# 天镜脆弱性扫描与管理系统 V6.0

## （分布版）

# 产品白皮书

启明星辰信息技术有限公司

# 版权声明

北京启明星辰信息技术有限公司 2004 版权所有，保留一切权利。

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外,其著作权或其他相关权利均属于北京启明星辰信息技术有限公司。未经北京启明星辰信息技术有限公司书面同意不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。本文档中的信息归北京启明星辰信息技术有限公司所有并受著作权法保护。

“天镜”为北京启明星辰信息技术有限公司的注册商标，不得仿冒。

**信息更新**

本文档及其相关计算机软件程序（以下文中称为“文档”）仅用于为最终用户提供信息，并且随时可由北京启明星辰信息技术有限公司（下称“启明星辰”）更改或撤回。

**声明**

本手册的内容随时更改，恕不另行通知。

北京启明星辰信息技术有限公司可能已经拥有或正在申请与本文档主题相关的各项专利。提供本文档并不表示授权您使用这些专利。您可将许可权查询资料用书面方式寄往北京启明星辰信息技术有限公司（地址）

北京启明星辰信息技术有限公司对本手册的内容不提供任何担保，本手册如有谬误，北京启明星辰信息技术有限公司概不负责，对于使用本手册造成的与其有关的直接或间接损失，亦概不负责。

# 目录


1 产品组成.....4
2 产品部署.....4
2.1 方案一：单机式部署.....4
2.2 方案二：分布式部署.....5
2.3 方案三：多级式部署.....6
3 系统配置.....6
4 功能特色.....7
4.1 管理功能.....7
4.1.1 分布管理、集中分析.....7
4.1.2 多级管理.....8
4.2 系统配置功能.....8
4.3 策略管理.....8
4.3.1 扫描计划定制.....8
4.3.2 系统使用授权限制.....9
4.4 自定义显示功能.....10
4.4.1 自定义分类结构显示.....10
4.4.2 显示自定义窗口.....10
4.4.3 重点关注自定义.....10
4.5 扫描功能.....11
4.5.1 端口服务智能识别.....11
4.5.2 可识别的扫描对象.....12
4.5.3 扫描漏洞分类.....12
4.5.4 数据库扫描.....12
4.5.5 Web 扫描.....12
4.6 漏洞信息规范.....12
4.7 报告功能.....13
4.7.1 趋势分析.....14
4.7.2 安全评估.....14
4.7.3 安全信息手册.....15
4.8 安全管理平台.....15
4.9 用户管理与审计.....16
4.10 系统升级能力.....17
5 扫描技术特色.....17
6 天镜产品型号组成.....17

# 1 产品组成

天镜分布式产品组成包含几个部分：

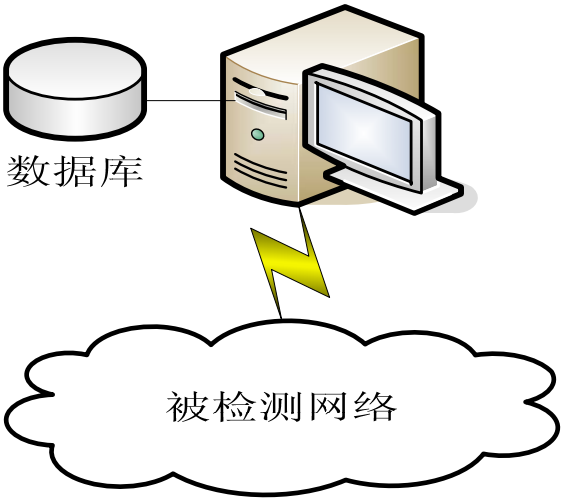
- **管理控制中心**：负责添加、修改扫描引擎的属性，进行策略编辑和扫描任务制定和下发执行，完成漏洞库和扫描方法的升级，同时支持主、子控设置；
- **综合显示中心**：实时显示扫描的结果信息。可以进行树形分类察看和分窗口信息察看，显示扫描进度，提供漏洞解释的详细帮助；
- **日志分析报表**：查询历史扫描结果，提供多种报表模版，形成图、表结合的丰富报表，以多种文件格式输出；
- **扫描引擎软件**：执行管理控制中心发来的扫描任务，返回扫描结果到综合显示中心显示并存入数据库中；
- **扫描对象授权**：通过授权许可具体的扫描引擎软件可扫描对象，包括同时扫描的数量，也可以指定那些目标可以扫描或禁止扫描；
- **数据库**：产品缺省提供 MSDE 的桌面数据库安装包，用户可以根据扫描规模的大小选用 MSDE 或者 SQL SERVER 作为使用数据库。

# 2 产品部署

## 2.1 方案一：单机式部署

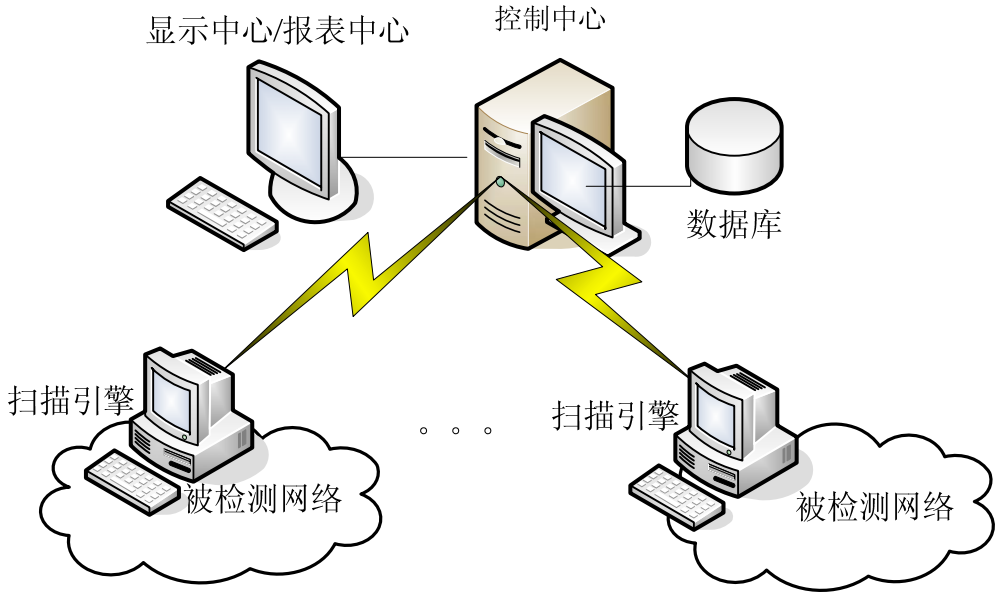
将天镜产品的各部分组件安装在同一台机器上，类似单机版扫描系统。该部署方式可在同一台机器上完成对天镜系统的使用操作。

控制中心/显示中心/报表中心/扫描引擎



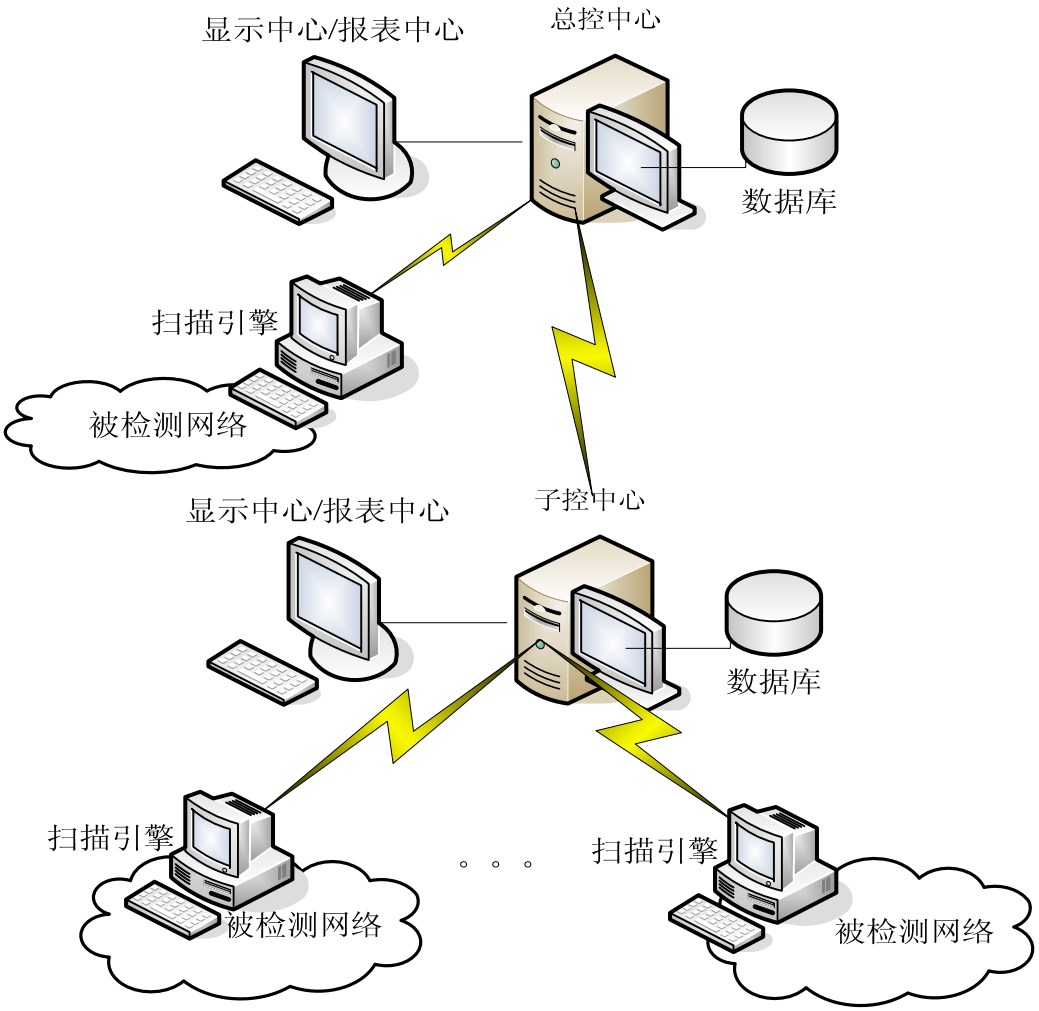

## 2.2 方案二：分布式部署

天镜产品部署通常如下所示，其功能组件可以部署在不同主机上，控制中心同时管理多个扫描引擎，不同的扫描引擎负责对不同网段的系统进行扫描检测，显示中心和报表中心可汇总显示各扫描引擎的扫描结果信息。



## 2.3 方案三：多级式部署

该部署方案适应于用户网络环境有不同的地域层次区分，每个地域均配有独立的安全管理人员，该人员负责管理本区域和其下属区域的安全管理。通过在各自区域放置管理中心，并且上级管理中心可以上传下级管理中心的扫描结果等信息。




# 3 系统配置

**1、硬件环境：**

本系统运行在硬件环境为 X86 架构的台式机或笔记本电脑。

- CPU：不低于 Pentium IV 2.2G
- 内存：不低于 512M

- 硬盘：不低于 50M 剩余空间，建议 200M 以上剩余空间
- 网卡：至少一块 100Mbps 以太网卡

**2、软件环境：**

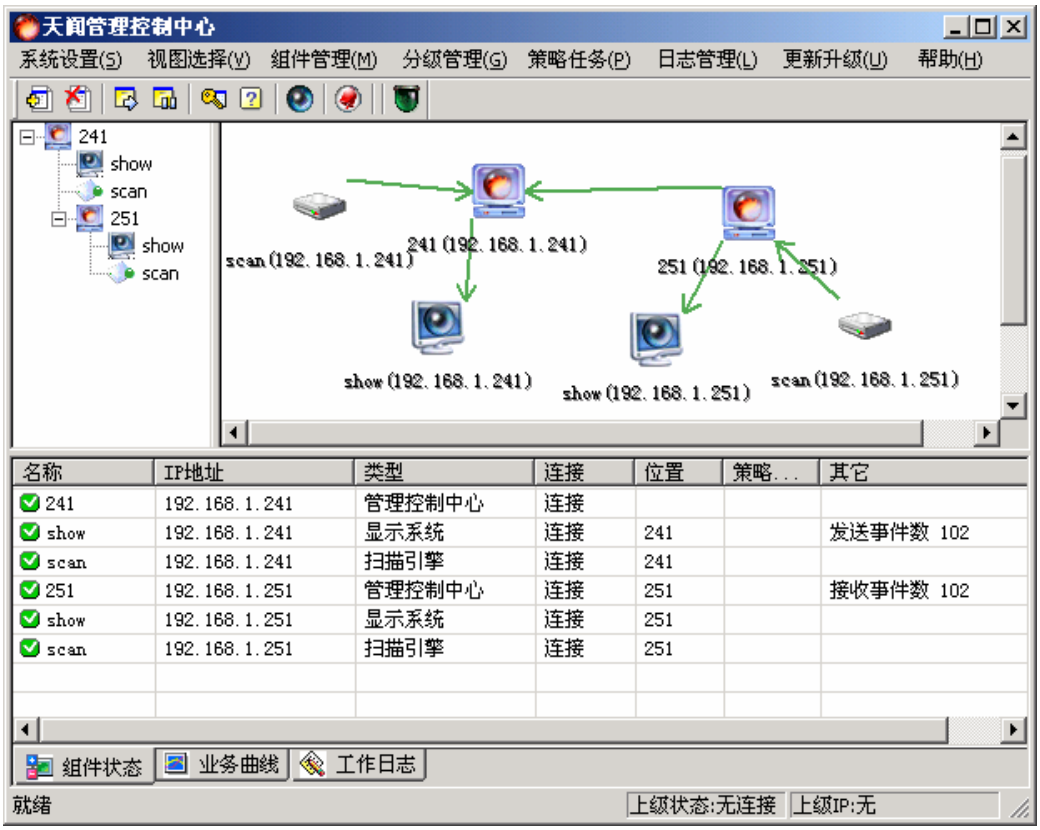
- 操作系统：中文版 Windows 2000 SP4 以上
- 浏览器：IE5.0 以上版本

# 4 功能特色

## 4.1 管理功能

### 4.1.1 分布管理、集中分析

通过天镜系统的分布式部署，各扫描引擎可以按不同的扫描策略同时进行多网络系统的漏洞检测，并将检测结果集中显示、集中分析。



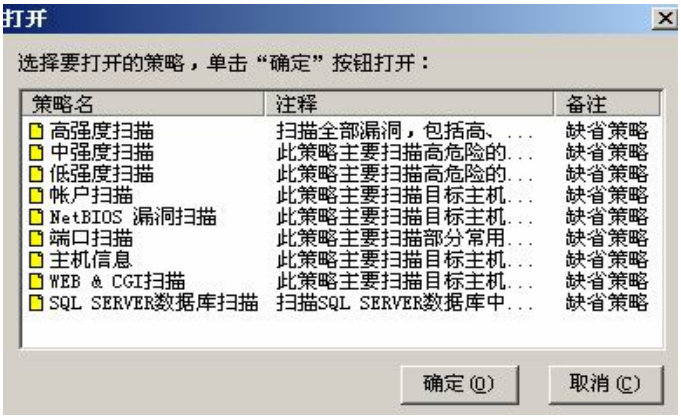
### 4.1.2 多级管理

对于拥有不同地域、大规模网络的用户，各个地域的网络安全管理员管理着本地域的网络安全状况，其上层的安全管理员可以上传检测结果、下达检测策略、统一管理、统一分析、统一升级；实现大规模网络环境下的全局风险控制、降低管理成本。

## 4.2 系统配置功能

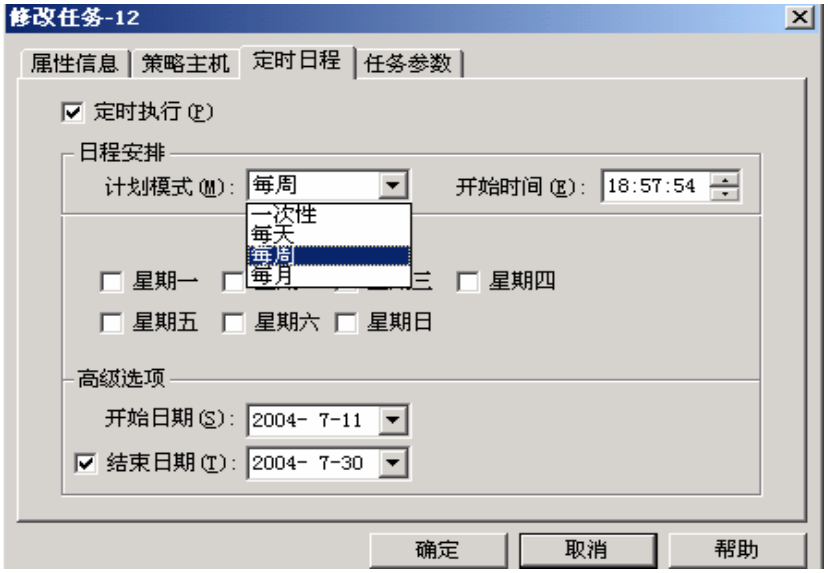
## 4.3 策略管理

天镜为用户提供缺省的十种扫描策略，用户可根据实际需求来选择合适的策略。同时，天镜灵活的策略自定义功能可以让用户根据特殊需要更改和编辑扫描策略。应用特定配置的策略，用户能实现不同内容、不同级别、不同程度、不同层次的扫描。



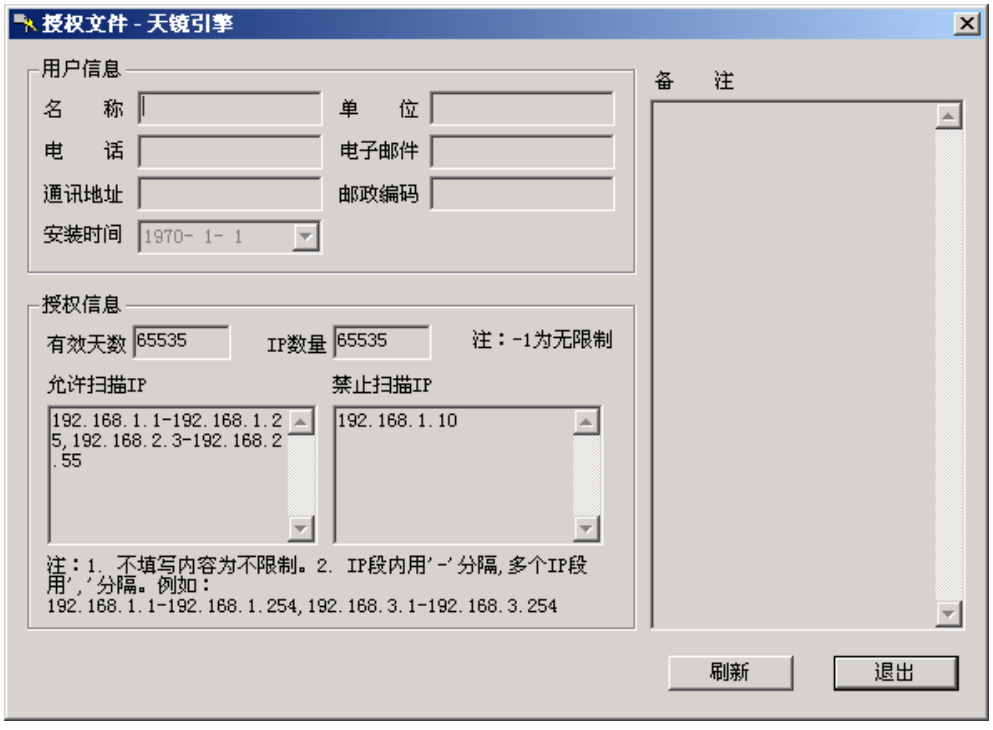

### 4.3.1 扫描计划定制

天镜支持扫描计划任务，可根据用户自定义的扫描计划来完成扫描任务，扫描任务可以按照不同时间类型（如每周、每月等）制定多个，分别自动执行，系统还支持计划有效期的设定。




## 4.3.2 系统使用授权限制

确保系统的使用安全、防止非法使用，本系统提供了硬件强制授权管理



## 4.4 自定义显示功能

### 4.4.1 自定义分类结构显示

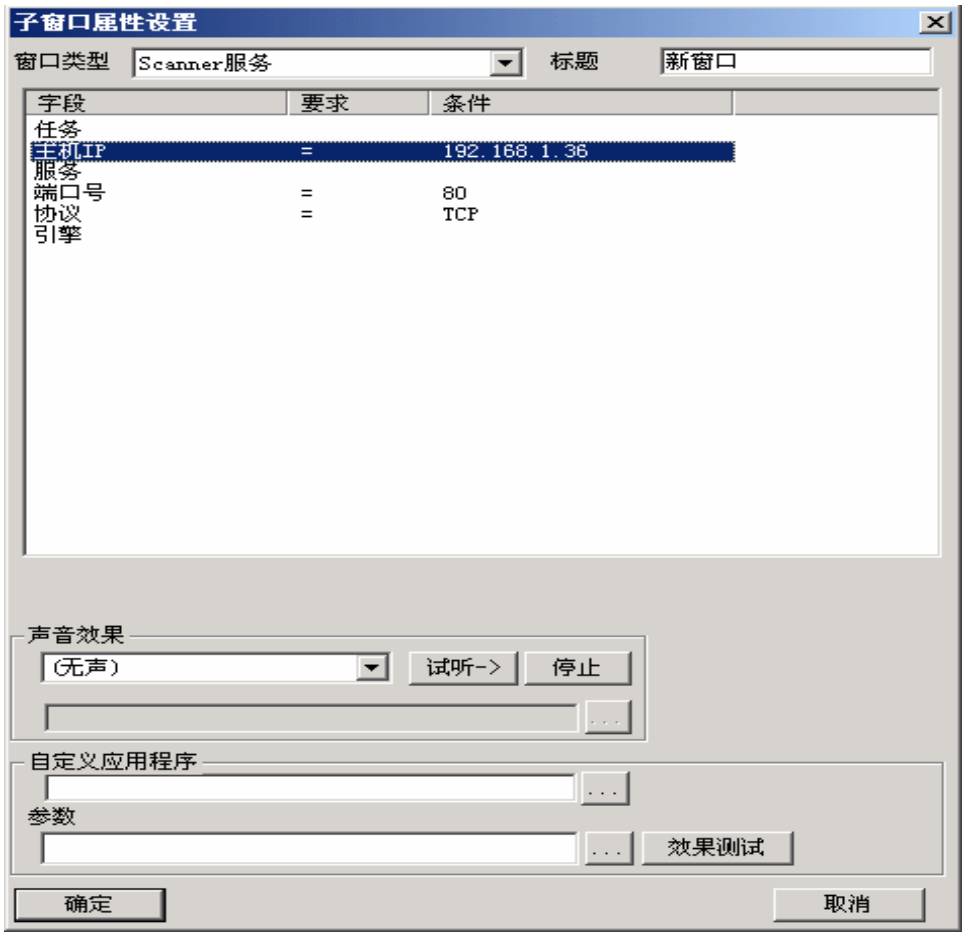
检测结果的分类窗口自定义:用户可根据需要，灵活地以树形结构分类显示扫描结果

### 4.4.2 显示自定义窗口

检测结果的详细信息窗口自定义：默认的显示窗口为 4 个，可以自由扩展到 10 个显示窗口

### 4.4.3 重点关注自定义

检测结果的重点关注信息自定义窗口：可以通过设置窗口属性，对扫描结果进行筛选过滤




## 4.5 扫描功能

### 4.5.1　端口服务智能识别

系统利用协议特征分析技术，可以识别非常规开放的端口上启用的服务

### 4.5.2 可识别的扫描对象

天镜能够准确的识别各种操作系统和主机名称，如 Win95/98/Me、Windows NT、Windows 2000/XP、Windows2003、Linux、Solaris、SCO Unix、HP Unix、IBM AIX、IRIX、BSD 等。

天镜可以扫描的对象包括各种服务器、工作站、网络打印机以及相应的网络设备如：3Com 交换机、CISCO 路由器、Checkpoint Firewall、HP 打印机、Cisco PIX Firewall 等。

天镜可以提供扫描对象的账户信息，便于检查是否异常账户出现。

### 4.5.3 扫描漏洞分类

Windows 系统漏洞、WEB 应用漏洞、CGI 应用漏洞、FTP 类漏洞、DNS、后门类、网络设备漏洞类、缓冲区溢出、信息泄漏、MAIL 类、RPC、 NFS、NIS、 SNMP、守护进程、PROXY、强力攻击等 1700 种以上

为确保网络的保密性，天镜系统够检测到网络中存在的网络监听设备。

### 4.5.4 数据库扫描

天镜目前支持对 MS SQL Server、Oracle、Sybase、DB2、MySQL 数据库的扫描功能。

天镜可以扫描数据库近二百多种漏洞，包含了有关空口令、弱口令、用户权限漏洞、用户访问认证漏洞、系统完整性检查、存储过程漏洞和与数据库相关的应用程序漏洞等方面的漏洞，基本上覆盖了数据库常被用做后门进行攻击的漏洞，并提出相应的修补建议。

### 4.5.5 Web 扫描

天镜可以扫描目标主机的 Web 服务，以发现 Web 服务器可能存在的漏洞。天镜支持常见的 IIS、Apache 等 Web 服务器的扫描，尤其对于 IIS 具有最多的漏洞检测能力。

## 4.6 漏洞信息规范

- 全面符合 CNCVE 标准；
- 兼容国际 CVE 标准；
- 与 BUGTRAQ 等其他漏洞标准对应。

## 4.7 报告功能

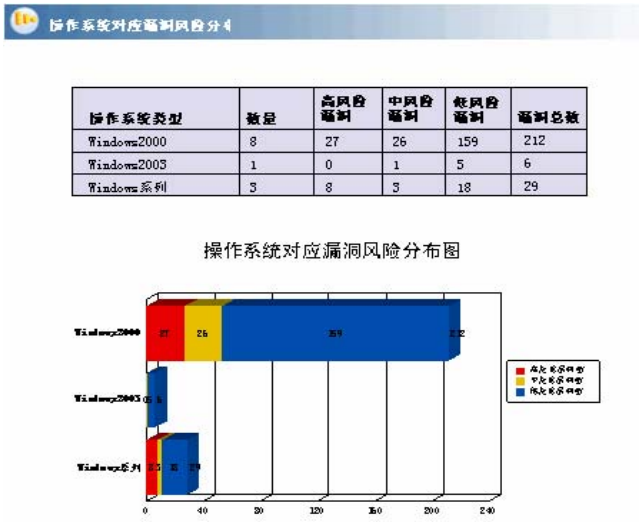
天镜具备全面详细的分析报告能力，可根据安全管理的不同角色定位按照要求生成面向主管领导、管理人员、技术人员的不同类型的报告。这些报告包括：分时间扫描任务执行报告、分时间扫描任务执行结果、报告不同时间的扫描结果趋势比较、管理性简报、技术报告、评估报告以及扫描采用策略报告

报告中的内容包括漏洞信息、漏洞主机信息、危险级别、修补建议等，并提供安全补丁供应商的热连接，以保证快速及时的修补漏洞。

报告形式中采用图、表以及详细文字说明结合，报告的标题格式可以由用户自定义，最后可以输出多种格式的报告（如 PDF、XML、 HTML 、EXCEL、WORD 等常见格式）

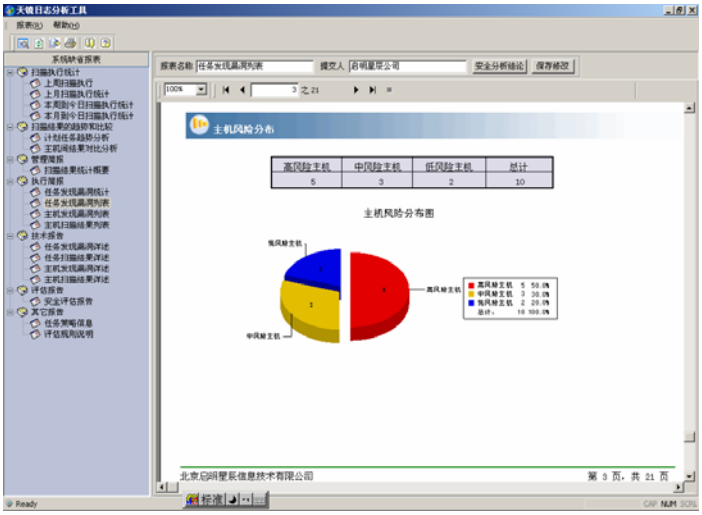
**1） 统计报告**

扫描结果不同分类的统计信息



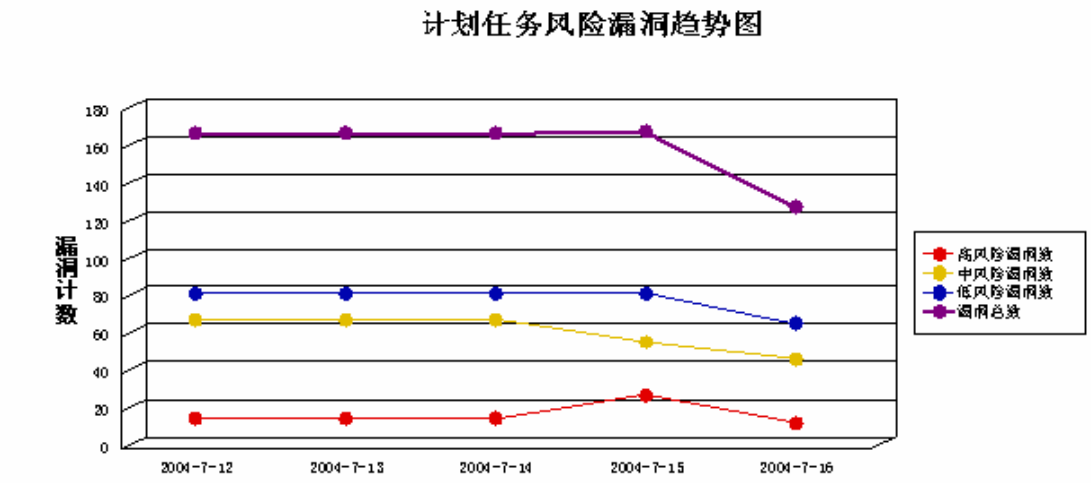

| 操作系统类型 | 数量 | 高风险漏洞 | 中风险漏洞 | 低风险漏洞 | 漏洞总数 |
|---|---|---|---|---|---|
| Windows2000 | 8 | 27 | 26 | 159 | 212 |
| Windows2003 | 1 | 0 | 1 | 5 | 6 |
| Windows系列 | 3 | 8 | 3 | 18 | 29 |

**2） 评估结果**



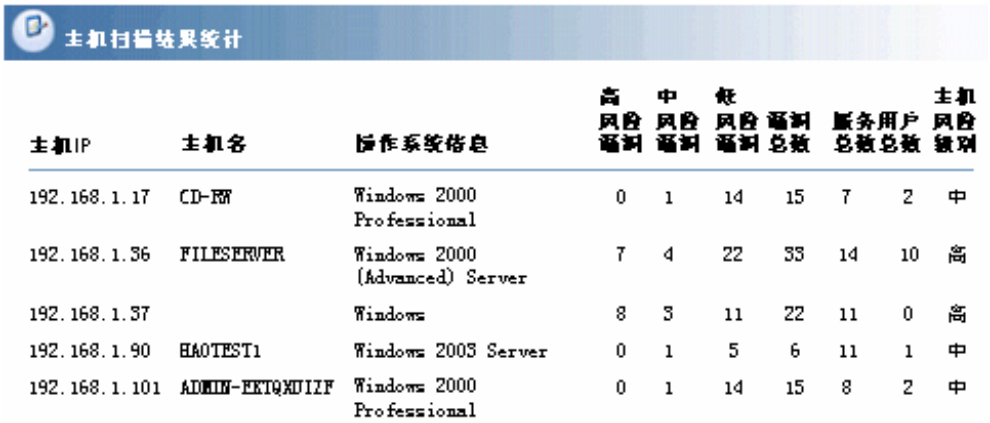

## 4.7.1 趋势分析

扫描结果的趋势分析




## 4.7.2 安全评估

按扫描结果确定主机的风险级别



主机扫描结果统计

| 主机IP | 主机名 | 操作系统信息 | 高风险漏洞 | 中风险漏洞 | 低风险漏洞 | 漏洞总数 | 服务总数 | 用户总数 | 主机风险级别 |
|---|---|---|---|---|---|---|---|---|---|
| 192.168.1.17 | CD-FAF | Windows 2000 Professional | 0 | 1 | 14 | 15 | 7 | 2 | 中 |
| 192.168.1.36 | FILESERVER | Windows 2000 (Advanced) Server | 7 | 4 | 22 | 33 | 14 | 10 | 高 |
| 192.168.1.37 | | Windows | 8 | 3 | 11 | 22 | 11 | 0 | 高 |
| 192.168.1.90 | HAOTEST1 | Windows 2003 Server | 0 | 1 | 5 | 6 | 11 | 1 | 中 |
| 192.168.1.101 | ADMIN-FEKTQXUIIF | Windows 2000 Professional | 0 | 1 | 14 | 15 | 8 | 2 | 中 |

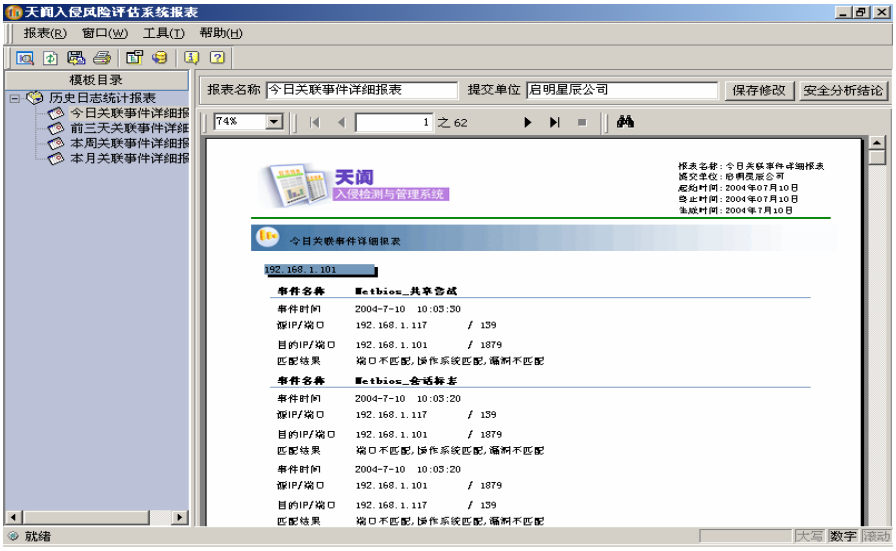
## 4.7.3 安全信息手册

详细的安全信息查询和参考手册，漏洞解释包括漏洞的说明、影响的系统、平台、危险级别以及标准的 CNCVE、CVE、BUGTRAQ 等对应关系以及链接信息；修补建议包括手动处理、加固建议以及补丁下载的详细提示。

## 4.8 安全管理平台

实现启明星辰天阗安全管理平台（IMS）系统的统一管理、入侵风险评估功能，即在

安全管理平台系统中，天镜扫描引擎、天阗检测引擎在平台的统一管理下，协同分析、利用天镜系统的系统脆弱性扫描结果，实时验证 NIDS 系统的安全预警事件的有效性，给出攻击对资产的威胁程度验证结果，降低 NIDS 系统的误报率。

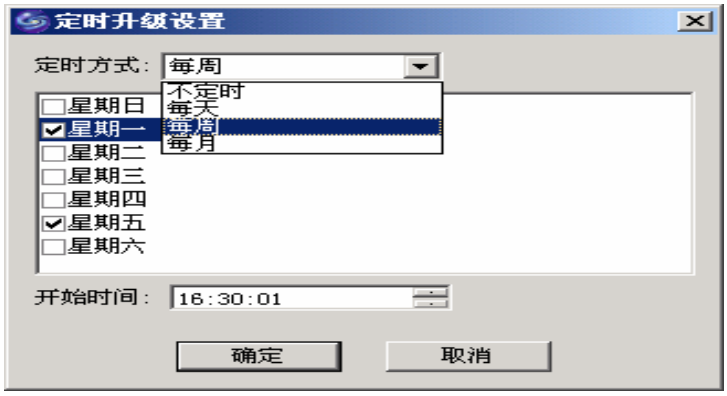



## 4.9 用户管理与审计

- 系统分用户、分权限使用与管理；
- 支持双因素身份认证：口令、身份卡配合使用；
- 用户、管理员的操作审计。

## 4.10 系统升级能力

系统提供了极为方便的升级方式，包括自动升级和手动升级两种，审计内容包括新增的漏洞方法和系统补丁程序两大部分。当现有系统的升级版本与公司网站提供的系统版本不一致时，可通过系统提供的升级方式进行实时在线升级。在统一管理控制的条件下，系统升级可以集中进行，即在控制中心对系统所有的各引擎系统进行自动升级。




# 5 扫描技术特色

- 渐进式扫描：根据被扫描主机的操作系统和主机应用等信息智能确定进一步的扫描流程；
- 授权扫描：系统支持用户提供被扫描主机的权限信息，以获取更深入、更全面的漏洞信息；
- 系统稳定性高：扫描过程实时正确处理各种意外情况：如网卡故障、资源耗尽等；
- 扫描系统资源占用少、速度快、误报低、漏报低、稳定性高。

# 6 天镜产品型号组成

| 型号名称 | 产品特点 | 应用特点 |
| --- | --- | --- |
| 单机版 | 使用简单、灵活易用 | 1、适合于移动式扫描；<br>2、如检测机不可移动，检测的网络子网规模较少 |

| | | |
|---|---|---|
| 便携版 | 1、硬件绑定的产品<br>2、专用网络脆弱性检测工具<br>3、使用简单、灵活易用<br>4、易于移动<br>5、产品本身具有防潮、防震 | 1、适合于移动式扫描；<br>2、检测各种网络规模环境<br>3、适合较大范围移动的环境 |
| 分布版 | 1、支持分布式扫描、集中管理分析；<br>2、支持多级式扫描和管理；<br>3、支持与天阗 NIDS 系统统一管理、综合分析。 | 1、适合于固定式部署；<br>2、按周期进行网络检测、按计划周期实施自动检测；<br>3、适合于大规模网络的检测<br>4、支持同时检测多个子网络；<br>5、适合于层次性、分级管理。<br>6、适合于 NIDS 安全事件与漏洞结果的综合分析 |