匡恩网络
守 护 未 来

根源分析
界面重构2.2版本

目录：

图例说明

	动态展示的效果
list item	背景色块，根据鼠标事件，显示不同的样式
button	功能按钮，可以是图标按钮、实体按钮、文字按钮，以该图例统一说明
①	提示信息、帮助信息图标，鼠标移至上方将显示弹窗
text	输入框，如有特殊效果，具体参照界面设计图
monitor	监视器功能使用现有的图形界面，不做改动

前置步骤 导入漏洞

外部框架

根源分析-任务名

关联漏洞

- [x] 漏洞1
- [x] 漏洞2

新建【根源分析】任务，选择需要导入的漏洞

导入漏洞

【导入】后默认显示第一个漏洞
并且【关联】对应的测试用例

此处预留位，
运行【用例检测】后将显示结果

根源分析-任务名

检测列表 漏洞1 VNC协议弱口令检测 FTP协议弱口令检测 配置设备 根源分析 分析结果

配置测试机

配置被测试设备/系统

自动读取漏挖的设备配置信息
否则，手动配置

进入根源分析

进入当前用例的根源分析界面

开始用例检测
点击后切换成【暂停】

停止所有分析

根源分析-任务名

检测列表　漏洞1　VNC协议弱口令检测　　配置设备　根源分析　分析结果

详情	测试用例	被测设备IP	端口
ⓘ	VNC协议弱口令检测	192.168.22.23	5900

用例检测

自动检测　开始　停止

状态 停止检测　已运行时间 00:00

ⓘ 用例检测结果

范围值	种子值	全选
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

抓包检测 ▶▶　删除

monitor

用例【检测方式】分为
【自动检测】（默认）
和 【手动检测】
通过【下拉】选择。

对检测结果进行抓包检测，如果未运行用例检测，将无法点击进入

根源分析-任务名

检测列表　漏洞1　VNC协议弱口令检测　　配置设备　根源分析　分析结果

详情	测试用例	被测设备IP	端口
ⓘ	VNC协议弱口令检测	192.168.22.23	5900

手动检测方式下，
必须输入【范围值】
【种子值】

用例检测

手动检测　范围值　2500　5000　种子值　10　开始　停止

状态 正在检测　已运行时间 12:00

范围值100-2500 种子值1　未发现

检测完成

状态列表
显示运行结果，如果发现失败点则在【检测结果】列表显示
用户最多只能得到【10个】结果，防止无限检测。

ⓘ 用例检测结果

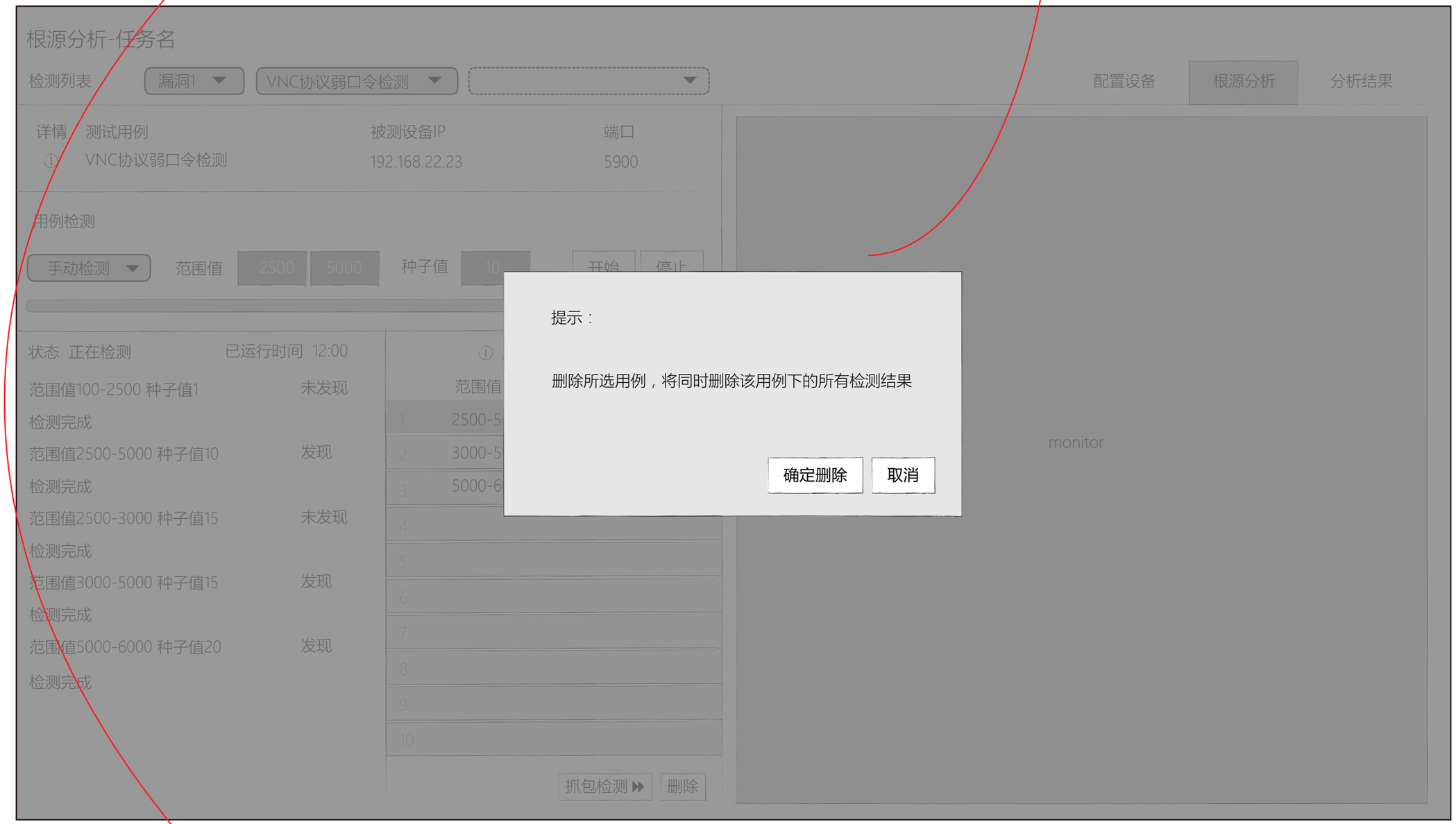
	范围值	种子值	全选
1	2500-5000	10	■
2	3000-5000	20	☑
3	5000-6000	15	☑
4			
5			
6			
7			
8			
9			
10			

抓包检测 ▶▶　删除

点击【抓包检测】将所选的用例【添加】
至列表并默认分析第一条用例

删除【所选用例】将清除该条【检测结果】，同时删除该用例下的【抓包检测结果】
此步骤无法还原，将给予【对话框】确认。

monitor


根源分析-任务名
检测列表
漏洞1
VNC协议弱口令检测
配置设备
根源分析
分析结果
详情
测试用例
被测设备IP
端口
VNC协议弱口令检测
192.168.22.23
5900
用例检测
手动检测
范围值
2500
5000
种子值
10
开始
停止
状态 正在检测
已运行时间 12:00
范围值100-2500 种子值1 未发现
检测完成
范围值2500-5000 种子值10 发现
检测完成
范围值2500-3000 种子值15 未发现
检测完成
范围值3000-5000 种子值15 发现
检测完成
范围值5000-6000 种子值20 发现
检测完成
范围值
1 2500-5
2 3000-5
3 5000-6
4
5
6
7
8
9
10
抓包检测
删除
monitor
提示：
删除所选用例，将同时删除该用例下的所有检测结果
确定删除
取消

根源分析-任务名

检测列表　漏洞1　VNC协议弱口令检测　范围值3000-5000 种子值20　范围值5000-6000 种子值15　配置设备　根源分析　分析结果

包编号	原IP	目的IP	协议	包长	
1	192.168.0.111	192.168.0.222	TCP	74	编辑
2	192.168.0.114	192.168.0.223	UDP	132	编辑
3	192.168.0.25	192.168.0.224	Modbus	90	编辑
4	192.168.0.111	192.168.0.222	TCP	74	编辑
5	192.168.0.114	192.168.0.223	UDP	132	编辑
6	192.168.0.25	192.168.0.224	Modbus	90	编辑
7	192.168.0.114	192.168.0.223	UDP	132	编辑
8	192.168.0.25	192.168.0.224	Modbus	90	编辑

按照包顺序显示包列表并给予【编号】

抓包检测　开始　停止

状态 停止检测　已运行时间 12:00

ⓘ抓包检测结果

包编号　全选

用例检测　保存结果

返回上一步

根源分析-任务名

检测列表　漏洞1　VNC协议弱口令检测　范围值3000-5000 种子值20

配置设备　根源分析　分析结果

弹出\收起编辑面板

	包编号	原IP	目的IP	协议	包长	
*	1	192.168.0.111	192.168.0.222	TCP	74	编辑
	2	192.168.0.114	192.168.0.223	UDP	132	编辑
	3	192.168.0.25	192.168.0.224	Modbus	90	编辑
	4	192.168.0.111	192.168.0.222	TCP	74	编辑
	5	192.168.0.114	192.168.0.223	UDP	132	编辑
	6	192.168.0.25	192.168.0.224	Modbus	90	编辑
	7	192.168.0.114	192.168.0.223	UDP	132	编辑
	8	192.168.0.25	192.168.0.224	Modbus	90	编辑

如果编辑后未保存，给予星号标记

焦点包和编辑包，有明显的背景区分

抓包检测　开始　停止

状态 正在检测　已运行时间 12:00

包编号
1 发现
2 发现
3 未发现
4 发现
5 未发现
6 发现
7 未发现
8 未发现

检测完成

①抓包检测结果

包编号	全选
1	■
2	☑
4	☑
6	■

用例检测　保存结果

收起面板　保存　还原

恢复包初始值

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
0001	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
0002	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
0003	■	■	■	■	■	■	■	■	■	■	■	■				

如果包修改后未保存，
弹窗提示需保存才能运行
保存后，消除标记

返回上一步

将所选的包保存至结果，当前版本包数据只保存在数据库里，
包括修改选项，该项操作不会在前端做展示

根源分析-任务名

检测列表 漏洞1 VNC协议弱口令检测 范围值3000-5000 种子值20 配置设备 根源分析 分析结果

结果列表

显示所有关联漏洞的用例列表

已完成分析
(完成整个流程)

漏洞1

VNC协议弱口令检测

1 VNC协议弱口令检测范围值3000-5000种子值20 下载pcap包 生成测试用例

2 VNC协议弱口令检测范围值5000-6000种子值15 继续分析

FTP协议弱口令检测

1 FTP协议弱口令检测范围值(未设置)种子值(未设置) 开始分析

跳转至对应的
【抓包分析】功能

未完成分析
(只完成了【用例检测】，未完成【抓包检测】)

漏洞2

IEC104协议模糊分析

1 IEC104协议模糊分析范围值(未设置)种子值(未设置) 开始分析

从设备检测开始
新的检测流程

ARP协议完整性测试

1 ARP协议完整性测试范围值(未设置)种子值(未设置) 开始分析

点击弹出windows保存对话框

未分析
(未进行任何分析)

弹出生成测试用例面板

在用例库中需要增加一个自定义的用例类型，展现的就是上面修改后的自定义用例，端口和变化值就是上述的端口和变化（范围值）
在选择用例时候也需要加一类：自定义用例测试。
把所有用户自定义生成的用例、根源分析生成的用例放进来，其中变化值等参数不可修改。

运行、暂停、停止按钮规则

1、【运行】键和【暂停】键互相切换，【运行（暂停）】时无法进行除【检测列表切换】及【导航切换】外的其他操作，必须等用例检测完成或者按下【停止】键后才可进行其他操作。

2、运行前需要判断【抓包检测】的包内容是否保存，如果未保存将提醒用户保存。

检测列表切换规则

1、【漏洞切换】漏洞之间的切换将进入设备配置界面，并配置设备。
2、【用例切换】用例之间的切换将进入设备配置界面，并配置设备。
3、【用例范围切换】用例范围的切换无需进入配置界面，直接进入当前用例的抓包检测界面。
4、任何切换操作，都将终止运行中的检测，目前无法做多进行检测，需要给予用户警示对话框。

导航切换规则

1、导航切换后，进入当前【检测列表】选项，所对应的功能界面。