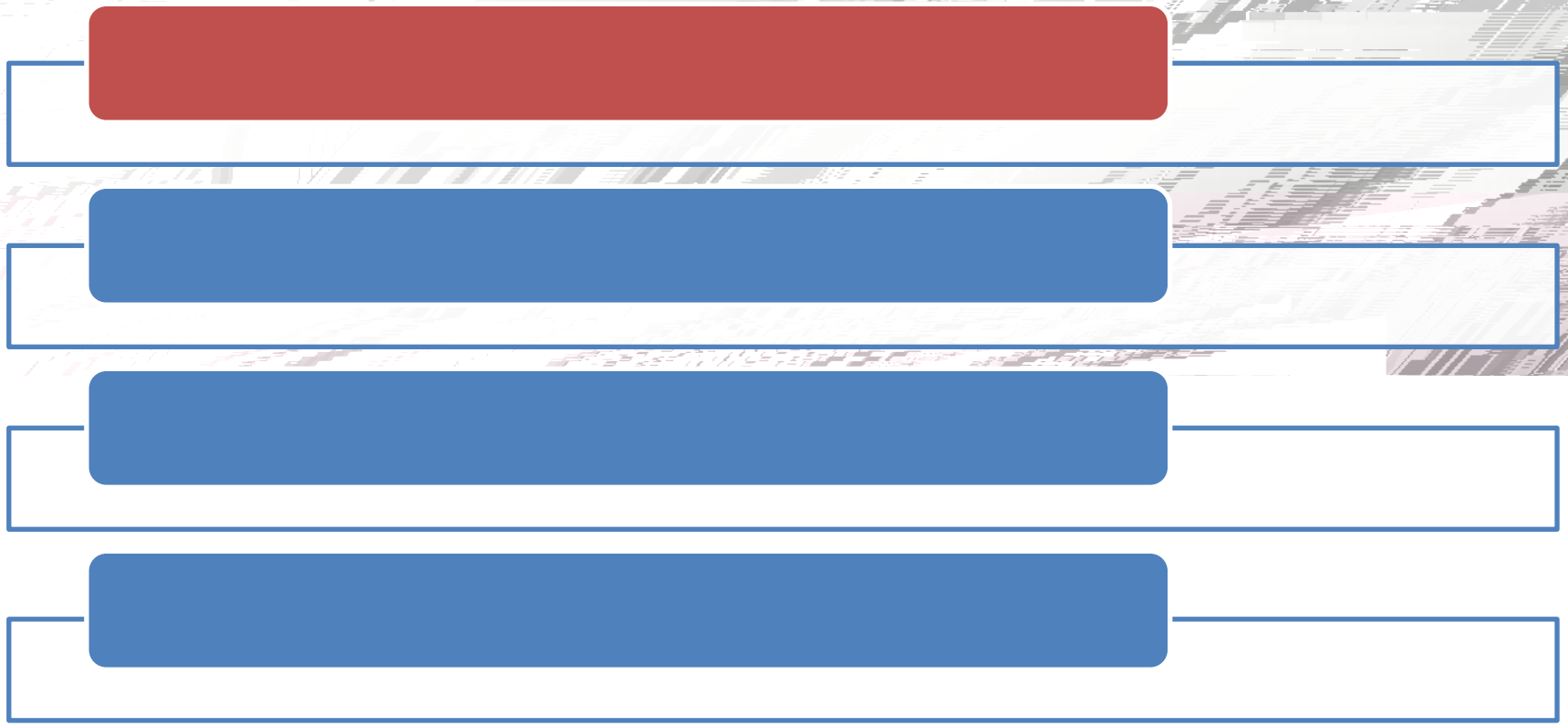
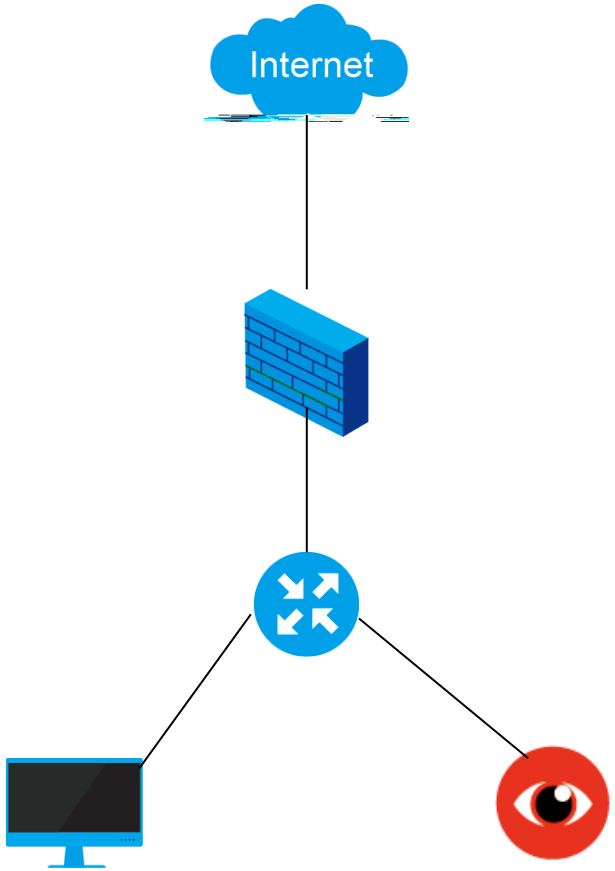
RG-

RG-Scan

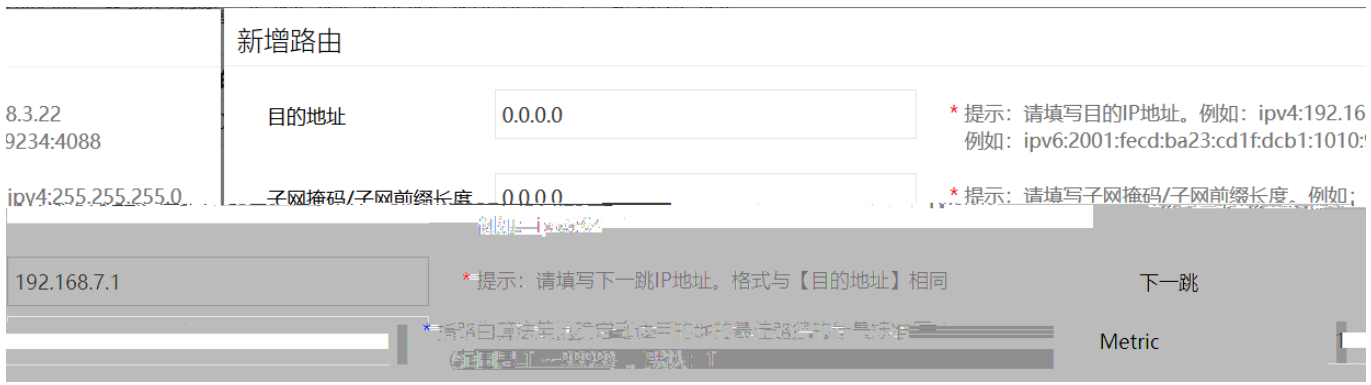
Contents




Internet

account/account
admin/admin


VLAN接口配置
基本配置
接口IP地址配置
新增
支持IPv4以及IPv6网络地址
192.168.7.160
255.255.255.0
192.168.1.200
255.255.255.0
完成

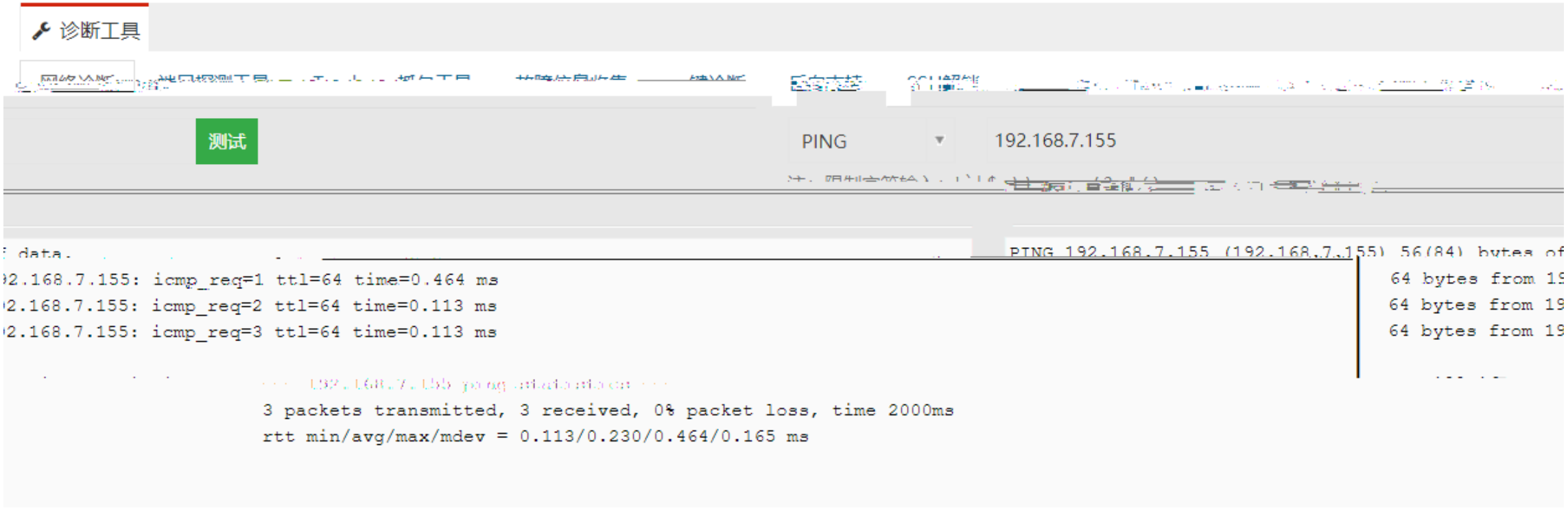

新增路由
目的地址
0.0.0.0
提示：请填写目的IP地址。例如：ipv4:192.16
例如：ipv6:2001:fecd:ba23:cd1f:dcb1:1010:
提示：请填写子网掩码/子网前缀长度。例如：
192.168.7.1
提示：请填写下一跳IP地址。格式与【目的地址】相同
下一跳
Metric

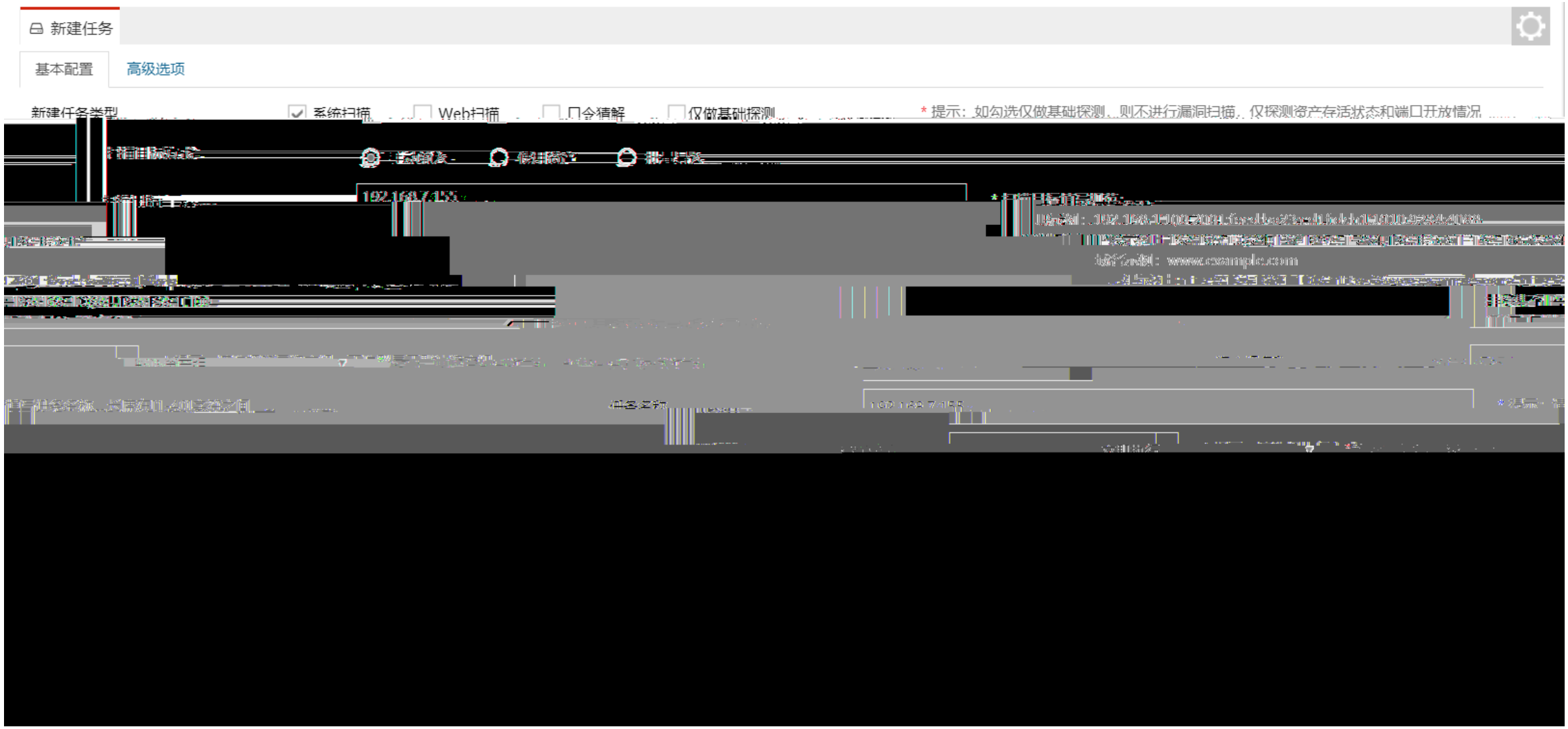
Contents

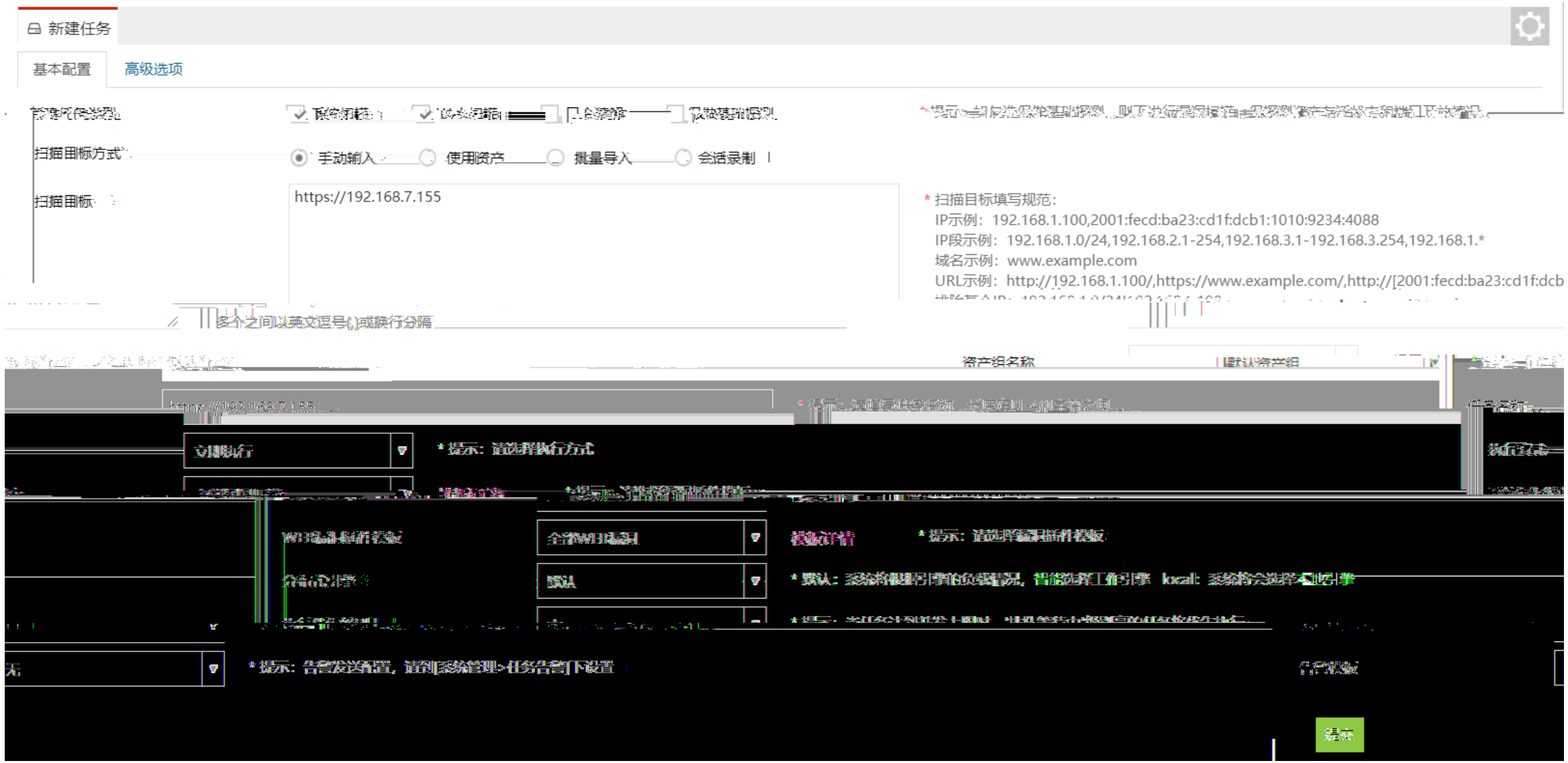
1

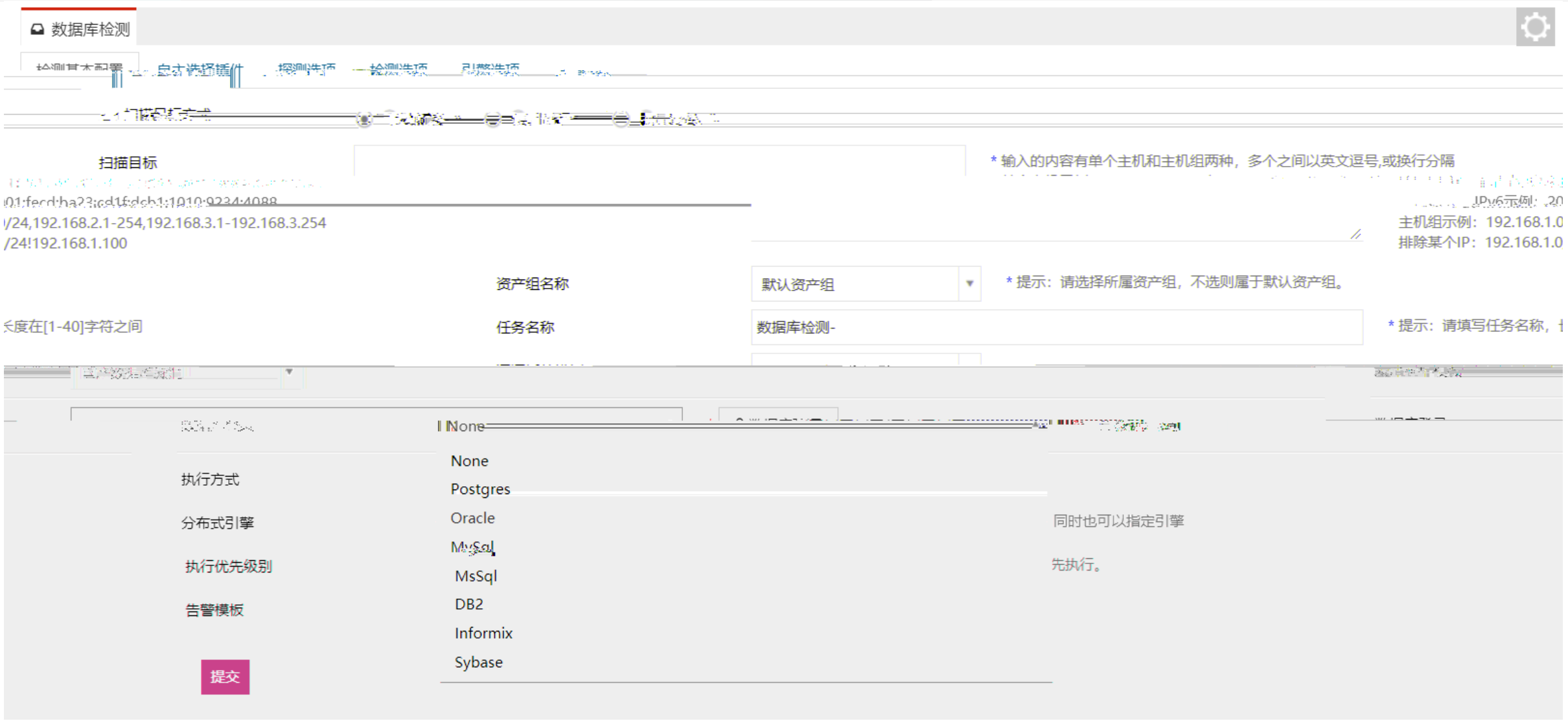
2

3


诊断工具
测试
PING
192.168.7.155
data.
PING 192.168.7.155 (192.168.7.155) 56(84) bytes of
2.168.7.155: icmp_req=1 ttl=64 time=0.464 ms
2.168.7.155: icmp_req=2 ttl=64 time=0.113 ms
2.168.7.155: icmp_req=3 ttl=64 time=0.113 ms
64 bytes from 19
64 bytes from 19
64 bytes from 19
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.113/0.230/0.464/0.165 ms


新建任务
基本配置
高级选项
新建任务类型
系统扫描
Web扫描
口令猜解
仅做基础探测
* 提示：如勾选仅做基础探测，则不进行漏洞扫描，仅探测资产存活状态和端口开放情况
192.168.7.155
www.example.com

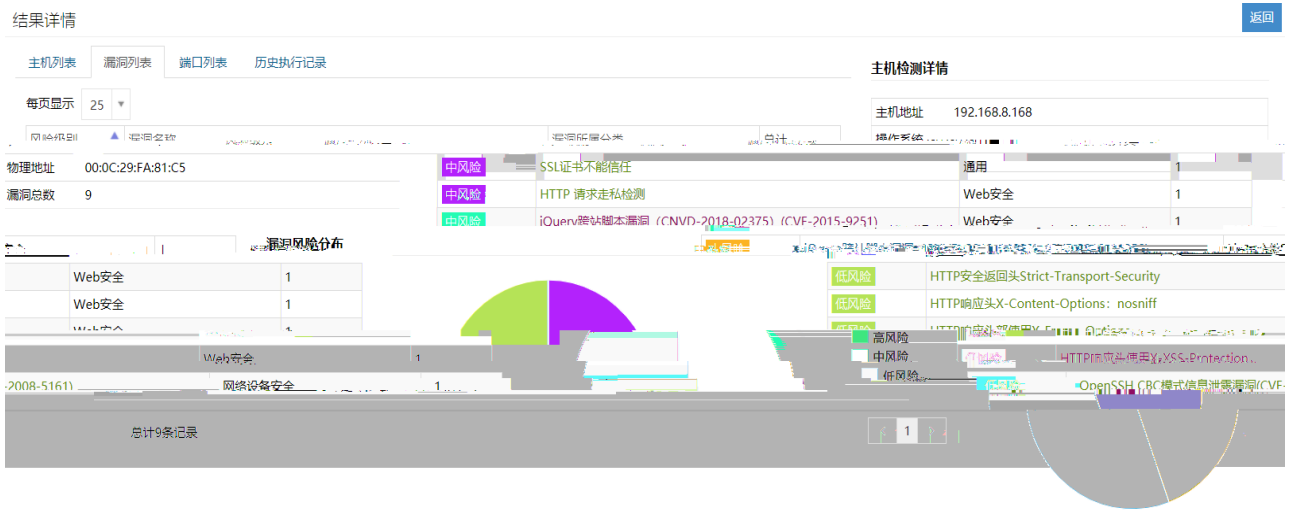

新建任务
基本配置
高级选项
扫描目标方式
手动输入
使用资产
批量导入
会话录制
扫描目标
https://192.168.7.155
* 扫描目标填写规范：
IP示例：192.168.1.100,2001:fecd:ba23:cd1f:dcb1:1010:9234:4088
IP段示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254,192.168.1.*
域名示例：www.example.com
URL示例：http://192.168.1.100/,https://www.example.com/,http://[2001:fecd:ba23:cd1f:dcb
多个之间以英文逗号(,)或换行分隔
资产组名称
默认资产组
* 提示：请选择执行方式
* 提示：请选择WEB插件模板
模板详情
* 默认：系统根据引擎的负载情况，智能选择工作引擎 local：系统将会选择本地引擎
* 提示：告警发送配置，请到[系统管理>任务告警]下设置


数据库检测
扫描目标
* 输入的内容有单个主机和主机组两种，多个之间以英文逗号,或换行分隔
/24,192.168.2.1-254,192.168.3.1-192.168.3.254
/24!192.168.1.100
主机组示例：192.168.1.0
排除某个IP：192.168.1.0
资产组名称
默认资产组
* 提示：请选择所属资产组，不选则属于默认资产组。
任务名称
数据库检测-
* 提示：请填写任务名称，
None
None
Postgres
Oracle
MySql
MsSql
DB2
Informix
Sybase
执行方式
分布式引擎
同时也可以指定引擎
执行优先级别
先执行。
告警模板
提交

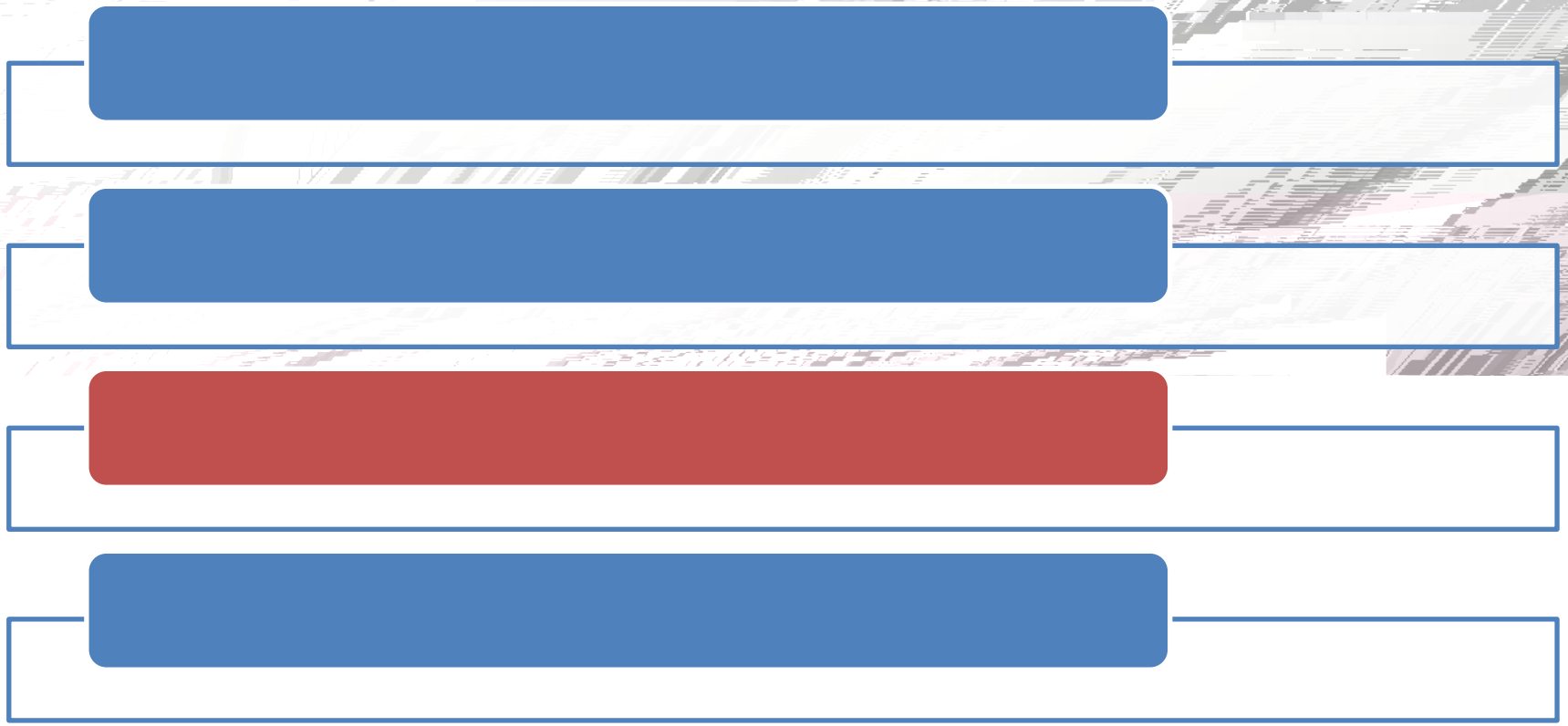

新建任务
基本配置
高级选项
扫描目标
192.168.7.155
* 扫描目标填写规范：
IP示例：192.168.1.100,2001:fecd:ba23:cd1f:dcb1:1010:9234:4088
排除某个IP：192.168.1.0/24!192.168.1.100
资产组名称
默认资产组
请选择执行方式
执行类型
立即执行
口令猜解高级
口令猜解服务
SSH, Oracle
* 提示：当任务达到并发上限时，'排队等待中'级别高的任务将优先执行
执行优先级别
提交


每页显示
25
任务名称
执行方式
扫描类型
优先级
任务进度
操作


结果详情
返回


结果详情
返回
主机列表
漏洞列表
端口列表
历史执行记录
每页显示
25
主机检测详情
主机地址
192.168.8.168
物理地址
00:0C:29:FA:81:C5
漏洞总数
9
中风险
SSL证书不能信任
通用
中风险
HTTP 请求走私检测
Web安全
漏洞风险分布
低风险
HTTP安全返回头Strict-Transport-Security
低风险
HTTP响应头X-Content-Options：nosniff
高风险
中风险
低风险
总计9条记录

Contents



>

/WEB /


资产漏洞查询
资产组
标签
请选择标签
导出EXCEL
192.168.8.193
NetBIOS多个IP地址枚举
1
Windows安全
低风险
OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)
1
网络设备安全
22/ssh
7.2
192.168.8.168
低风险
HTTP安全返回头Strict-Transport-Security
1
Web安全
443/www
5.0
192.168.8.168
1
Web安全
443/www
4.0
192.168.8.168
中风险
中风险
1
通用
低风险
HTTP响应头使用X-XSS-Protection
1
Web安全
443/www
http://192.168.7.97:5357/
1
A6 敏感信息泄漏

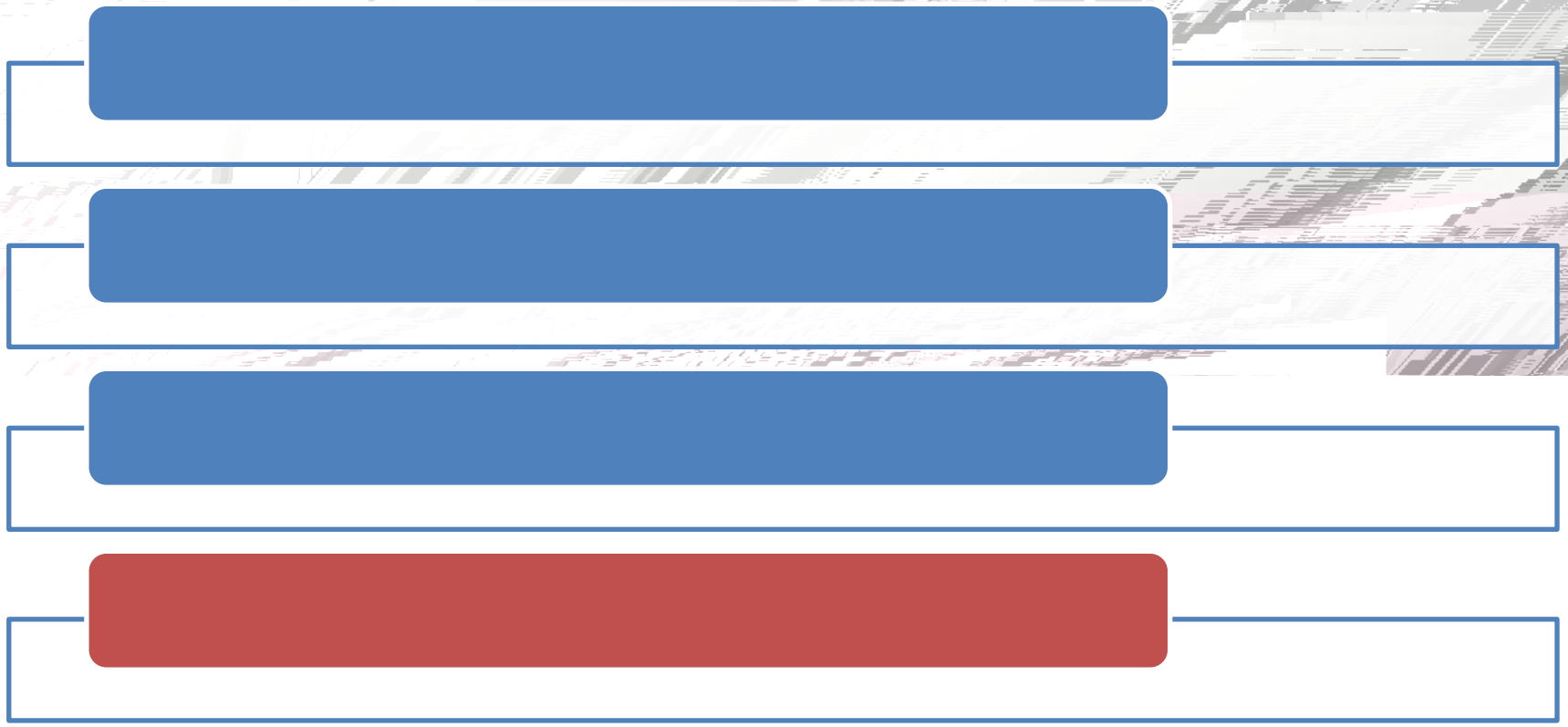
>


系统漏洞
WEB漏洞
资产组:
系统扫描-非登录扫描资产
漏洞变化
2019-06-12 21:07:02 至 2019-06-12 21:54:11
对比
没有检索到数据
总计0条记录
减少漏洞
高风险
BIND DNSSEC Key处理错误拒绝服务漏洞(...
服务:dns 端口:53 协议:udp
2019-06-05 22:45:23
2019-06-05 23:26:02
服务:ssh 端口:22 协议:tcp
服务:dns 端口:53 协议:udp
服务:mysql 端口:3306 协议:tcp
OpenSSH sshd拒绝服务漏洞(CVE-20
ISC BIND 9 DNS递归解析器拒绝服务
ISC BIND 9 DS响应断言失败拒绝服务
Oracle MySQL Server拒绝服务漏洞

>

HTML WORD PDF EXCEL XML

Contents



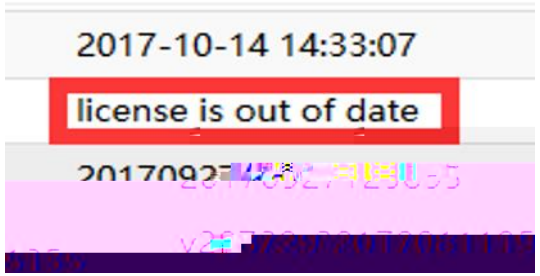
> /

1

2

FTP

3



license is out of date

1

admin account

account/account

> >


任务列表
工作列表
新增
刷新
全部任务
搜索[回车/TAB]
每页显示
25
执行方式
开始时间
结束时间
检测耗时
进度
操作
任务名称
手动执行
2018-01-17 10:58:21
2018-01-17 10:58:41
20秒
发现漏洞数：0 发现主机数：0
立即执行
禁用
系统扫描-

1

2

3

1 IP

2

a. “ ”

b. “ ICMP PING”

c. “ ” 50

d. “ ”

3 DNS DNS 127.0.0.1