H3C SecPath 漏洞扫描系统

产品概述

H3C SecPath 漏洞扫描系统是由新华三技术有限公司（以下简称 H3C 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、安平、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。

H3C SecPath 漏洞扫描系统产品外观图

产品特点

五合一扫描能力

H3C SecPath 漏洞扫描系统能够全方位检测 IT 系统存在的脆弱性，从系统扫描、Web 扫描、数据库扫描、安全基线扫描和弱口令扫描五大类发现信息系统、网站页面、数据库安全漏洞，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，检查不合规的设备配置，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，及时进行自我修补。

丰富的扫描对象

支持网络环境中几乎全部类型主机的漏洞扫描和脆弱性检测。

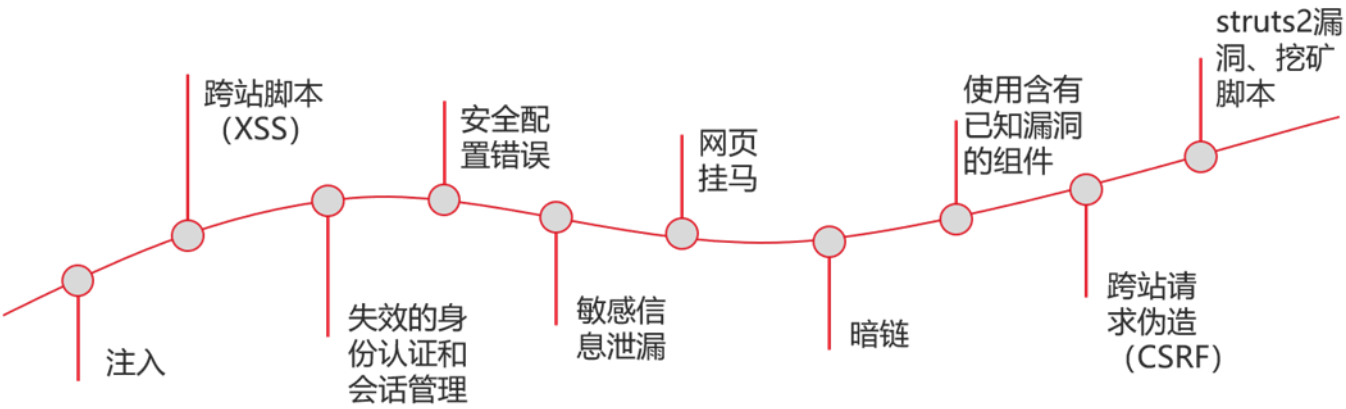
- 网络主机：服务器、客户机、网络打印机、移动设备、虚拟化设备等；
- 操作系统：Microsoft Windows 9X/NT/2000/XP/2003、苹果操作系统、国产操作系统、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD、HPUX 等；
- 网络设备：Cisco、Juniper、H3C、F5、3Com、Checkpoint 等主流厂商网络设备；
- 安全设备：Checkpoint、赛门铁克、Cisco、Juniper、Palo Alto 等主流厂商的安全设备；
- 应用系统：数据库、Web、FTP、电子邮件等。
- 工控设备：PLC、SCADA、DCS、工控专用网络设备等专业的工控设备；
- 物联网设备：国内知名摄像头厂商、索尼、Brickcom、佳能等摄像头设备；佳能、惠普等打印机设备；

全面的扫描能力

- 漏洞库涵盖丰富的安全漏洞和攻击特征，兼容国内及国际标准；
- IPv4/IPv6 双栈协议地址管理、漏洞扫描、安全报告、结果上送等；
- 系统登录扫描；
- 验证式扫描。

基于强大爬虫的 web 扫描能力

支持提供 OWASP 定义的 TOP 10 Web 威胁如注入（SQL 注入、Cookie 注入、Xpath 注入、代码注入、框架注入、Base64 注入、命令注入、操作系统命令注入）、XSS 跨站脚本、伪造跨站点请求（CSRF）、网页挂马、暗链、敏感信息泄露、安全配置错误等漏洞风险等漏洞扫描服务。通过基于爬虫的网站漏洞扫描技术，能够有效识别 Web2.0 以及 Flash，保障 Web 漏洞扫描的全面性。



国内外数据库厂商漏洞兼容

系统漏洞知识库涵盖各种主流的数据库厂商，涵盖各种常见的漏洞类型。

便捷的漏洞验证工具集

误报是一种常见的现象，提供一键式漏洞验证工具集，包含 SQL 注入漏洞验证、浏览器漏洞验证及通用漏洞验证。运维人员可以直接在系统界面中选择相应的协议并填充测试字段对目标进行漏洞验证。针对系统已发现的漏洞还可以实现一键填充式自动验证功能，降低人工操作难度的同时保障漏洞扫描结果的准确性。

产品规格

功能	特性及描述
网络协议	IPv4
	Ipv6

功能	特性及描述
任务管理	多方式任务录入：手动输入、资产导入、批量导入 支持定时执行、立即执行、周期执行 支持执行优先级别设置 支持新增系统扫描、Web扫描、数据库扫描、弱口令扫描、基线配置扫描任务
系统扫描	支持设置存活探测方式 支持SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS协议的登陆扫描
Web扫描	支持并发线程数设置 支持大小写敏感或不敏感的检测方式 支持Web扫描代理检测，能够使用HTTP代理和SOCKS代理方式 支持设置检测的最大页面数 支持设置爬虫爬取单个页面的大小 支持设置Web扫描的起始URL、网站域名、扫描根目录、例外URL 支持Cookie/Session、 Form、Basic、NTLM、Digest登录认证扫描
数据库扫描	支持主流数据库漏洞的检测，包括：Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix、人大金仓、神通、南大通用、达梦等 支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL认证，SID、数据库名称、实例名称及实例号等登录选项的设置 支持Postgres、MySql、MsSql数据库的在线登录验证
弱口令扫描	支持常见服务如TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、REDIS、SFTP弱口令检测 支持常见数据库如Oracle、MySQL、PostgreSQL、MsSQL、DB2、MongoDB的弱口令检测 支持设置对单个服务的口令猜解速率设置 支持设置单个服务口令猜解的并发线程数，值越大，探测速度越快
基线配置扫描	支持对常见网络设备、安全设备、操作系统、数据库、应用服务器等的配置核查 支持通过TELNET、SSH、SMB、RDP、WinRM协议进行安全配置核查
探测未知站点	支持自动探测网段的未知站点，并可转为WEB扫描资产
会话录制	支持Web会话录制，根据录制好的内容进行Web扫描

功能	特性及描述
报表管理	报表具备导出5种常见格式报表的能力，包括：Excel、Word、HTML、PDF、XML 支持自定义报表的logo及公司信息 支持报表导出压缩包设置密码导出 可跟据漏洞状态（新建、误报、已修复）筛选导出报表
系统管理	支持检测结束发送HTML报表至指定邮箱 支持检测结束发送短信、SNMP Trap、Syslog告警 支持对系统CPU、内存、磁盘、网络状态、设备授权到期、特征库授权到期设置告警及告警值 支持在线、代理方式、FTP方式、本地导入方式升级系统特征库 支持PING、WGET基本诊断工具 支持使用默认或自定义HTTP请求信息等验证通用Web漏洞 支持提供SQL注入验证工具、使用默认参数或自定义参数进行SQL注入漏洞验证 支持通过浏览器进行漏洞验证，自动跳转至对应漏洞页面进行漏洞验证

组网应用

H3C SecPath 漏洞扫描系统一般旁路部署在运维管理区，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。

- 单机部署

适用于网络较为集中，独立使用，中小型规模的网络环境，与被检测环境通信可达即可，部署方便“无损”部署，不影响客户网络和业务。

- 分布式部署

适用于层级网络结构，由总部集中进行管理、检查，网络规模较大的网络环境，统一下发、数据汇总、集中管理，统一评估，适满足大型或超大型网络环境部署需求。

选配信息

硬件主机选购一览表

模块	数量	备注
H3C SecPath SysScan-SE 漏洞扫描系统	1	必配<三选一>
H3C SecPath SysScan-ME 漏洞扫描系统	1	必配<三选一>
H3C SecPath SysScan-AE 漏洞扫描系统	1	必配<三选一>

硬件主机功能模块选购一览表

模块	数量	备注
H3C SecPath SysScan-SE Web 漏扫功能模块授权函	1	选配
H3C SecPath SysScan-ME Web 漏扫功能模块授权函	1	选配
H3C SecPath SysScan-AE Web 漏扫功能模块授权函	1	选配
H3C SecPath SysScan-SE 基线扫描功能模块授权函	1	选配
H3C SecPath SysScan-ME 基线扫描功能模块授权函	1	选配
H3C SecPath SysScan-AE 基线扫描功能模块授权函	1	选配

硬件主机特征库升级授权函选购一览表

模块	数量	备注
H3C SecPath SysScan-SE 漏洞库升级授权函（含操作系统、数据库、WEB 应用的漏洞规则库和基线特征库），1 年	1	选配
H3C SecPath SysScan-ME 漏洞库升级授权函（含操作系统、数据库、WEB 应用的漏洞规则库和基线特征库），1 年	1	选配
H3C SecPath SysScan-AE 漏洞库升级授权函（含操作系统、数据库、WEB 应用的漏洞规则库和基线特征库），1 年	1	选配

硬件主机可扫描 IP/域名数量授权函选购一览表

模块	数量	备注
H3C SecPath SysScan-E 扫描 64 个 IP 地址或域名授权函	1	首次必配<六选一>
H3C SecPath SysScan-E 扫描 128 个 IP 地址或域名授权函	1	首次必配<六选一>
H3C SecPath SysScan-E 扫描 256 个 IP 地址或域名授权函	1	首次必配<六选一>
H3C SecPath SysScan-E 扫描 512 个 IP 地址或域名授权函	1	首次必配<六选一>
H3C SecPath SysScan-E 扫描 1000 个 IP 地址或域名授权函	1	首次必配<六选一>
H3C SecPath SysScan-E 无限 IP 地址或域名授权函	1	首次必配<六选一>

云漏扫授权函选购一览表

模块	数量	备注
H3C SecPath SysScan-Cloud 漏洞扫描系统一年订阅授权函，64 个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统一年订阅授权函，128 个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统一年订阅授权函，512 个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统一年订阅授权函，无限制个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统永久订阅授权函，64 个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统永久订阅授权函，128 个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统永久订阅授权函，512 个可扫描 IP 地址。	1	必配<八选一>
H3C SecPath SysScan-Cloud 漏洞扫描系统永久订阅授权函，无限制个可扫描 IP 地址。	1	必配<八选一>

云漏扫特征库选购一览表

模块	数量	备注
H3C SecPath SysScan-Cloud 漏洞扫描系统/数据库/Web/基线功能 1 年特征库升级授权函	1	选配

安管一体机漏扫主机选购一览表

模块	数量	备注
H3C SecPath SysScan-VE 虚拟化漏洞扫描系统授权函,含数据库/系统扫描/Web 扫描/基线核查扫描功能	1	必配

安管一体机漏扫特征库选购一览表

模块	数量	备注
H3C SecPath SysScan-VE 漏洞库升级授权函（含操作系统、数据库、WEB 应用的漏洞规则库和基线特征库），1 年	1	选配

新华三技术有限公司
北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504