UNIS XSCAN 系列漏洞扫描系统

UNIS-XSCAN-G10

UNIS-XSCAN-G20

产品概述

UNIS XSCAN 系列漏洞扫描系统是由北京紫光恒越网络科技有限公司（以下简称 UNIS 公司）在多年的安全研究沉淀和服务实践经验的基础上，自主研发的一款用于评估网络运行环境安全风险的产品，可以对各类服务器、网络设备、安全设备等操作系统环境、数据库环境、Web 应用等进行综合漏洞扫描检测。该产品主要用于分析和指出存在的相关安全漏洞及被测系统的薄弱环节，给出详细的检测报告，在业务环境受到危害之前为安全管理员提供专业、有效的安全分析和修补建议，该产品已经成为安全管理员的主流使用工具。该产品广泛应用于政府、公安、教育、卫生、电力、金融等行业，帮助用户解决目前所面临的各类常见及最新的安全问题，同时满足如等级保护、行业规范等政策法规的安全建设要求。

产品特点

◆ 融合多种漏洞检查能力为一体

UNIS XSCAN 系列漏洞扫描系统能够全方位检测 IT 系统存在的脆弱性，发现信息系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

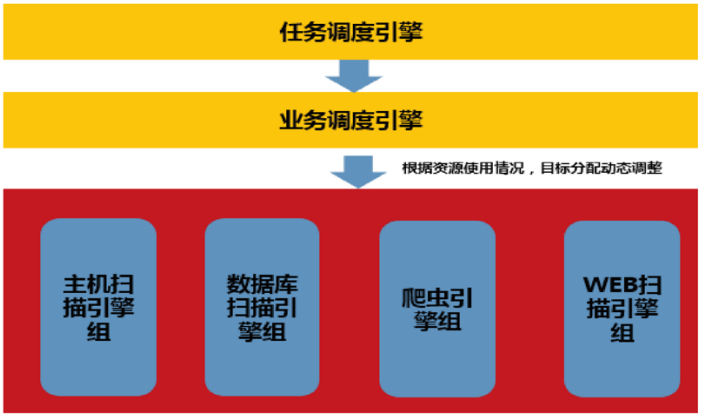
◆ 领先的扫描技术

产品采用 B/S 设计架构，运用高效稳定的核心扫描引擎，综合多种端口检测技术、智能服务识别、授权登陆扫描、安全优化扫描、知识键依赖检测等先进技术，通过脚本预加载方式，提高脚本调度效率和执行效率。Web 漏洞扫描采用智能页面爬取和手动页面抓取相结合实现立体式页面抓取、资源动态调节、代理缓存机制和实时任务调度等领先技术，实现了对大规模网站的快速、稳定的扫描。全面、深度、准确地检测网络中潜在的各种应用弱点，有助于提高主动防御能力。

多种端口检测技术	授权登录扫描	智能爬虫功能
智能服务识别	定时扫描功能	主动与被动扫描
多种服务识别	安全优化扫描	手动爬取功能
知识键依赖检测	漏洞先进管理	COOKIE录制

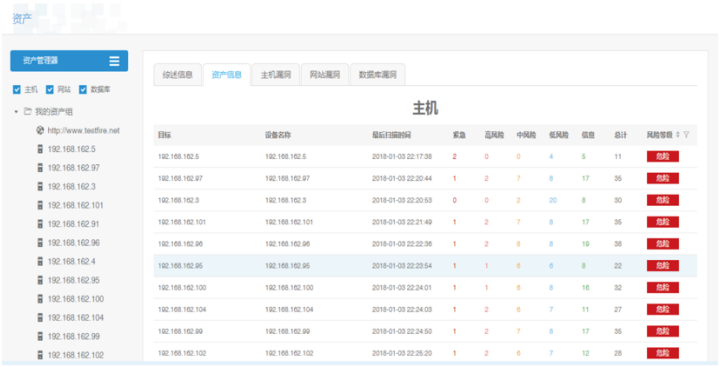
◆ 先进的引擎管理

为了保证漏洞扫描的可靠性和稳定性，产品运用多引擎分离技术，各引擎相互独立，采用通讯方式实现引擎间交互，引擎包括（任务调度引擎、业务调度引擎、系统漏扫引擎、数据库扫描引擎、爬虫引擎和 Web 漏洞检测引擎）。根据引擎资源的使用情况，目标调度和资源分配实现动态调整，在保证准确率的前提下大幅提高了检测的速度。



◆ 精细的资产管理

引入以资产为导向的漏洞管理模型，实现资产风险快速定位。精细的资产管理，能够对企业的网络资产进行完整有序的梳理，主动与被动相结合的资产发现，帮助企业深度抓取 IT 边界及遗忘资产，并通过计算模型完成资产分级与建模，并以逻辑拓扑的形式进行组织并图形化展示。通过对扫描资产的管理，主动发现与周期扫描进行监控资产安全漏洞，并能够结合漏洞评价，计算主机、网络、数据库、Web 应用的脆弱性风险，直观了解企业全网资产的健康状态，为风险评估和风险监控提供必要支撑。

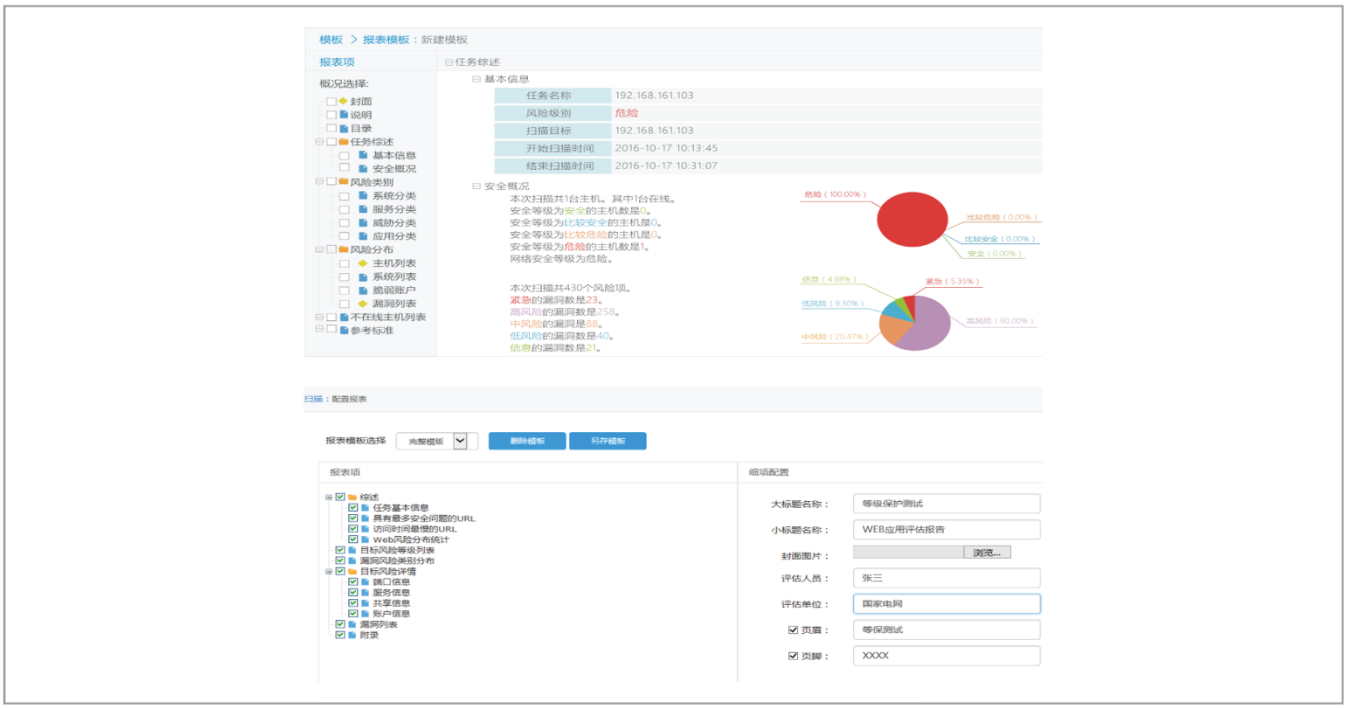


◆ 丰富的漏洞知识库

系统漏洞知识库涵盖对各种主流操作系统、网络设备、安全设备、数据库、应用程序的漏洞检测，漏洞知识库数量国内领先。知识库中的漏洞信息、漏洞描述支持全中文展示，同时兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等国内外主流标准。Web 漏洞知识库全面支持 OWASP TOP 10 检测，支持对当前各种主流的 WEB 应用、WEB 容器、国内外主流 CMS 及各类第三方组件的常见漏洞检测。漏洞修复建议清晰、详细，可操作性强。漏洞知识库更新频率保持每周至少一次，重大漏洞即时更新。

◆ 人性化的报表展示

采用报表与图型相结合对扫描结果进行分析，可以方便直观呈现给用户，并提供漏洞分级、相应加固建议方案以及自定义报表内容。定性的趋势分析和定量的风险分析，让用户更加直观地了解当前网络安全状况。用户可以自定义报表样式，保存成模板，满足用户不同应用场景。产品支持 HTML、WORD、PDF、XML、CSV 等主流格式的报表输出。产品支持常规报表、行业报表（OWASP Top 10）、等级保护合规报表、趋势分析报表，提供多层次、多角度、多种格式、满足不同管理角色需求的详细的脆弱点分析报表。



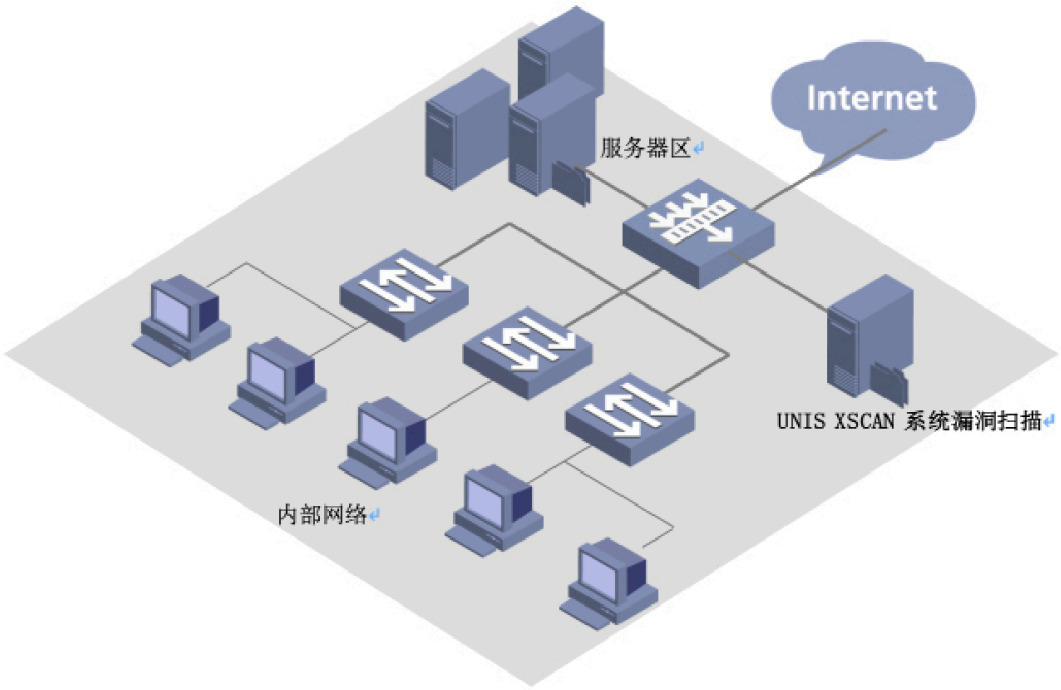
产品规格

属性		XSCAN-G10/XSCAN-G20
资产管理	资产管理功能	支持资产分组管理 支持资产导入导出功能 支持查看各资产风险等级统计功能
	资产自动发现	资产自动发现和手动添加相结合功能
扫描对象	操作系统	Windows、Linux、Unix 等主流操作系统漏洞扫描
	数据库	MSSQL Server、Oracle、MySQL、DB2、Informix 等主流数据库漏洞扫描
	应用服务	FTP、RDP、SMTP、POP3、WWW 等主流应用服务漏洞扫描
	设备	支持 H3C、HuaWei、Cisco、HP、Nortel、Juniper、Apple、Arris、Symantec 等主流的网络设备及安全设备漏洞扫描
	Web 服务器	IIS、Websphere、Weblogic、Apache、Tomcat、zope 等主流 Web 服务器
	第三方组件	Discuz、大汉 CMS、骑士 CMS、CMSEASY、齐博 CMS、通达 CMS、XHP CMS、Drupal、Joomla 、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2 等国内外常见第三方组件等各类开源系统漏洞扫描
扫描	扫描任务	支持对多个扫描任务并发执行，多任务自动调度，支持扫描计划任务管理，一次性或周期性地执行扫描任务，并自动发送扫描结果
	口令猜测	支持多种口令猜测方式，包括利用 FTP、TELNET、SMB、SSH、RDP、VNC 等主流协议进行口令猜测，允许外挂用户提供的用户字典与口令字典
	深度扫描	支持主动扫描、被动扫描两种模式 支持手动爬行功能 支持 Cookie 录制功能
	多种网站认证方式	多种网站认证方式：支持包括 Basic、Digest、NTLM 在内的认证方式，支持 HTTP 和 SOCKS 代理，并支持各种代理的认证方式
	动态爬虫	支持 Web2.0，通过执行网页中的 JavaScript 脚本获取其中的链接
		解析 FLASH 中 URL，链接抓取更加全面
		模拟鼠标点击提取页面中的 URL
		从 Javascript 文件中提取 URL

属性		XSCAN-G10/XSCAN-G20
扫描	HTTPS 协议扫描	支持 HTTPS 协议：能够自动获取所有必须的要素，对基于 SSL 传输的内容进行分析，可对网银、证券交易等基于 HTTPS 协议的 WEB 应用进行自动安全评估
	网站目录结构	支持对目标网站进行完整深度扫描，获取网站文件列表，在扫描过程中区分目录、文件等大小写设定；并支持检测网站是否备案
	流量限制	支持对 http 连接请求进行流量限制
	关键字检测	对含有特殊关键字的链接忽略检测的功能，防止影响客户的业务正常支行
	HTTP 表单自动填充	HTTP 表单自动填充和对包含 textaea 元素的表单进行测试
	支持常见的 Web 应用弱点检测	支持 OWASP TOP 10 等主流安全漏洞，如：SQL 注入、Cookie 注入、XSS 跨站脚本、框架注入、链接注入、隐藏字段、CSRF 跨站伪造请求、命令注入、命令执行、代码注入、遍历目录、弱口令、LDAP 注入、表单绕过、服务器端包含注入、EL 表达式注入、文件包含、管理后台、敏感信息泄漏、第三方组件、其他各类 CGI 漏洞等各种类型
	取证功能	利用发现的漏洞，通过渗透测试来验证漏洞存在的真实性
报表	专业报表	支持生成任务报表，行业报表和等级保护报表
	报表格式	支持 PDF、Word、HTML、XML，WEB 漏扫模块还支持 Excel、CSV
	报表模版	支持自定义报告内容和报表样式
系统管理	产品升级	支持在线升级、离线升级、定时升级
	磁盘告警	支持设置磁盘使用告警，当磁盘空间达到上限，系统将发出告警
	数据备份	支持系统数据的备份和恢复功能
	日志管理	支持记录漏扫操作日志、告警日志，支持日志记录查询、删除、导出至 syslog 服务器等
	网络工具	系统内置一些常用的网络工具，包括 ping、路由跟踪、端口扫描等
	加解密工具	系统内置 MD5、SHA1、Base64 等常用加解密工具
	HTTP 工具	系统内置 HTTP GET/POST/HEAD/PUT/DELETE/OPTIONS/TRACE 等模拟请求测试工具

典型组网

UNIS XSCAN 系列漏洞扫描系统一般部署在运维管理区，与扫描对象保持 IP 可达，通过配置扫描任务定期地对网络中多个不同的网段的主机、数据库、Web 应用等进行全面、深入的检测，同时生成相应的漏洞解决方案，用户根据这些解决方案来对目标系统和应用做相应的加固和防护，及时将网络的安全风险降到最低。



UNIS XSCAN 系列漏洞扫描系统

北京紫光恒越网络科技有限公司

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-62166890
传真：010-51652020-116
版本：

http://www.unishy.com

客户服务热线
400-910-9998