文档密级：公司公开

优炫综合安全评估系统

产品介绍

北京优炫软件股份有限公司

目　　录

1　产品概述 1

2　产品优势 2

3　主要功能 4

4　典型部署 6

1 产品概述

图　2U 设备外观示意图

优炫综合安全评估系统（UXSINO Scan Platform，简称 UX-SCANP）是基于漏洞知识库，通过采集信息、执行漏洞检测脚本对指定的远程计算机系统、应用程序、数据库、WEB 服务、网络设备、安全设备的安全脆弱性进行检测，发现可被利用漏洞、不安全配置并实时预警的一款主动防御产品。

该系统涵盖了系统漏洞检测、网站监控预警、数据库漏洞检测、基线配置检查、弱口令检测和等保合规检查等功能模块。能够全面发现信息系统中存在的各种脆弱性问题，包括各种安全漏洞、安全配置问题、不合规行为等，还能够对网站可用性、篡改、敏感关键字、网马和暗链等进行 24 小时不间断监测、实时预警，形成整体安全评估报告，对安全状况进行可视化展示。

2 产品优势

(1) 一键资产识别

1) 扫描发现网络中存活的主机；
2) 支持对目标主机执行多种方式的端口扫描；
3) 识别端口对应的服务；
4) 识别操作系统类型，如 Windows、Linux、Unix 等；
5) 识别网络中安装的数据库类型，如 MySQL、MSSQL、Oracle 等。

(2) 完备的漏洞规则库

产品包含将近 50000 条策略，包括有：WINDOW 测试、UNIX 测试、数据库测试、WEB 测试、网络设备测试、防火墙测试等，涵盖了所有常见的系统。目前漏洞知识库完全兼容 CVE 国际标准，按风险级别分为高、中、低、信息四个级别。

另外还提供完善的漏洞风险级别、漏洞类别、漏洞描述、漏洞类型、漏洞解决办法及扫描返回信息，并提供有关问题的国际权威机构记录（包括 CVE、Bugtraq 编号），以及与厂商补丁相关的链接。

(3) 高效的检查速率

产品采用并发规则、并发任务扫描等多项技术及独创的脚本引擎调度算法，对同样的目标系统进行检测时，扫描的速度大大高于其它同类型扫描产品。另一方面由安全研究小组精心编写的漏洞检测规则插件也很好的保证了检测的准确性，从而保证了在正确率的前提下大幅提高了检测的效率。

在进行大规模扫描时，产品支持分布式部署，充分利用多台硬件资源与带宽，加快扫描速度。

(4) 先进的漏洞管理方案

扫描系统遵循“漏洞生命周期”原理，并将之划分为五个阶段，即漏洞扫描、漏洞预警、漏洞分析、漏洞修复、修复验证，最终达到漏洞被修复的效果，形成漏洞管理闭环。

(5) 丰富的监控报告

1) 多维度的监控报告展示；
2) 根据漏洞类型展示风险情况；
3) 根据危险等级展示风险情况；
4) 详细的漏洞内容展示；

5) 支持导出多种格式的报告，如 pdf、word、html 等。

(6) 实时预警

（1）支持实时系统预警；

（2）支持实时邮件预警；

（3）支持实时短信预警。

(7) 权威、高效、专业的等保合规检查

以公安部制定的信息安全等级保护检查工具箱技术规范为设计理念，完全满足规范要求。

将耗时的政策检查自动化，实现了信息安全等级保护工作检查的流程化管理，让耗时的政策检查更快捷高效。

3 主要功能

(1) 网站监控

a) 支持全部主流 Web 服务器，如 IIS、Apache、Nginx、Weblogic、Websphere 等；

b) 支持扫描各种编程语言，如 PHP、ASP、ASPX、JSP 等；

c) 支持全部主流数据库，如 Oracle、Mysql、MSSQL、DB2、Postgresql 等；

d) 支持全部常见 CMS，如 Wordpress、Joomla!、Phpcms、织梦 CMS 、Discuz!等；

e) 支持全部主流框架，如 Struts2、Spring 等。

(2) 系统漏扫

a) 可对操作系统、应用程序、WEB 服务器、数据库、网络设备、虚拟化设备等进行扫描；

b) 漏洞知识库包括将近 50000 条漏洞规则，覆盖了缓冲区溢出漏洞、拒绝服务攻击漏洞、弱口令、信息泄露漏洞等全部常见漏洞；

c) 支持安全扫描，保证扫描过程中目标系统正常运行；

d) 支持对 EXSI 进行登录扫描。

(3) 数据库扫描

支持所有主流数据库，如：Oracle、MySQL、SQLServer、Infomix、Sybase、达梦、人大金仓、DB2 等。

包含提权漏洞、缓冲区溢出漏洞、访问控制漏洞、SQL 注入漏洞、执行权限过大漏洞、访问权限绕过漏洞等几千个检查项。

(4) 基线配置核查

1) 支持常见操作系统的安全登录检测。

   a) 主流 Windows 系统（XP/2003 Server/WIN2008/Win 7/win8 等）；

   b) 支持 AIX、Solaris 系统、HP-UX 等；

   c) Linux（Centos、Redhat、suse 等）；

   d) 国产操作系统(红旗、中标麒麟等)。

2) 支持常见数据库，包括 Oracle 、DB2、Mysql、SQL Server、达梦数据库的检查；

3) 支持常见中间件，包括常见的 Apache、IIS、TOMCAT 等主流服务软件；

4) 支持常见网络及安全设备，包括 Cisco、Juniper、华为、H3C 等厂家的主流产品的配置检查；

5) 支持常见虚拟化设备，包括 Exsi、Xenserver 等。

(5) 弱口令扫描

支持对 SMB、FTP、POP3、SMTP、SSH、TELNET、SNMP、RDP、redis、Oracle、MySQL 等协议进行弱口令扫描；支持自定义用户名、口令字典。

包含提权漏洞、缓冲区溢出漏洞、访问控制漏洞、SQL 注入漏洞、执行权限过大漏洞、访问权限绕过漏洞等几千个检查项。

(6) 木马病毒检查

a) 支持对系统关键目录、全盘进行木马病毒扫描，支持自定义扫描目录；

b) 支持发现系统中的木马程序、Rootkit、间谍程序、流氓软件、蠕虫病毒、其它恶意程序等。

(7) 网站恶意代码检查

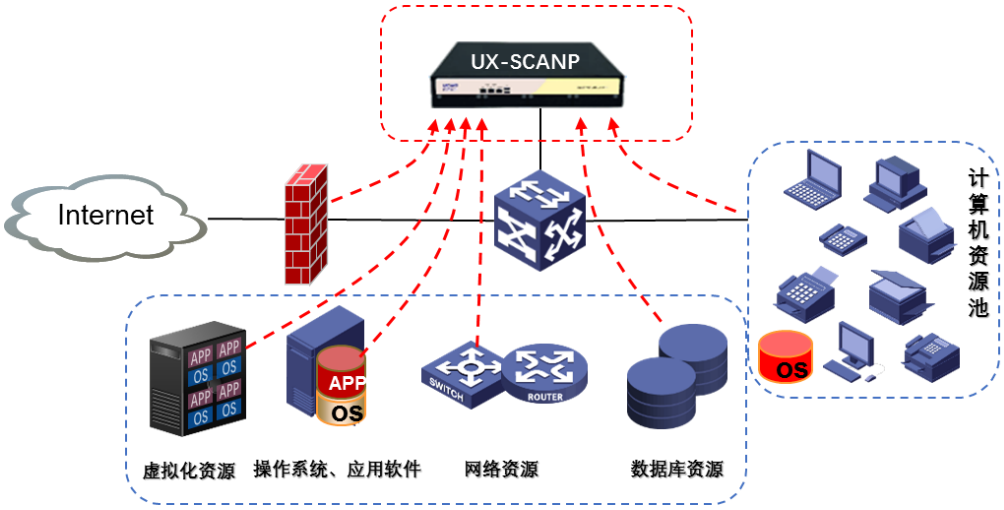
a) 检查 WEB 服务器目录路径中 ASP、ASPX、JSP、PHP、CSS 等是否感染或存在恶意代码；

b) 支持 IIS、Apache、nginx、weblogic、Websphere、Tomcat 等 WEB 服务器。

(8) 等保合规检查

依据《信息安全 等级保护检查工具箱技术规范》，在深入分析与研究常见安全漏洞以及流行的攻击技术基础上，通过与漏洞扫描、配置核查模块联动，实现对物理安全、主机安全、网络安全、应用安全、数据库安全等系统及配置检查，实现对信息系统“定级、备案、测评、整改、安全自查和监督检查”全过程的监督管理。

4 典型部署


UX-SCANP
Internet
计算机资源池
OS
APP
OS
SWITCH
ROUTER
虚拟化资源
操作系统、应用软件
网络资源
数据库资源