安恒等级保护工具箱
作业指导书

变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本 A/0	葛方隽/2021.3	吕萍/2021.3	

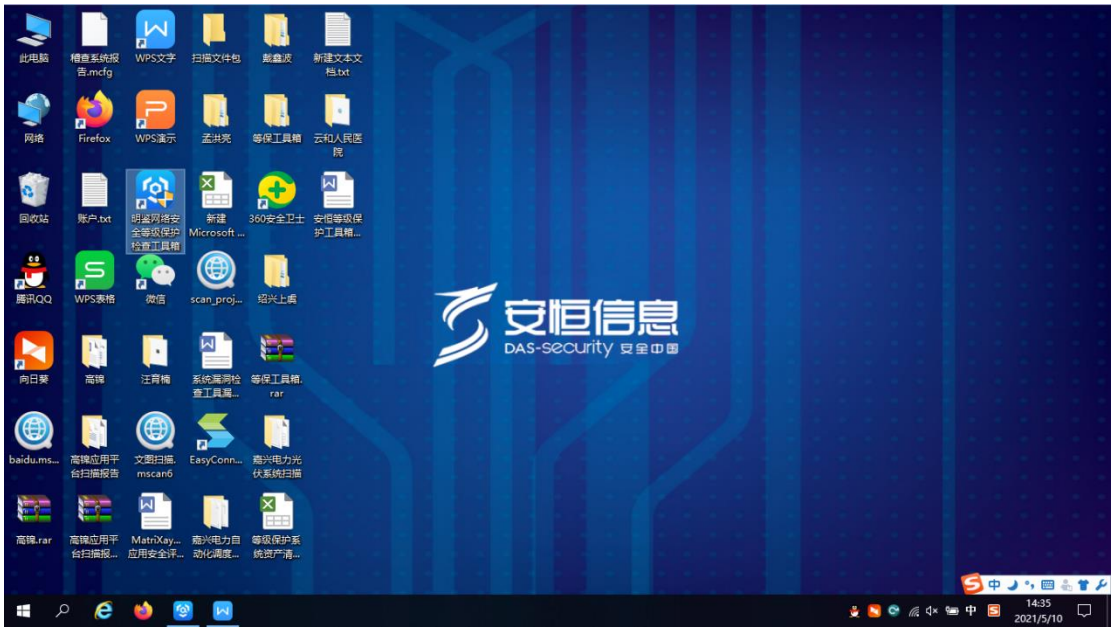
1 工具主要功能

安恒明鉴网络安全等级保护检查工具箱(监管版)《以下简称等保工具箱或工具箱)是公安机关网安部门开展网络安全检查其作的体化专用便携式监察装备,具有规范检查、工具调用、结果展示等功能集成定制有专门的安全检查工具,为公安机关网络安全执法检查提供专业检查知识和检查方法并实现对获取数据的关联分析、统计比对、处理流转等功能,提高网络安全执法检查的常态化标准化和规范化水平。

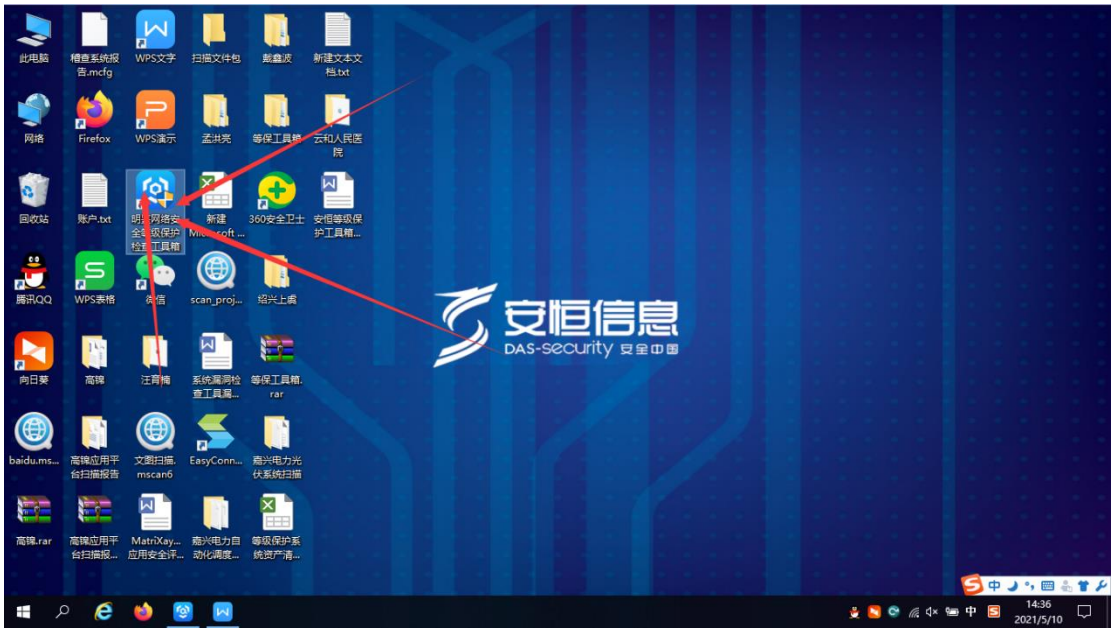
安恒明鉴网络安全等级保护检查工具箱主要功能：应用系统漏洞扫描、主机系统漏洞扫描、数据库漏洞扫描、主流网络/安全设备的配置核查,检查内容支持自定义筛选导出（支持导出格式为 word、PDF、XML）。

2 工具开机及调试步骤

开机登录明鉴网络等级保护工具箱（密码在账户.txt）

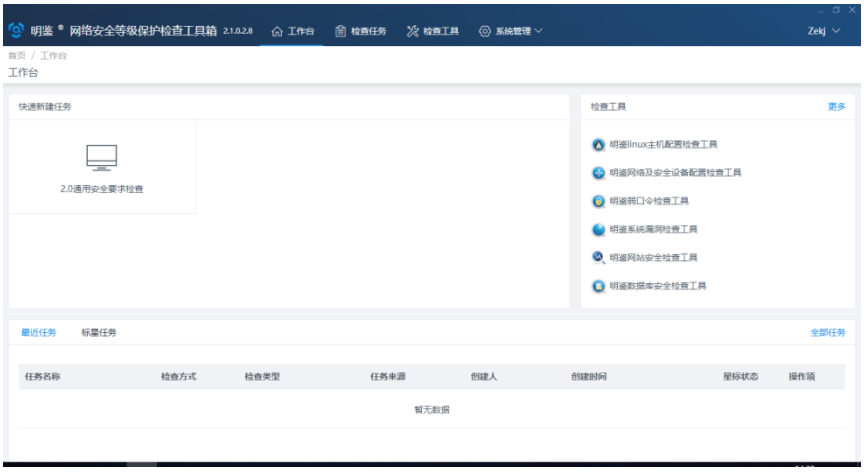


在工具箱的左侧/右侧 USB 接口插入电子狗，同时点击打开桌面明鉴信息安全等级保护检查工具箱



在登录界面输入登录账户和密码，登录工具箱系统

成功登录工具箱系统，工具箱界面如下



3 扫描任务执行步骤

工具分在线监测工具和离线监测工具，根据实际需求选择对应工具。在线工具需要联通网络，具体操作如下所示：

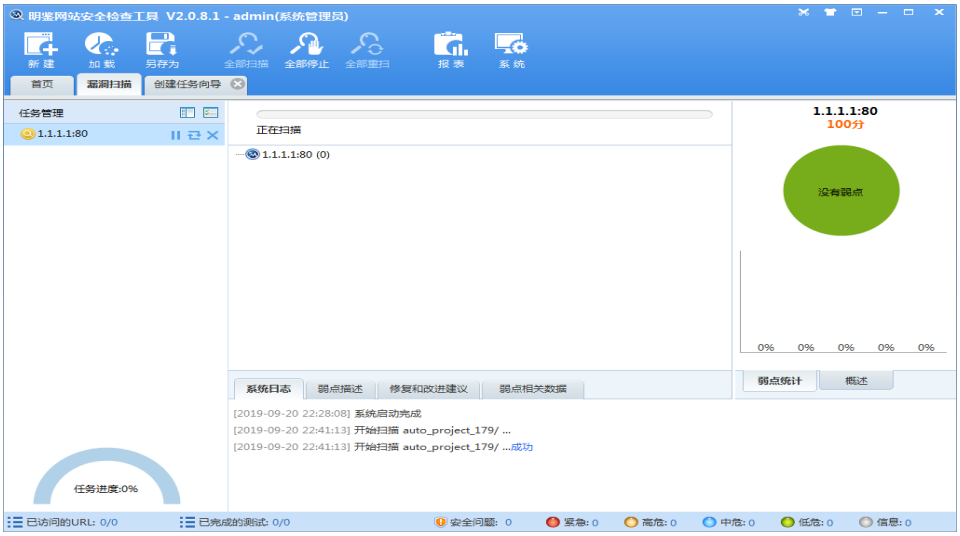
3.1 明鉴网站安全检查工具

点击运行网站安全检查工具

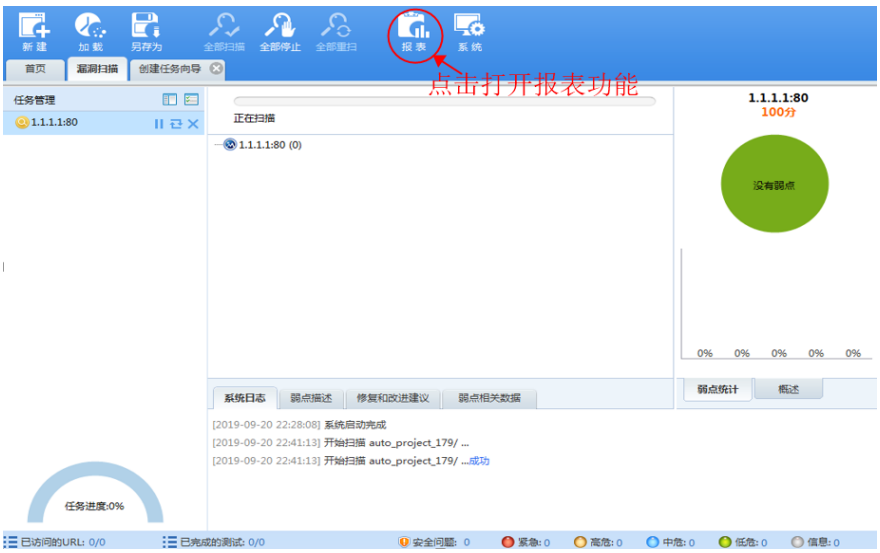
打开网站检查运行界面如下

输入扫描对象的 IP 地址或域名

执行网站扫描任务（扫描过程中）



待扫描任务完成后，点击报表，如图：



待扫描任务完成后，浏览及导出扫描结果，如图：

3.2 明鉴系统漏洞检查检查工具

支持常用 Windows. Unix. Linux 等系统操作系统 ,支持多种扫描策略，包括常规完全扫描、可强度扫描、低强度扫描等,支持对网络设备进行漏洞扫描.

具体操作如下：

点击运行系统漏洞检查工具

工具界面如下所示：

单击完成开始扫描

扫描完成

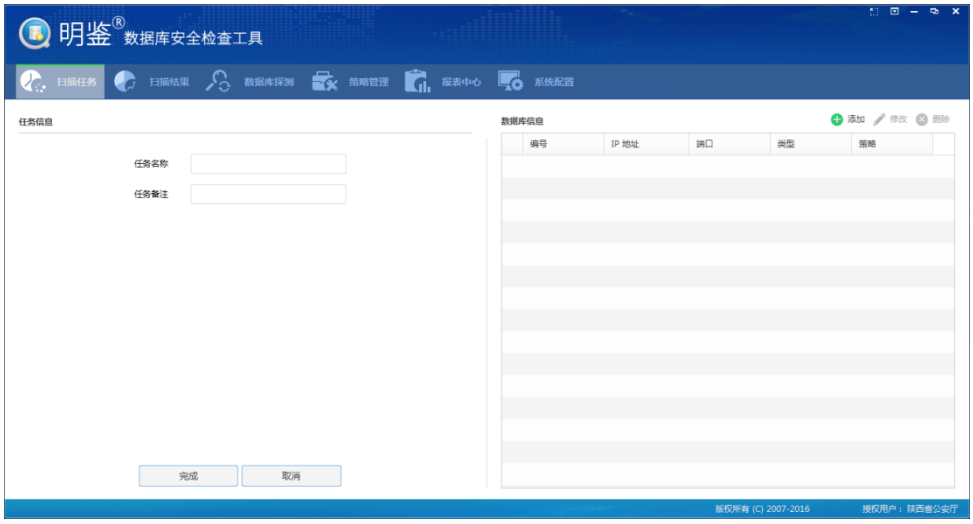
点击报表管理

选中对应报表，点击导出报表（一般导出一份 word 一份 pdf）

3.3 明鉴数据库安全检查工具

支持远程方式扫描数据库的配置信息、安全策略、参数账号口令安全、远程服务、端口和漏洞等信息，支持系统 SqlServer. Oracle. MySql. Sybase 等 主流数据库.具体操作如下：

（1）单击“明鉴数据库安全检查工具” 运行，出现如下界面点击向导并根据实际情况添加需要扫描的 IP 地址



(4)扫描开始等待完成。

(2) 在报表中心选中扫描完成的报表并导出报表（word 格式）

3.4 明鉴网络及安全设备配置检查工具

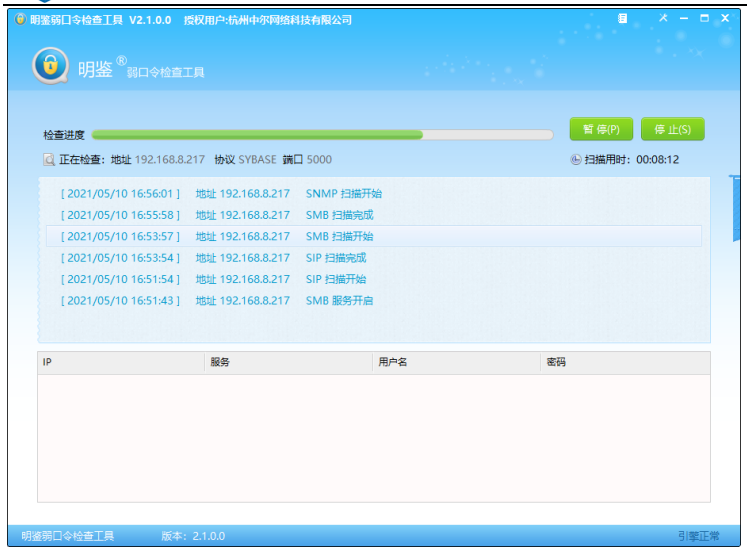
单击运行网络及安全设备配置检查工具

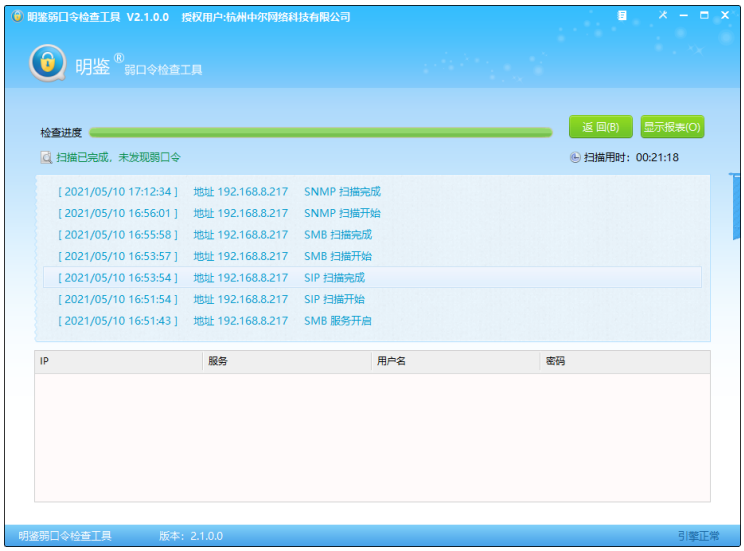
根据客户提供的设备厂商、设备用户名密码、登录协议、端口等，输入进工具点击开始检查

3.5 明鉴弱口令检查工具

单击运行弱口令检查工具

输入检查地址，单击开始扫描





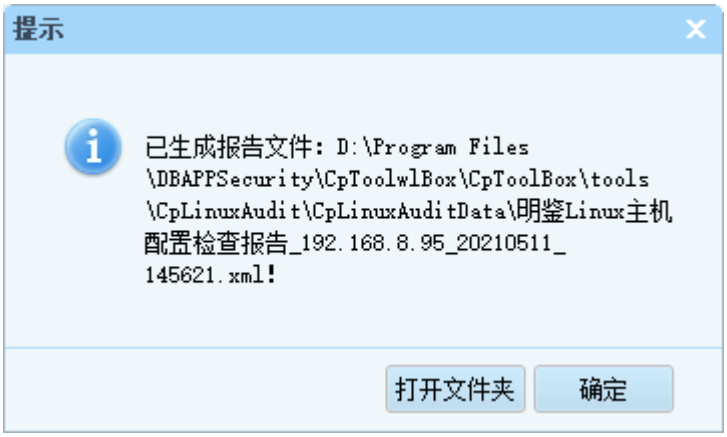
点击显示报表

3.6 明鉴 linux 主机配置检查工具

单击运行 linux 主机配置检查工具

输入对应的 linux 主机 IP、用户名、密码，点击开始检查，等待检查完成

检查完成后可以点击打开文件夹找到报告位置



或者点击显示报表来查看检查报表