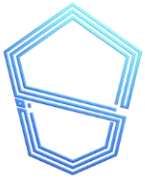
洞察安全检测系统

使用指南



科安软件
KEAN SOFTWARE

2022 年 4 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改或撤回，恕不另行通知。本公司已尽最大努力确保本文档内容准确可靠，但不提供任何形式的担保，任何情况下，科安软件均不对（包括但不限于）最终用户或任何第三方因使用本文档而造成的直接或间接的损失或损害负责。

信息反馈

如果您有任何宝贵意见，请反馈：

地址：陕西省西安市国家民用航天产业基地东长安街 501 号运维国际总部大厦 B 座 C703 室

电话：029-88747422

网址：http://www.ekean.cn/

目 录

第 1 章　产品简介

1.1 产品概述

洞察安全检测系统是专门用于网络设备、信息系统等用户资产扫描与漏洞发现以及终端设备基线安全检测的系统，可帮助用户提前发现网络资产与网络资产的安全性并给出有效的修复意见，通过提前发现安全漏洞可大大提高用户的网络安全防御能力，阻止黑客利用漏洞对用户网络资产进行攻击和破坏。

1.2 产品特点

科安洞察安全检测系统使用用户自定义的检测主题与检测频率对目标进行安全检测，任务运行漏洞检测时则使用了内部的安全匹配策略模型进行漏洞匹配，首先对设备进行识别，根据策略模型进行判定发送哪些 POC，而不是盲目且无效的发送全部漏洞库中的 POC，可对被检测主机影响最小化，并且给网络带宽带来最小的影响。

设备识别中不过只有应用识别与版本检测，还贴心加入了 HTTP/HTTPS 网站的页面截图，对用户现有资产进行整理。内部任务运行时，任务运行引擎自动分配任务量，对不同优先级的任务进行自动分配，大大提升了运行效率并减少了漏洞扫描时对网络的影响，从而保证用户网络应用正常运行。

第 2 章　安装部署与登录

2.1 配置要求

配置项	要求描述	数量
推荐配置要求	•Linux x86_64 based ubuntu 16.04	1 台
	•16 Core CPU	
	•内存：16GB RAM	
	•磁盘空间：最小 1T 可用空间	

2.2 安装部署

洞察安全检测系统通过旁路并联在网络中，通过配置扫描任务实现对网络中的设备进行发现，识

别以及漏洞检测。设备管理口连接管理网络，并配置相应的 IP 地址和默认网关。

2.3 系统登录

a.输入指定 URL

在浏览器地址栏中输入指定的 URL（例如：http://192.168.x.x:20216）进入登录页面，如下图：

图 1 登录页面

b.鉴权登录

在登录页输入已经注册的账号和密码（例如：账号 admin，密码 ******），输入对应的动态验证码，点击登录按钮，弹框提示登录成功，页面跳转到系统首页。

图 2 首页

注：权限说明

(1) admin 账号登录（超级管理员）：该账号具有最高权限，使用该账号登录可以展示所有的页面。账号：admin 密码：*******

(2) systemadmin 账号登录（系统管理员）：该账号的登录后的权限只展示部分页面，具有部分权限：扫描管理、漏洞管理、资产管理、历史报告和运维中心。账号：systemadmin 密码：*******

(3) audit 账号登录（审计员）：该账号登录后的权限只展示部分页面：日志中心。账号：audit，密码：*******

2.4 版本升级

此功能主要涉及到预升级设备的数据库、项目和 poc 的升级。

步骤：使用 admin 账号登录后，进入洞察安全检测系统首页，点击右下角版本升级按钮，会弹出下图所示弹窗：

图 3 升级页面

c.引擎版本升级

点击选择文件按钮，在本地选择对应的数据库压缩包（mysql.tar.gz），最后点击升级按钮完成升级。

b.漏洞版本升级

点击选择文件按钮，在本地选择对应的 poc 压缩包（poc.tar.gz），最后点击升级按钮完成升级。

c.系统版本升级

点击选择文件按钮，在本地选择对应的系统压缩包（insght.tar.gz），最后点击升级按钮完成升级。

d.全部升级

点击选择文件按钮，在本地选择对应的 all 压缩包(all.tar.gz)，最后点击升级按钮完成升级。

2.5 商品亮点

- 根据不同行业制定不同渗透测试方案，人工+系统辅助安全测试，出具检测报告与修复意见。
- 对于高危严重漏洞、资产由安全专家进行手工验证，输出检测报告与修复意见。
- 对信息系统资产进行基线检查核验，并出具报告与相关整改意见。
- 可以提供安全意识培训、应急响应、安全加固等安全服务，提高企业整体安全意识。

第 3 章　主要功能

1. 渗透测试服务

模拟模拟黑客攻击手法，对资产网络系统安全进行检测评估，包括系统漏洞、应用漏洞、程序漏洞、后门检测等等，并加以安全专家手工检测工具辅助，出具完善的检测报告与对应修复意见。

2. 资产漏洞服务

对各类硬件设备、各类协议、主机系统等资产进行漏洞扫描，高位严重漏洞资产由安全专家辅助手工验证，出具检测报告及其对应修复意见。

3. 基线核查服务

提供对客户信息系统资产的基线安全核验，并出具相关整改意见。

4. 安全意识培训服务

提供对各类企业人员安全意识培训服务，预防近源于 APT 攻击，提高企业整体安全意识。

5. 应急响应服务

根据客户应急安全管理体系，针对各种网络安全突发事件进行安全响应与技术支持。

6. 安全加固服务

从基线检查安全要求，对客户主机进行调整策略，安装补丁，安全软件等进行加固，并修补存在的安全问题。