天镜脆弱性扫描与管理系统

V6.0（单机版）

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。

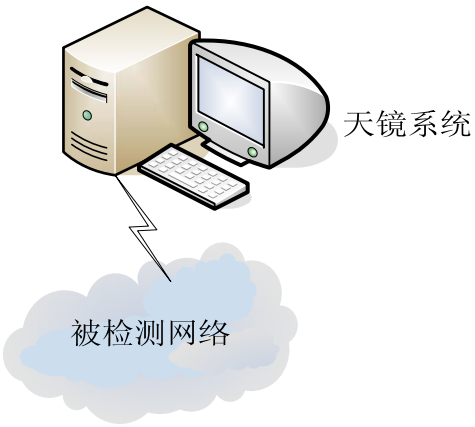
目　录

1 产品功能

天镜脆弱性扫描与管理系统（单机版）是一个软件产品，能够综合检测网络系统中存在的弱点和漏洞，并以报表的方式提供给用户，适时提出修补方法和安全实施策略。系统内含基于国际标准建立的安全漏洞库检测，并通过网络升级与最新漏洞检测保持同步。

2 产品部署

天镜单机版的部署非产简单，可以被安装在便携机或 PC 工作站上，用户将其连接到被扫描的网络环境中即可进行用户网络环境的脆弱性检测。如下图所示：



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 方便易用的系统

天镜系统使用简单、易于操作。以下几个部分为该系统的主要功能组成：

1、启动扫描：输入扫描地址、选取扫描策略；

2、查看结果：查看扫描后的结果信息；

3、策略编辑：根据用户的网络设备环境，定制　不同的扫描策略；

4、报表分析：分析、统计扫描结果信息；

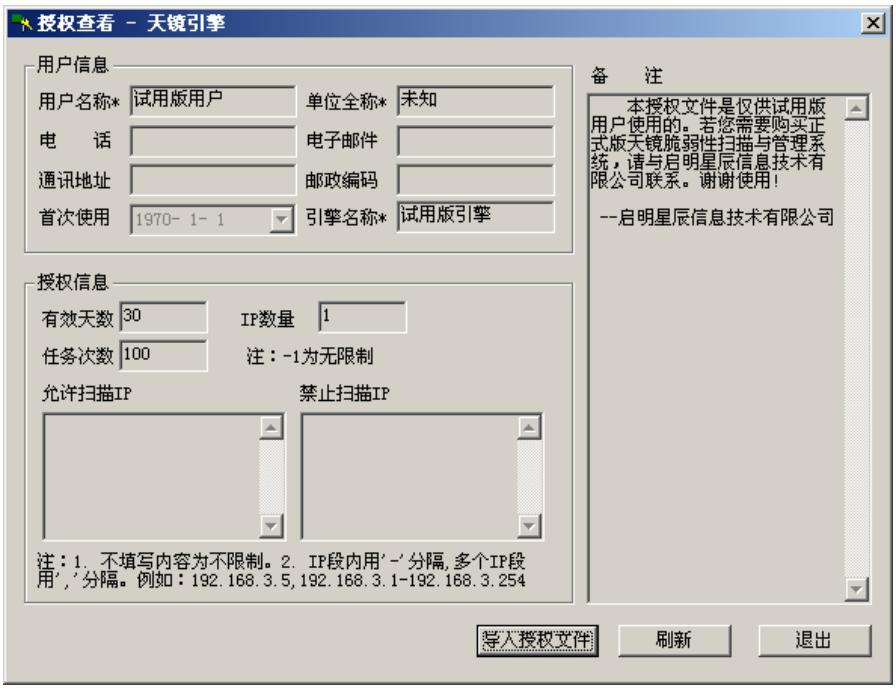
5、用户管理：分配不同的用户管理权限；

4.1.1 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。

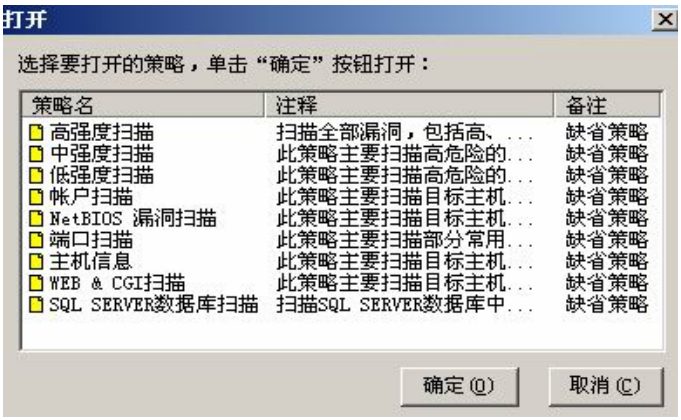
4.1.2 系统使用授权限制

确保系统的使用安全、防止非法使用，本系统提供了强制授权管理



4.1.3 灵活的策略定制

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。



系统为用户提供了灵活方便的策略选择模板，以适用于在不同的网络环境下的扫描需求。系统提供了以下的策略分类模板：

- 按操作系统分类
- 按风险级别分类
- 按 CVE 编号分类
- 按标准模式分类
- 按系统升级分类

为方便用户扫描策略的异地移植，本系统提供了扫描策略的导入/导出功能：

- 导出功能：支持扫描策略导出功能，确保用户在一个天镜系统使用的策略能够很容易的应用到另外一个天镜系统中；
- 导入功能：与导出功能相对应，确保扫描策略的灵活移动。

4.2 强大的扫描能力

4.2.1 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

4.2.2 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 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。

4.2.3 扫描漏洞分类

天镜系统可扫描任何基于 TCP/IP 的网络主机，无论网络核心是采用 FDDI、ATM 还是千兆以太网，只要目标主机支持 TCP/IP 协议，就可对其进行扫描;系统具体的扫描内容分类如下：Windows 共享类、 Web 服务类、CGI 类、信息搜集类、强力攻击类、守护进程类、电子邮件服务类、FTP 服务类、DNS 类、网络管理 SNMP 类、Proxy 类、协议欺骗类、RPC 类、 NFS 类、NIS 类、后门类、网络设备类、蠕虫病毒类、缓冲溢出和拒绝服务攻击类、数据库类等。

产品发布时支持的漏洞检测的数量：1700 种以上

4.2.4 数据库扫描

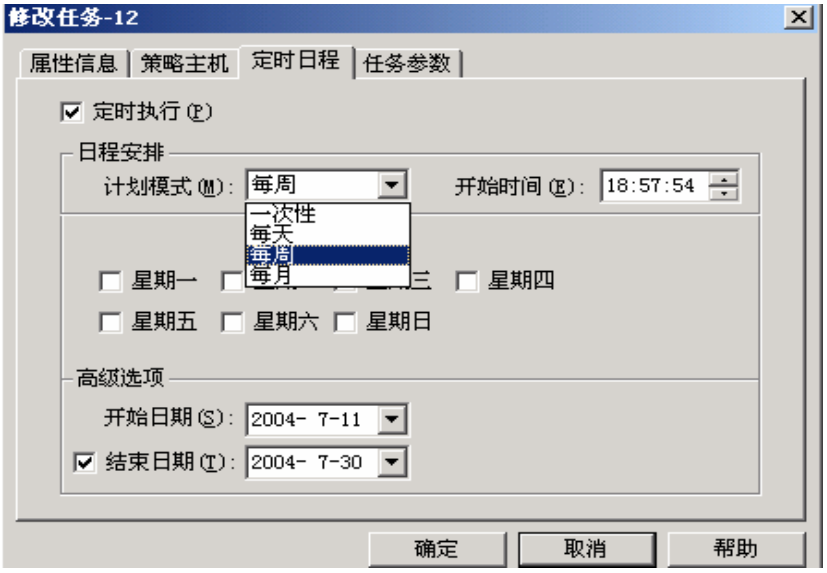
天镜目前支持对 MSSQL Server、Oracle、Sybase、DB2 数据库的扫描功能。

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。

4.3 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。



4.4 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。

4.5 报告功能

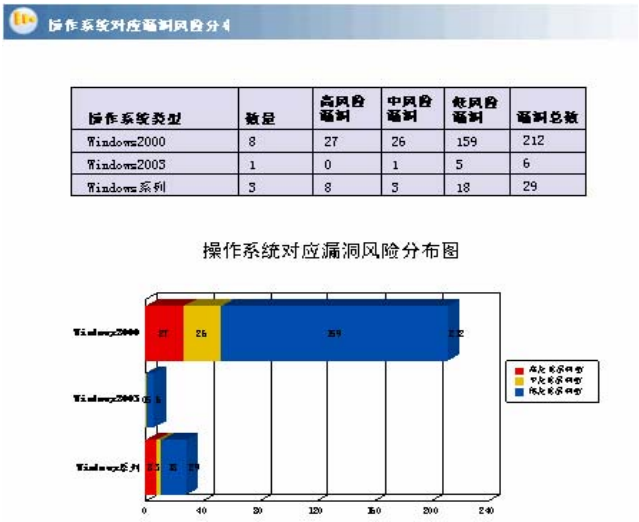
天镜具备全面详细的分析报告能力，可根据安全管理的不同角色定位按照要求生成面向主管领导、管理人员、技术人员的不同类型的报告。这些报告包括：分时间扫描任务执行报告、分时间扫描任务执行结果、报告不同时间的扫描结果趋势比较、管理性简报、技术报告、评估报告以及扫描采用策略报告

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

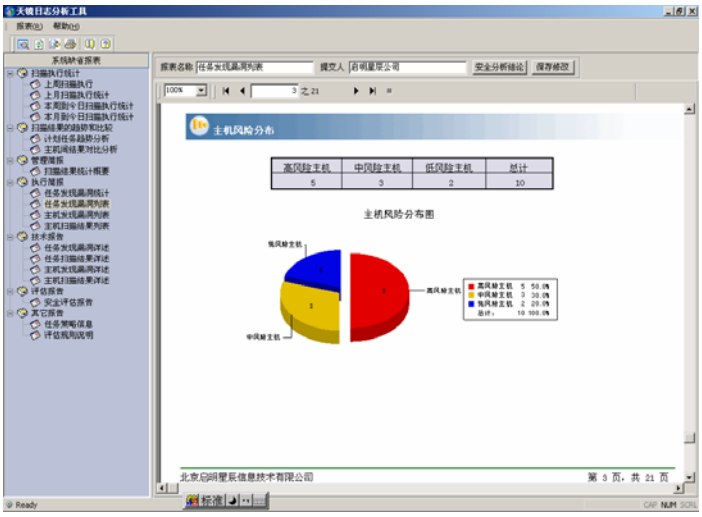
扫描结果不同分类的统计信息



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

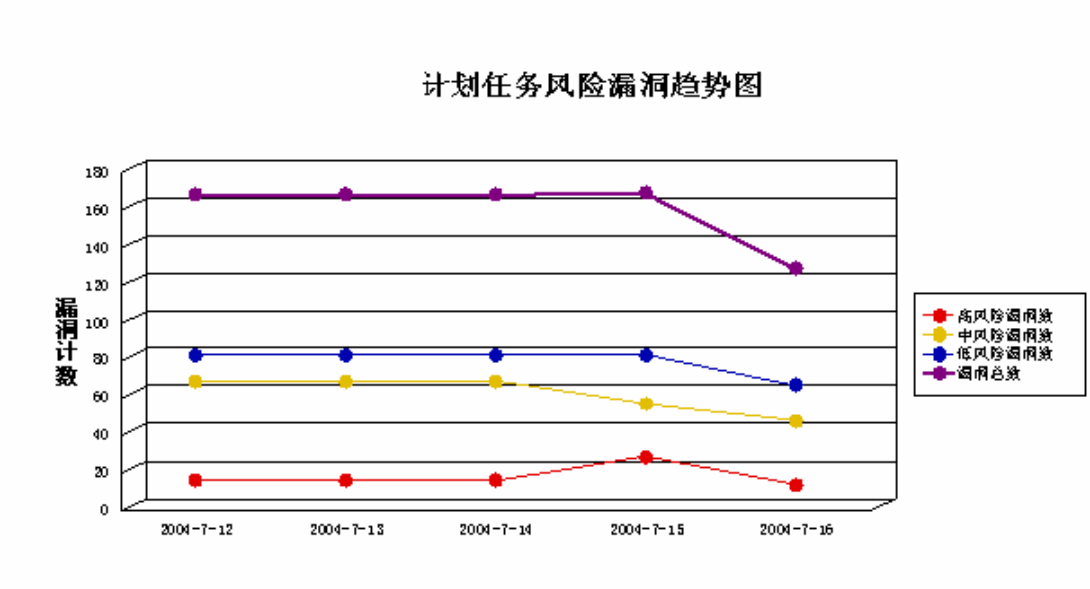
操作系统对应漏洞风险分布图

2） 评估结果



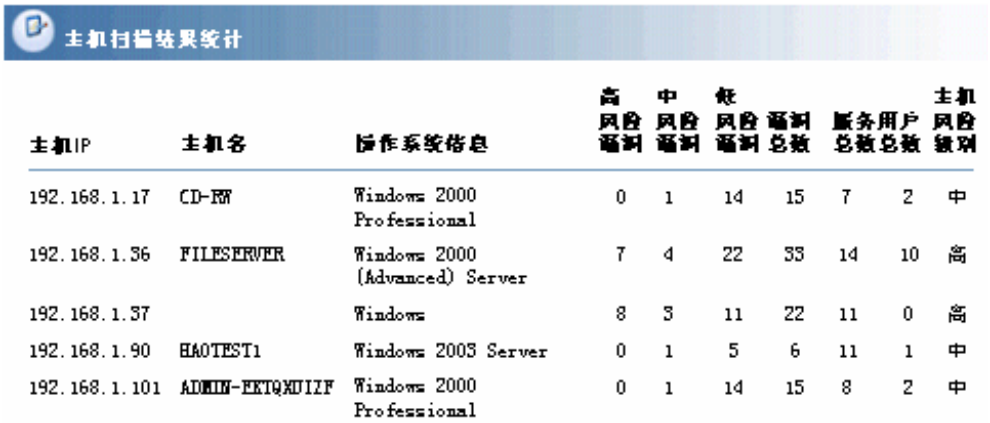
4.5.1 趋势分析

扫描结果的趋势分析



4.5.2 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-FBF	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-FETQXUIIF	Windows 2000 Professional	0	1	14	15	8	2	中

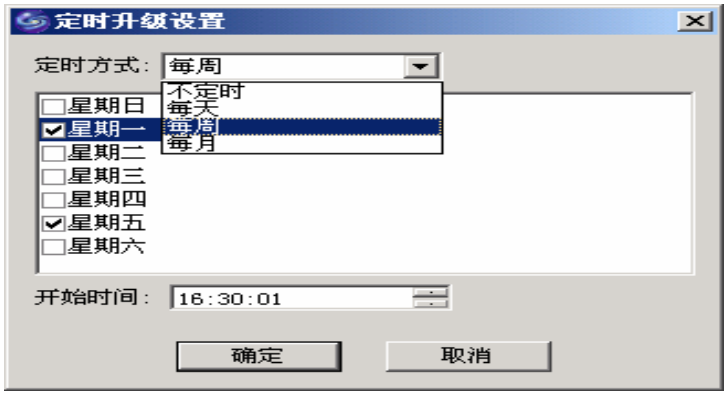
4.6 安全信息手册

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。

4.7 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。



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。