SCANNER
亿阳网警安全扫描器
技术白皮书

Version 1.0

文档编号：SCANNER3498
2003 年 9 月 10 日

版权说明

商标信息

北京亿阳信通股份有限责任公司
网站：www.boco.com.cn
地址：
邮编：
电话：
传真：
Email：

目录

前言

文档范围

本文档主要介绍网络安全扫描器（以下简称：SCANNER）的技术相关特性，主要功能，典型应用方式和各种性能指标等。

期望读者

期望了解本产品主要技术特性的拥护、系统管理员、网络管理元等。本文档假设您对下面的知识有一定的了解：

- Unix 和 Win 操作系统；
- Internet 协议；
- 网络安全相关基本知识。

内容总结

第一章：产品概述
第二章：产品功能
第三章：产品检测范围
第四章： 产品特点
第五章：产品技术特点
第六章：性能指标
第七章：产品运行环境
第八章：产品型号

获得帮助

安全相关资料可以访问公司安全网站：http://security.boco.com
本产品相关最新信息可以访问网站：http://security.boco.com/scanner/
本产品的技术支持可以拨打电话：
您也可以给技术支持部门发电子邮件，Email 地址是：
yanweihai@boco.com.cn

1 产品概述

亿阳网警扫描器是北京亿阳安全利用自身的技术优势和技术条件开发的，用于网络系统安全性检测和分析的专业工具。该工具参考了国外成熟技术、是自主版权、自主设计、自主开发的符合我国国情的民族化的安全产品。该工具是适用于信息安全执法机构及其它指定的政府及关键部门的专用检测工具，具有极大的专业性和专用性。亿阳网警扫描器已被指定为信息安全主管部门的专用检测工具。

2 产品功能

2.1 32大类800项全方位网络安全漏洞检测

亿阳网警扫描器可检测国际权威组织公布的网络安全漏洞共计达 800 条，这些漏洞分为 32 个类别，如下表所示：

表 2.1 检测漏洞分类表

分类 ID	分类名称
01	端口扫描(Port Scaning)
02	后门程序(Backdoor)
03	口令检测(BruteForce)
04	浏览器(Browser)
05	CGI 脚本(Cgi-Bin)
06	进程和服务(Daemons)
07	数据库(DataBase)
08	域名服务(DNS)
09	拒绝服务(DOS)
10	防火墙(FireWall)
11	文件传输服务(Ftp)
12	信息获取(info)
13	网上即时消息(Instant_Messaging)
14	LDAP
15	网络环境(NetWork)
16	网络嗅探器(NetWork_Sniffers)
17	网络文件服务(NFS)
18	网络信息服务(NIS)
19	协议欺骗(Protocol_Spoof)
20	路由器和交换机(Router&Switch)
21	RPC 攻击(RPC)
22	NetBIOS
23	电子邮件(E-Mail)
24	简单网络管理(SNMP)
25	NT 操作系统强壮性检测(NT Critical Issues)
26	NT 补丁程序检测(NT Patches)
27	NT 策略配置检测(NT Policy Issues)
28	NT 注册表检测(NT Registry)
29	NT 相关服务检测(NT Services)
30	NT 用户检测(NT Users)
31	Web 服务器(Web Servers)
32	X-Windows

2.2 详尽的漏洞解释和补救说明

亿阳网警扫描器中对每一条漏洞均有详尽的漏洞解释，包括漏洞 ID 号，漏洞名称，漏洞描述，漏洞危害度和相关参考等。并对漏洞的补救提供详细的说明和建议，包括配置说明，补丁信息或相关厂商网址的链接。

2.3 专业和预制两种配置方式

亿阳网警扫描器预制 10 种针对特殊行业的检测配置，可由用户通过用户界面直接选取，方便快捷，大大缩减进行检测配置的繁琐步骤。对于拥有专业水平的用户，亿阳网警扫描器提供专业配置方式，其中包括每一项漏洞检测的选取，以及漏洞检测中的参数设置，这种灵活的配置方式可满足不同网络环境的检测工作要求。

2.4 即时和定时两种检测方式

亿阳网警扫描器提供两种检测方式，即时方式适用于现场检测和突击性安全检查，定时方式适用于定期检测或非工作时间检测。定时方式可以有效避开系统运行时间，在系统相对空闲时区进行检测工作，从而减少检测过程中对网络系统的影响。定时检测方式特别适合 ISP、证券等不可中断网络系统的检测。

2.5 多种格式的检测分析报告

亿阳网警扫描器提供文本（TXT）、超文本（HTML）、WORD 文档（RTF）三种格式的报告输出，同时还有报告分级功能，适用于不同级别用户的要求。检测报告中包含检测出的每一个漏洞的详细解释、危害度、相关建议等信息，并使用形象的多种图形和表格进行统计分析表示。

2.6 联机自动升级

众所周知，信息安全是动态的，每一天每一时刻都有可能有新的安全漏洞被发现，检测工具必须及时快速地升级才能够检测出新的安全漏洞，亿阳网警扫描器提供最快速最便捷的升级方法：联机自动升级功能。只要与 Internet 相联，点击一下产品中的升级菜单按钮，整个产品升级过程会全自动完成，升级后的产品即可检测最新发现的安全漏洞。建议用户至少每两周升级一次。

3 产品检测范围

亿阳网警扫描器的检测范围涉及到操作系统、网络设备、安全防护设备和应用程序等。

3.1 操作系统

包括 Windows95/98/NT/Me/2000/XP 等系统，Novell 系统，SunOS 系统，Linux 系统，IRIX 系统，DG-UX 系统，AIX 系统，HP-UX 系统，BSD 系统等。

3.2 网络设备

包括路由器，交换机，网关，网络打印机，调制解调器等。

3.3 安全防护设备

包括防火墙，监控器，网管，认证中心等。

3.4 应用程序

包括 CGI/ASP/JSP 程序，数据库系统，邮件系统，浏览器，后门程序等。

4 产品特点

4.1 自主版权的网络安全扫描器

目前，国外产品中也有相似的网络安全检测工具，但均存在不同程度的技术出口限制，或者仅允许较低较旧版本的出口，或限制某些技术含量高和敏感的检测模块的出口。国外产品针对中国定制的版本系统均存在一定程度的技术保留和技术隐藏成分，更有甚者，在这些定制版本中含有隐秘的后门程序，以达到他们不可告人的政治和军事目的，所以国外检测工具产品是不可信赖的。

4.2 自动化安检工具

稍具规模的网络系统均包含大量的计算设备和网络设备，网络整体安全情况比较复杂，加之网络系统中的技术人员水平参差不齐，手工检测效率低，检测结果不一致，亿阳网警扫描器是一个统一的高效率的自动化检测工具，具有友好的用户界面，方便灵活的系统配置功能，能够对网络系统的整体安全性进行实时的检测和分析。

4.3 满足特殊要求

二十一世纪是信息化的世纪，网络技术和网络应用飞速发展，这种情况下，党政机关技术安全保卫部门以及证券系统迫切需要自动化的安全检测工具，对党政机关内部以及证券系统的网络系统安全性进行有效的和全面的技术检测，亿阳网警扫描器本身具有的专业性和专用性使得它能够满足这种特殊的应用需要。

4.4 统一解决新技术追踪问题

众所周知，当今网络技术飞速发展，日新月异，伴随而来的网络安全问题也层出不穷。每隔一段时间，国际权威组织 CERT 都公布大量的网络安全漏洞，这些漏洞涉及操作系统、网络设备、安全设备或应用软件的最新技术，对于国内网络系统，不可能也没有必要花费大量的人力物力来长期追踪这些新技术以及出现的新漏洞，更做不到及时地检测和发现这些新漏洞在本身网络系统中的存在。亿阳网警扫描器通过自身检测模块的不断更新和调整，将国际权威组织公布的最新安全漏洞在最短的时间段内加入到安全检

测项中，使用户能够得到及时的和最新的安全检测服务，从而统一解决了新技术追踪问题。

5 产品技术特点

5.1 适用所有基于TCP/IP网络系统的检测

亿阳网警扫描器可以对所有基于TCP/IP协议的网络系统进行检测，其中包括局域网，城域网和广域网。亿阳网警扫描器可以检测任何与Internet相连接的网络系统。

5.2 高效率的多线程双重并行检测

亿阳网警扫描器内部采用多线程技术，实现了多目标多模块双重并行检测，大大缩短了检测时间，提高了检测效率。

5.3 支持对Novell系统的检测

一些企业特别是证券公司网络系统中仍然存在一定数量的Novell系统，亿阳网警扫描器支持对Novell系统的检测，可确保整体网络系统的安全性。

5.4 可扩充的框架结构易于快速升级

亿阳网警扫描器的内部设计采用可扩充框架结构，实现检测模块化处理，确保新的网络安全漏洞的检测功能能够方便快捷地加入到产品中。

5.5 用户界面简洁

亿阳网警扫描器具有友好的用户界面，仅需输入检测目标和必要的检测配置既可自动进行检测，检测整个过程无须用户干预，检测结束后自动生成检测报告。亿阳网警扫描器的操作界面非常简洁，如下图所示：

（待加）

图 5.1 亿阳网警扫描器主界面

6 性能指标

6.1 扫描速度性能指标

典型情况下的扫描速度指标如下表:
表 1:100M 局域网情况

扫描主机数量	扫描时间
1-10	（待加）
10-20	（待加）
20-40	（待加）
1 个通常 C 类网络(60%以上主机存活)	（待加）

表 2:10M 局域网情况

扫描主机数量	扫描时间
1-10	（待加）
10-20	（待加）
20-40	（待加）
1 个通常 C 类网络(60%以上主机存活)	（待加）
10 个 C 类(总共约 50 主机存活)	（待加）

6.2 扫描带宽占用指标

典型工作情况下占用带宽为 8~28kb/s。

6.3 漏洞检测数量分类指标

截止到 2003-9-10，SCANNER 拥有漏洞检测插件如下：

漏洞类型	记录数目(个)
信息探测类	（待加）
网络设备与防火墙	（待加）
RPC 服务	（待加）
Web 服务	（待加）
CGI 问题	（待加）
文件服务	（待加）
域名服务	（待加）
Mail 服务	（待加）
Windows 远程访问	（待加）
数据库问题	（待加）
后门程序	（待加）
网络拒绝服务	（待加）

其他服务	（待加）
其他问题	（待加）
总计	

7 产品运行环境

硬件要求

CPU： PIII 400 以上

内存： 128M（建议 256M）

硬盘剩余空间：50M 以上

网卡： 10M/100M 自适应

调制解调器： 56K

显示分辨率： 800*600 256 色

软件要求

Windows 2000 Professional 中文版 或

Windows 2000 Server 中文版 或

Windows XP Professional 中文版

特别说明：本产品不能运行在 Windows95/98/NT/Me 等系统上。

8 产品型号

亿阳网警扫描器具有以下两种产品型号：

限 IP 型

纯软件形式，限定检测 IP 地址范围，即只能对加密锁中的指定 IP 地址进行检测，适用于企事业单位内部网络系统的网络安全漏洞检测。

不限 IP 型

纯软件形式，不限 IP 地址，即可由用户输入并检测任意 IP 地址，适用于国家信息安全主管部门和金融证券等监管部门。