏洞类型 | 否 | 是 | 是 | 是 | 否 | 否 | 是 | 1 |
| | 其它 | 否 | 0.3 | 0.2 | 0.4 | 0.1 | 0.1 | 0.1 | 1 |
| 组合条件是否支持逻辑（与、或、非）表达式 | | 否 | 是 | 否 | 与 | 是 | 是 | 与 | 1 |
| 是否可以自由控制报告中漏洞描述的详细程度 | | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 1 |
| 是否能够定制报告生成模版 | | 是 | 否 | 否 | 是 | 是 | 否 | 是 | 1 |
| 是否可以自由控制报表中信息的组织结构 | | 是 | 否 | 否 | 否 | 否 | 否 | 是 | 1 |
| 是否可以针对主机间进行比较的结果生成报告 | | 是 | 否 | 否 | 是 | 否 | 是 | 是 | 1 |
| 能够生成的报告格式 | | 0.2 | 0.6 | 0.6 | 0.3 | 0.5 | 1 | 0.4 | 1 |

附表A6.2 报表信息完善程度和正确性测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 扫描起止日期、时间、开销时间 | 是 | 否 | 否 | 是 | 0.3 | 是 | 是 | 1 |
| 扫描使用的策略名称 | 否 | 否 | 否 | 是 | 是 | 是 | 是 | 1 |
| 生成报告的策略名称 | 是 | 是 | 否 | 否 | 是 | 是 | 是 | 1 |
| 扫描结束的状态（中断、扫描完毕） | 否 | 否 | 否 | 是 | 否 | 是 | 否 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 扫描目标的描述信息（总数目、IP地址等） | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 根据漏洞的危险级别统计分析得到的报表和图表 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 根据漏洞的操作系统类型统计分析得到的报表和图表 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 根据漏洞的类型统计分析得到的报表和图表 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 针对每台主机列出扫描该主机收集到的信息（端口、服务、帐号、路由信息等） | 是 | 否 | 否 | 是 | 0.75 | 是 | 是 | 2 |
| 根据扫描获得的路由信息生成可视化的拓扑图 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 为每台主机列出该主机上存在的漏洞列表 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 对每个漏洞都简单介绍存在该漏洞的软件的作用 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 对每个漏洞都描述该漏洞可能造成的危害 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 对每个漏洞都给出易于理解的名字 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 对每个漏洞都描述了存在漏洞的原因 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 对每个漏洞都提供了修补漏洞的方法 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 根据提供的修补方法能够有效的修补漏洞，而不需要参考其它资料 | 否 | 是 | 是 | 是 | 是 | 否 | 是 | 1.5 |
| 提供了能够获得该漏洞相关信息的网站 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1.5 |
| 提供了其它机构对该漏洞的命名（如Bugtraq或CVE） | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 提供了与该漏洞相关的软件厂家的联系方法 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 提供的报告为中文信息 | 否 | 是 | 是 | 是 | 否 | 是 | 否 | 2 |
| 是否提供对整个系统的安全程度的综合评估 | 否 | 否 | 否 | 是 | 是 | 是 | 否 | 1.5 |

附表 A7.1 系统的日志、审计功能测试结果

| 测试项目 | | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|---|
| 是否有完整的日志 | | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1 |
| 包含的日志信息 | 管理员登陆、退出 | 是 | 0.5 | 0.5 | 是 | 否 | 否 | 否 | 1 |
| | 扫描开始和结束 | 是 | 是 | 是 | 否 | 否 | 否 | 是 | 1 |
| | 扫描策略的导入导出 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | 1 |
| | 扫描结果的导出和删除 | 否 | 是 | 否 | 是 | 否 | 是 | 是 | 1 |
| 是否有完整的审计 | | 否 | 否 | 否 | 是 | 否 | 是 | 否 | 1 |
| 包含的审计信息 | 审计功能的开启和关闭 | 否 | 否 | 否 | 是 | 否 | 是 | 否 | 1 |
| | 读取、修改和破坏审计数据 | 否 | 否 | 否 | 是 | 否 | 是 | 否 | 1 |
| | 对鉴别机制的使用 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| | 所有使用鉴别机制的请求 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| | 任何对系统配置参数的修改 | | 是 | 否 | 是 | 否 | 是 | 否 | 1 |
| 日志信息是否可以导出 | | 否 | 是 | 是 | 否 | 否 | 是 | 是 | 1 |
| 审计信息是否可以导出 | | 否 | 是 | 是 | 否 | 否 | 是 | 否 | 1 |

附表 A7.2 系统的安全策略测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 本地密码文件是否有保护 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 本地密码文件是否有数据完整性保护 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 扫描IP 地址限制 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 在任何操作前的身份鉴别 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 2 |
| 系统是否具有重鉴别功能 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 2 |
| 系统是否可以设定登录空闲时间 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 系统是否具有鉴别失败处理 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 1.5 |
| 系统是否可以设定失败次数 | 否 | 否 | 否 | 是 | 否 | 是 | 否 | 1 |
| 使用不同的管理员登录系统，登录时是否可以看到其他管理员遗留的鉴别信息 | 是 | 否 | 否 | 否 | 否 | 否 | 是 | -1 |
| 是否可以对其他管理员生成的扫描策略信息进行察看和设置 | 否 | 否 | 否 | 否 | 否 | 是 | 是 | -1 |
| 察看是否可以对其他管理员生成的扫描日志信息进行察看和设置 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | -1 |
| 扫描策略信息是否能提供对文件的保密性和完整性鉴别 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 2 |
| 扫描日志是否能提供对重要文件的保密性和完整性鉴别 | 否 | 是（数据库） | 否 | 是 | 否 | 是 | 否 | 2 |

附表 A8 系统的互动性功能测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 是否支持与防火墙互动 | 否 | 否 | 否 | 是 | 否 | 否 | 否 | 1 |
| 与防火墙互动时，可向防火墙传送哪些信息 | 否 | 否 | 否 | 1 | 否 | 否 | 无 | 1 |
| 与防病毒产品的互动 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 与防病毒互动时，可向防病毒传送哪些信息 | 否 | 否 | 否 | 无 | 否 | 否 | 无 | 1 |
| 其他互动方式 | 否 | 否 | 0.1 | 0.2 | 否 | 0.1 | 0.4 | 1 |
| 是否互动接口程序 | 是 | 否 | 否 | 是 | 否 | 是 | 是 | 1 |

附表 A9 文档测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 是否提供安装说明文档 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 根据该安装说明文档是否能够正确地安装 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否提供了用户操作手册 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 根据该用户操作手册是否能够很容易就学会操作 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |
| 是否提供安装说明和操作手册的电子文档 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |

附表 A10 系统脆弱性发现能力的测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 是否发现 administrator 用户的密码为空 | 是 | 是 | 是 | | 是 | 是 | 是 | 1 |
| 是否发现 administrator 用户的密码为 123 | 否 | 是 | 是 | 无明显结果 | 是 | 是 | 否 | 1 |
| 是否发现 root 密码为 12345678 | 否 | 否 | 否 | | 否 | 否 | 否 | 1 |
| 是否发现操作系统重要目录设置为共享 | 是 | 否 | 0.5 | 是 | 是 | 是 | 是 | 1 |
| 是否发现受密码保护的共享目录的密码为 111 | 否 | 否 | 否 | 否 | 否 | 是 | 否 | 1 |
| 是否发现共享目录可写 | 否 | 否 | 否 | 否 | 否 | 否 | 是 | 1 |
| 是否发现 IIS 服务器目录列表可见 | 是 | 是 | 是 | 否 | 是 | 是 | 是 | 2 |
| 是否发现 FTP 服务器匿名用户可以访问 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 是否发现 FTP 服务器匿名用户文件可写权限 | 否 | 是 | 是 | 否 | 否 | 否 | 是 | 2 |
| 是否发现 SMTP 服务器匿名用户可以转发邮件 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 是否发现 SNMP 服务只读权限口令为 PUBLIC | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |

附表 A11 系统智能化的测试

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 是否能够识别该系统为WINDOWS系统 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1.5 |
| 是否能够识别标准端口80上提供的是WEB服务 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 是否能够识别标准端口80上提供的WEB服务是IIS | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 是否能够自动通过该端口探测WEB服务器的漏洞 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 2 |
| 在识别出WEB服务器的类型之后是否只扫描与该WEB服务器相关的漏洞。 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 2 |
| 如果WEB服务器运行在其它端口，是否能够自动识别该端口上提供的是WEB服务并自动通过扫描该端口探测WEB服务器的漏洞。 | 是 | 否 | 否 | 否 | 是 | 是 | 是 | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 将木马程序运行在非标准端口，该扫描系统是否能够正确识别出该端口上运行的程序为木马程序。 | 是 | 否 | 否 | 否 | 否 | 是 | 否 | 1 |
| 是否能够根据获得的路由信息绘制出整个系统的拓扑图。 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 1 |
| 在虚拟主机情况下，是否能够使用IP反查出域名后，自动扫描该域名扫描目标WEB服务器。 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 1.5 |
| 在服务器中途断连接时，是否能够识别出网络已经断开并停止扫描。 | 否 | 否 | 否 | 是 | 否 | 否 | 是 | 1 |

附表 A12 扫描速度测试

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 没启动防火墙时扫描端口使用的时间 | 0.95 | 0.65 | 0.8 | 0.8 | 1 | 0.75 | 0.6 | 1 |
| 没启动防火墙时探测到的端口列表 | 0.5 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 0.7 | 1 |
| 启动防火墙时扫描端口使用的时间 | 0.95 | 0.65 | 0.75 | 0.8 | 1 | 0.75 | 0.65 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 启动防火墙时探测到的端口列表 | 0.6 | 0.6 | 0.6 | 1 | 0.6 | 0.5 | 0.6 | 1 |
| 扫描漏洞使用的时间 | 0.95 | 0.85 | 0.85 | 1 | 1 | 0.95 | 0.65 | 1 |
| 扫描发现漏洞的数目 | 0.2 | 0.4 | 0.45 | 0.15 | 0.05 | 0.5 | 1 | 1 |

附表 A13 扫描系统开销测试结果

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 扫描系统启动前，CPU利用率 | 1 | 1 | 0.95 | 1 | 0.95 | 0.95 | 1 | 1 |
| 扫描系统启动前，内存占用大小 | 1 | 0.8 | 0.85 | 1 | | 0.95 | 0.8 | 1 |
| 扫描系统启动前，进程数 | 0.95 | 1 | 0.85 | 1 | | 0.9 | 0.85 | 1 |
| 扫描系统启动后，CPU利用率 | 1 | 1 | 0.9 | 1 | 0.7 | 0.9 | 0.9 | 1 |
| 扫描系统启动后，内存占用大小 | 1 | 0.9 | 0.95 | 1 | | 1 | 0.8 | 1 |
| 扫描系统启动后，进程数 | 0.95 | 0.95 | 0.85 | 1 | | 0.9 | 0.8 | 1 |
| 扫描系统过程中，CPU利用率 平均值 | 0.8 | 1 | 0.9 | 1 | 0.6 | 1 | 1 | 1 |
| 扫描系统过程中，CPU利用率 峰值 | 0 | 0 | 0 | 0.4 | 0.5 | 1 | 1 | 1 |
| 扫描系统过程中，CPU利用率 最小值 | 1 | 1 | 1 | 1 | 0.9 | 1 | 1 | 1 |
| 扫描系统过程中，平均 | 0.187 p/s | 0.589p/s | 0.182 p/s | 2.750p/s | 60% | 10.644M | 299552K | 1 |
| 扫描系统过程中，峰值 | 4.008 p/s | 44.797p/s | 11.317 p/s | 21.335p/s | 60% | 10.644M | 299552K | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 内存占用大小 | 最小值 | 0 p/s | 0p/s | 0 p/s | 0 p/s | 60% | 10.644M | 299552K | 1 |
| 扫描系统过程中，进程数 | 平均值 | 0.9 | 1 | 1 | 0.9 | | 0.7 | 0.7 | 1 |
| | 峰值 | 0.9 | 1 | 1 | 0.8 | 0.9 | 0.7 | 0.7 | 1 |
| | 最小值 | 0.9 | 1 | 1 | 1 | | 0.7 | 0.7 | 1 |
| 扫描花费时间 | | 0.9 | 0.8 | 0.8 | 1 | 0.9 | 1 | 0.8 | 1 |
| 扫描过程中，网络带宽占用 | 网络平均占用率 | 0.6 | 0.95 | 0.95 | 0.8 | 0.8 | 0.8 | 1 | 1 |
| | 网络数据包数量 | 0.6 | 1 | 1 | 1 | 0.8 | 0.8 | 0.9 | 1 |
| | 发送的总字节数 | 0.6 | 0.8 | 0.8 | 0.8 | 0.6 | 0.75 | 1 | 1 |

附表 A14 扫描系统稳定性

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 硬盘资源耗尽时是否正常运行 | 是 | 是 | 否 | 是 | 是* | 是 | 是 | 1 |
| 网络连接中断时是否正常运行 | 否 | 是 | 是 | 否 | 否* | 否** | 否 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 是否正确处理网卡故障 | 否 | 是 | 是 | 否 | 否* | 否** | 否 | 1 |
| 是否正确处理返回异常故障 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 1 |

附表 A15 按漏洞的风险分类统计厂商的漏报率/误报率

| 风险等级 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 高 | 0.57 /0.05 | 0.69 /0.026 | 0.64 /0.02 | 0.81 /0.01 | 0.97 /0.01 | 0.70 /0.02 | 0.82 /0.01 | 1 |
| 中 | 0.56 /0.06 | 0.60 /0.03 | 0.69 /0.03 | 0.80 /0.01 | 0.67 /0.02 | 0.66 /0.01 | 0.83 /0.01 | 1 |
| 低 | 0.52 /0.04 | 0.64 /0.02 | 0.63 /0.02 | 0.81 /0.02 | 0.71 /0.01 | 0.64 /0.02 | 0.84 /0.01 | 1 |

附表 A16 按漏洞的存在的操作系统分类统计厂商的漏报率/误报率

| 操作系统 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| Linux | 0.71 /0.03 | 0.43 /0 | 0.43 /0.01 | 1 /0 | 1 /0.01 | 0.71 /0.01 | 0.43 /0.01 | 1 |
| Win2k | 0.55 /0.08 | 0.62 /0.05 | 0.62 /0.04 | 0.86 /0.01 | 0.93 /0.01 | 0.54 /0.04 | 0.81 /0.03 | 1 |
| BSD | 0.5 /0.03 | 0.5 /0.01 | 0.5 /0.01 | 0.8 /0.014 | 0.7 /0.01 | 0.8 /0.01 | 0.6 /0.01 | 1 |
| XP | 0.76 /0.04 | 0.88 /0 | 0.73 /0.01 | 0.66 /0.02 | 0.95 /0.01 | 0.98 /0.01 | 0.80 /0.01 | 1 |
| Su n | 0.44 /0.11 | 0.46 /0.05 | 0.46 /0.06 | 0.51 /0.06 | 0.51 /0.04 | 0.77 /0.01 | 0.67 /0.01 | 1 |
| HP | 0.41 /0.07 | 0.67 /0.05 | 0.73/ 0.04 | 0.69 /0.02 | 0.41 /0.01 | 0.76 /0.01 | 0.86 /0.01 | 1 |

附表 A17 按漏洞的入侵手段分类统计厂商的漏报率/误报率

| 入侵手段 | 安氏 | 冠群金辰 | 亿阳信通 | 中联绿盟 | 赛门铁克 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 任意执行代码 | 0.56 /0.04 | 0.69 /0.02 | 0.64 /0.03 | 0.78 /0.02 | 0.99 /0.01 | 0.69 /0.02 | 0.82 /0.01 | 1 |
| dos 攻击 | 0.69 /0.04 | 0.74 /0.03 | 0.69 /0.03 | 0.95 /0.01 | 0.99 /0.01 | 0.68 /0.02 | 0.78 /0.01 | 1 |
| 信息泄露 | 0.45 /0.05 | 0.60 /0.02 | 0.59 /0.01 | 0.81 /0.01 | 0.90 /0.01 | 0.63 /0.01 | 0.80 /0.01 | 1 |
| 非法 | 0.5 | 0.55 | 0.65 | 0.67 | 0.82 | 0.68 | 0.88 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 访问系统 | /0.14 | /0.03 | /0.03 | /0.03 | /0.01 | /0.01 | /0.02 | |
| 危险服务开放 | 0.58 /0.01 | 0.74 /0.03 | 0.79 /0.02 | 0.76 /0.01 | 0.15 /0.02 | 0.64 /0.02 | 0.82 /0.02 | 1 |
| 非法修改系统配置 | 0.64 /0.06 | 0.76 /0.06 | 0.68 /0.06 | 0.88 /0.03 | 0.96 /0.01 | 0.76 /0.01 | 0.96 /0.01 | 1 |
| 其他 | 0.55 /0.045 | 0.57 /0.03 | 0.59 /0.02 | 0.86 /0.01 | 0.87 /0.02 | 0.69 /0.01 | 0.85 /0.01 | 1 |

附表 A15.1 客观增补测试项目（以不使目标系统宕机为优）

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 宕机 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 管理器和扫描引擎之间通信的稳定性 | 2 | 1.8 | 1.8 | 1.8 | 2 | 1.4 | 2 | 2 |

附表 A15.2 主观增补测试项目

| 测试项目 | 安氏 | 冠群金辰 | 亿阳信通 | 赛门铁克 | 中联绿盟 | 启明星辰 | 中软国际 | 权重 |
|---|---|---|---|---|---|---|---|---|
| 设备熟悉程度及解答正确性 | 1.2 | 2 | 2 | 2 | 2 | 1.4 | 2 | 2 |
| 应急反应速度及人员重视程度 | 1.8 | 2 | 1.6 | 2 | 2 | 2 | 1.4 | 2 |

# 附录 B 网络扫描器产品测试评分规则

## B.1 漏洞扫描评分总表

根据省公司的需求反馈情况，网络扫描产品测试组确定了测试评分的权重，满分 100 分。详见下表。

| 测试大项 | 测试小项 | 大项权重 | 小项权重 |
|---|---|---|---|
| 扫描器系统功能测试结果 | 部署和管理测试结果 | 34 | 6 |
| | 系统升级能力测试结果 | | 2 |
| | 系统配置测试 | | 1 |
| | 扫描策略定制 | | 6 |
| | 信息收集能力测试结果 | | 6 |
| | 扫描文档和报表 | | 6 |
| | 系统日志、审计与系统安全策略 | | 6 |
| | 系统的互动性 | | 1 |
| | 安装文档及用户手册 | | 0 |
| 漏洞扫描测试 | 系统的漏报率 | 48 | 12 |
| | 系统的误报率 | | 20 |
| | 系统的脆弱性测试 | | 8 |
| | 系统的智能化程度测试 | | 8 |
| 性能测试 | 扫描速度 | 10 | 4.5 |
| | 扫描系统资源开销 | | 1 |
| | 稳定性测试 | | 4.5 |
| 增补的客观测试项目 | 宕机 | 4 | 2 |
| | 服务器端与客户端连接错误 | | 2 |
| 增补的主观测试项目 | 设备熟悉程度及解答正确性 | 4 | 2 |
| | 应急反应速度及人员重视程度 | | 2 |

某厂家最终得分为每张子表得分之和。

在后续内容将分别描述网络入侵检测产品测试各大项的评分规则。

## B.2 系统功能测试评分

系统功能当中共 9 张子表，每张表得分的计算方式为：针对某厂家设备将该表每一项的得分加权累加（此权重参见附录 A 中附表的最后一列）后所得的结果除以该表的应得总分（即所有测试项均完全通过）再乘以该表所对应的权重（此权重参见总评分表最后一列）。其中，“是”表示 1，“否”表示“0”。

如：某厂家的“部署和管理”子表每一项得分加权累加后为 7，而该表的应得总分为 20.5（将小权重累加），然后算出本子表的得分为（7÷20.5）×6＝2.05（四舍五入）。

系统功能测试的总分即为各个子表得分的总和。

### B.3 漏洞扫描测试评分

漏洞扫描测试的总分为将以下 4 个方面的得分按照总评分表中所列出的小项权重（此权重参见总评分表最后一列）进行加权平均所得。

#### B.3.1 漏报率的计算方法

漏报率的评分方式为先分别按照漏洞的 3 种分类方式（即按操作系统、按漏洞的危险级别、攻击的方式）计算出单独的结果，然后将这三个结果进行平均算出总分。而每种分类方式的得分为相应的漏报比例按照权重加权平均得出的结果，权重分别如下：

1. 操作系统：

| 操作系统类型 | 权重 |
|---|---|
| WINDOWS | 4 |
| SOLARIS | 4 |
| HP-UNIX | 3 |
| LINUX | 1 |
| BSD | |

2. 攻击类型：

| 攻击类型 | 权重 |
|---|---|
| 任意执行代码 | 3 |
| 非法访问系统 | |
| DoS 攻击 | 3 |
| 信息泄漏 | 2 |
| 非法修改系统配置 | |
| 危险服务开放 | 1 |
| 其他 | |

3. 危险级别

| 危险级别 | 权重 |
|---|---|
| 高风险 | 5 |
| 中风险 | 3 |
| 低风险 | 2 |

#### B.3.2 误报率得分的计算方法

同漏报率的计算方法。

### B.3.3 系统脆弱性得分的计算方法

系统的脆弱性测试的得分也是通过表格（权重参见附表 A10）来体现的，其计算方式同“系统功能”的评分。

### B.3.4 系统的智能化程度得分的计算方法

同“系统脆弱性得分计算方法”,权重参见附表 A11。

## B.4 性能测试评分

性能测试主要包括三部分内容。

### B.4.1 扫描速度测试

这一测试的目的以量化的方式比较不同扫描系统的扫描速度，为了能够以一种公平的方式比较不同系统的扫描速度，

- 启动和没启动防火墙时扫描端口使用的时间评分标准如下：
  3 分钟以下为 1 分；
  3～8 分钟为 0.95～0.9 分；
  9～15 分钟为 0.9～0.8 分；
  16～25 分钟为 0.8～0.75 分
  26～40 分钟之间为 0.7～0.65 分；
  41～60 分钟之间为 0.65～0.6；
  60 分钟以上为 0.55 分；
- 启动与没启动防火墙时探测到的端口列表：
  以实际打开的端口列表为基准表，各个厂家实际探测到的端口列表在基准表中所占的比例即为所得分值，对于厂家探测到的基准表之外的端口则不予考虑。
- 扫描漏洞使用的时间评分标准如下：
  3 分钟以下为 1 分；
  3～8 分钟为 0.95～0.9 分；
  9～15 分钟为 0.9～0.85 分；
  16～25 分钟为 0.8～0.75 分
  26～40 分钟之间为 0.75～0.65 分；
  41～60 分钟之间为 0.65～0.6；
  60 分钟以上为 0.55 分；
- 扫描发现漏洞的数目：
  以各厂家所发现的最大数目为基准作为 1 分，其他的与最大数目相比所得的比值即为其所得分值。

### B.4.2 扫描系统资源开销

由于各厂家的机器配置不同，很难用一个统一的标准来评定，因此 CPU 利用率、内存占用大小、进（线）程数等都仅作参考，主要考虑扫描花费时间和扫描过程中的网络带宽占用情况。

- 扫描系统启动前后的 CPU 利用率：

以 0%为 1 分，5%以下为 0.95 分，此后每增加 5%，减 0.05 分

- 2.2 扫描系统启动前后的内存占用大小：

以各厂家的数据中的最小值为 1 分，作为基准，每增加 50k 减 0.05 分；

- 2.3 扫描系统启动前后的进程数：

以各厂家中数据中的最小值为基准，每增加 5 个进程减 0.05 分；

- 2.4 扫描系统过程中，CPU 利用率：

平均值以 5%以下为 1 分，没增加 5%减 0.1 分；

峰值与最小值以 5%以下为 1 分，每增加 10%减 0.1 分；峰值 100%为 0 分；

- 2.5 扫描系统过程中的进程数

20 个以下为 1 分，每增加 10 个减 0.1 分；

- 2.6 扫描花费时间：

3 分钟以下为 1 分；

3～5 分钟为 0.8 分；

6～15 分钟为 0.6；

15 分钟以上酌情评分；

- 2.7 扫描过程中的网络带宽占用情况：

网络平均占用率 （单位：字节/秒）：

5K 以下为 1 分；

5K～30K 之间每增加 5K 减 0.05 分；30K 以上每增加 10K 减 0.05 分；

网络数据包数量：

15，000 以下为 1 分；每增加 5，000 减 0.05 分；

发送的总字节数

1500K 以下为 1 分，每增加 500K 减 0.05 分；

### B.4.3 稳定性测试

计算方式同“系统功能”的评分，权重参见参见附表 A14。