DPtech Scanner1000 漏洞扫描系统

杭州迪普科技有限公司

产品概述

漏洞，是指在硬件、软件、协议实现或系统安全策略上存在缺陷，攻击者能够在未授权的情况下对系统进行访问或破坏。它会成为入侵者侵入系统和植入恶意软件的入口，影响系统用户的切身利益。漏洞扫描工具是一种能在计算机、信息系统、网络及应用软件中查找安全弱点的程序。通过对目标系统进行探测，向目标系统发送数据，并将反馈结果与漏洞特征库进行匹配，分析出目标系统上存在的安全漏洞。

随着 Web 应用越来越普及，针对 Web 漏洞扫描的需求越来越迫切，迪普科技推出 DPtech Scanner1000 系列漏洞扫描系统。DPtech Scanner1000 具备主机漏洞扫描、Web 漏洞扫描和安全基线检查三个功能模块，在保留传统的漏洞扫描系统的基础之上，还能够针对 Web 服务，如 :Web 网站、B/S 架构业务系统进行漏洞扫描。同时，Scanner1000 还能够根据不同行业的安全标准，进行安全基线检查，满足等级保护中安全管理方面的要求。

产品特点

- **轻松应对超大规模的扫描目标**

  DPtech Scanner1000 可支持超过 1000+以上的混合扫描目标配置，不论对象为主机 IP 地址，或者网站域名 URL 地址，均支持批量导入，一次性完成针对大规模目标的扫描任务。

- **全面精确的 Web 安全扫描**

  DPtech Scanner1000 支持针对 Web 应用系统进行代码级检测，帮助用户消除跨站脚本攻击、SQL 注入、网页挂马等潜在 Web 威胁

- **主动防御，智能联动**

  DPtech Scanner1000 对防护对象进行安全扫描，将输出的扫描报告导入到 DPtech WAF3000 设备中，DPtech WAF3000 能够自动生成针对扫描结果中漏洞的相应策略，既减轻了维护人员工作量，同时又保证安全策略的准确性。

- **基线检查，安全合规**

  DPtech Scanner1000 能够根据不同行业以及不同等级的安全要求，灵活地调整基线标准，使得用户能够提前进行合规性检查，主动调整安全配置，保证基础设施能够满足安全管理维度的相关要求。

- **自动补丁管理，及时解决潜在风险**

  DPtech Scanner1000 能有效的和微软的 WSUS 服务进行联动，当检测到相关漏洞后，可以通知管理员在指定主机上启用相应的 WSUS 联动配置，当有漏洞补丁发布时，该主机就会主动到指定的 WSUS 更新服务器获取最新的漏洞修复补丁。

- **漏洞库自动更新，持续安全防护**

  DPtech Scanner1000 漏洞扫描系统采用迪普科技应用识别与威胁特征库 APP-ID，该特征库可进行自动、及时、准确的升级，从而确保漏洞判断准确无误。

产品系列

Scanner1000-Blade

Scanner1000-GS

Scanner1000-MS

功能价值

技术优势	功能价值
支持多种网络资产	支持终端设备、服务器、路由/交换设备等网络资产 支持多种操作系统（Windows/Linux/Unix）、应用服务、数据库
支持大规模目标扫描	支持超过 1000 以上的扫描目标对象 支持批量导入 IP 地址、域名 URL 混合的目标对象
安全基线检查	支持根据不同行业不同等级的安全要求，灵活地调整基线标准，主动发现和提出安全管理方面的整改意见
深度 Web 漏洞扫描	Web 服务器检测、插件检测、配置检测、注入攻击漏洞检测、注射攻击漏洞检测、远程文件检索漏洞检测、文件上传检测、FORM 弱口令检测、数据窃取检测、GOOGLE-HACK 检测、中间人攻击检测、Web2.0 AJAX 注入检测、Cookies 注入检测、弱口令扫描
网页木马检测	支持各种类型木马检测、木马分析、木马溯源
应用漏洞扫描	SMTP/POP3、FTP、SNMP、端口扫描、弱口令扫描
多种扫描方式	支持定时扫描、手动扫描等多种扫描方式
支持网络爬虫方式	可自定义扫描深度、预定义用户登录参数、提供交互式用户登录参数设置、支持并发扫描
自动漏洞修复能力	自动补丁管理，可与微软 WAUS 联动
丰富的报表功能	可提供扫描结果对比、漏洞报告、统计分析等多种报表类型，漏洞风险级别采用统一的 CVSS 国际标准评分，以更准确衡量漏洞的危险级别，为漏洞修补工作的优先级提供指导