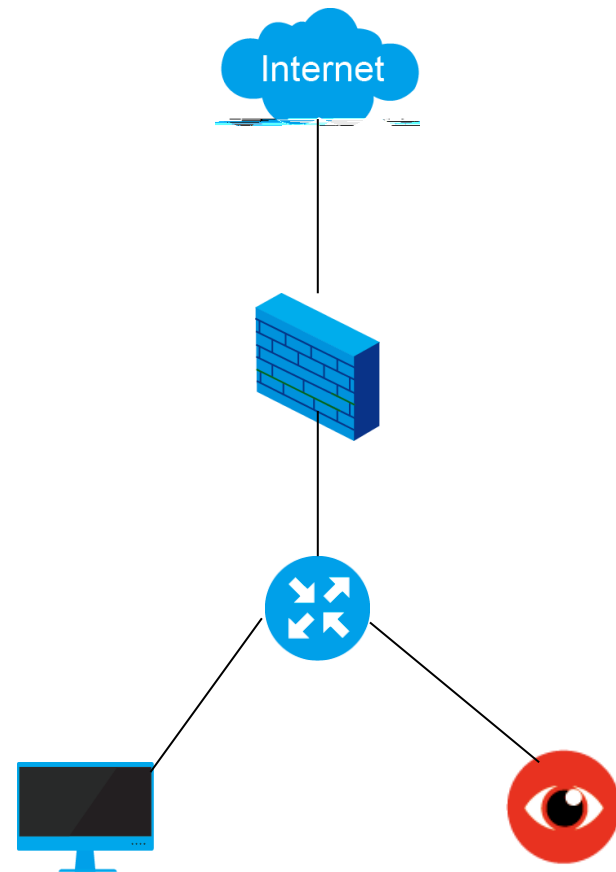


RG-Scalable Management / P / Span

## RG-Scan

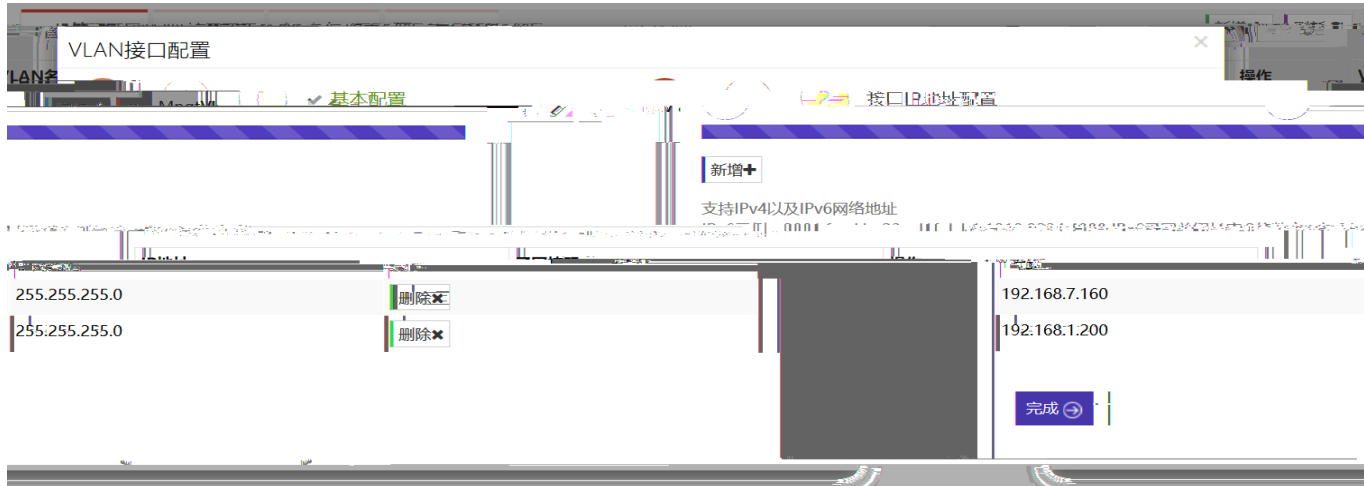


# Contents



account/account  
admin/admin



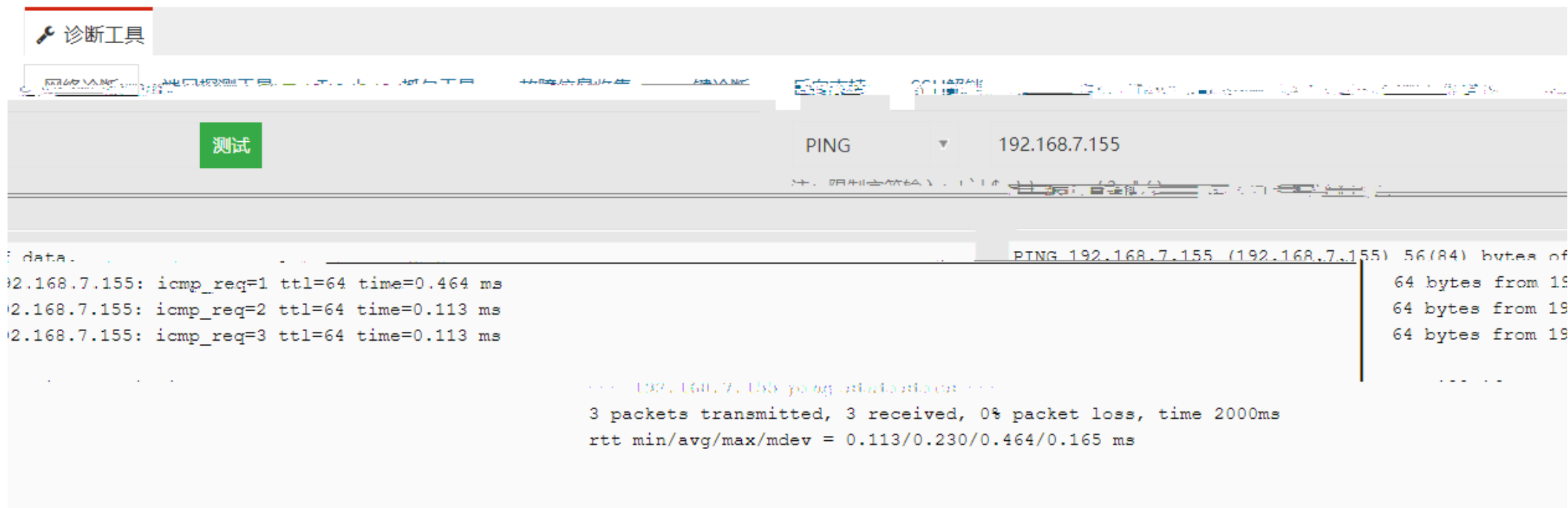
新增路由	
8.3.22 9234:4088	<p>目的地址 <input type="text" value="0.0.0.0"/> * 提示: 请填写目的IP地址。例如: ipv4:192.16.1.1 例如: ipv6:2001:fece:ba23:cd1f:dcb1:1010:1</p> <p>子网掩码/子网前缀长度 <input type="text" value="0.0.0.0"/> * 提示: 请填写子网掩码/子网前缀长度。例如: 255.255.255.0 例如: ipv6:64</p> <p>下一跳 <input type="text" value="192.168.7.1"/> * 提示: 请填写下一跳IP地址。格式与【目的地址】相同</p> <p>Metric <input type="text" value="1"/></p>



# Contents



1  
2  
3



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







检测基本配置 目标选择插件 探测选项 检测选项 引擎选项

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

IPv6示例: 2001:fe0d:ha23:cd1:fdcb1:1010:0234:4088

主机组示例: 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254

排除某个IP: 192.168.1.0/24!192.168.1.100

\* 提示: 请选择所属资产组, 不选则属于默认资产组。

资产组名称

默认资产组

\* 提示: 请填写任务名称, 长度在[1-40]字符之间

任务名称

数据库检测-

同时也可以指定引擎

先执行。

MySQL

None

执行方式

None

Postgres

分布式引擎

Oracle

执行优先级

MySQL

MsSql

告警模板

DB2

Informix

Sybase

提交

新建任务
⚙️

基本配置
高级选项

扫描目标:

示例: http://192.168.1.100/, https://www.example.com/, http://[2001:fece:ba23:cd1:fdcb1:1010:9234:4088]

单个IP: 192.168.1.0/24|192.168.1.100

默认资产组:

资产组名称:

任务名称:

执行方式:

命令猜解高级:  命令猜解服务:  SSH, Oracle:

公有云引擎:

执行优先级:

任务描述:

\* 扫描目标填写规范:  
IP示例: 192.168.1.100,2001:fece:ba23:cd1:fdcb1:1010:9234:4088  
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

\* 提示: 请选择所属资产组, 不选则属于默认资产组

\* 提示: 请选择执行方式

\* 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

\* 提示: 任务发送配置, 请到系统管理-任务管理-配置

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
192.168.8.168	手动执行	存活探测	中	100%	立即执行
192.168.8.168	手动执行	系统扫描	中	100%	立即执行

结果详情



结果详情

主机列表 漏洞列表 端口列表 历史执行记录

主机地址: 192.168.8.168

漏洞名称	风险等级	所属类别	数量
通用	中风险	物理地址	1
Web安全	中风险	漏洞总数	9
18-02375) (CVF-2015-9251)	中风险	Web安全	1
低风险	低风险	HTTP安全	1
低风险	低风险	HTTP安全	1
高风险	中风险	HTTP安全	1
中风险	低风险	Web安全	1
低风险	低风险	网络设备安全	1

漏洞风险分布

总计9条记录

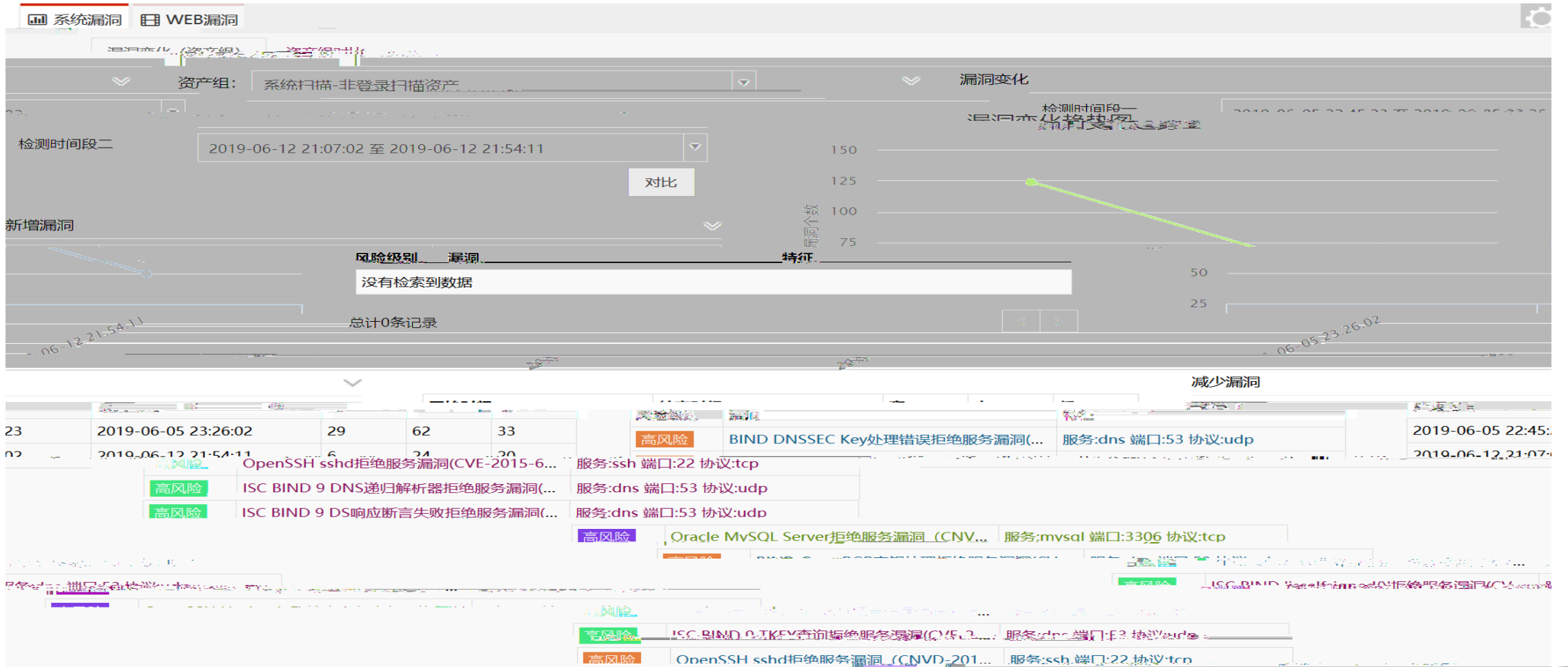
# Contents


>

/WEB /

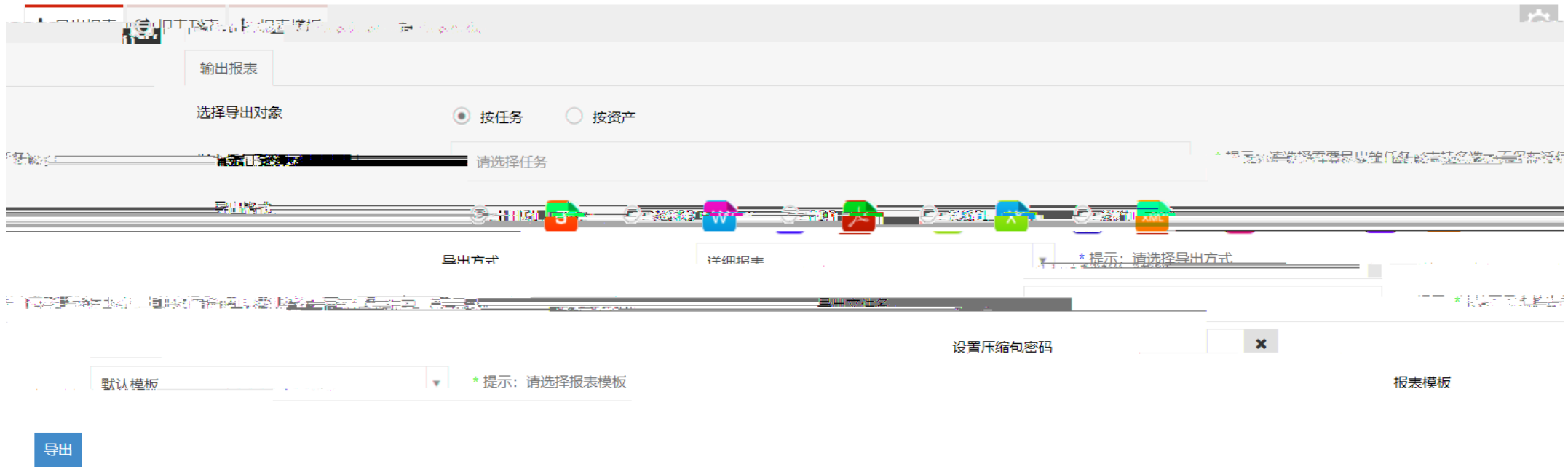
漏洞名称	漏洞等级	漏洞编号	漏洞来源	端口/服务	漏洞评分	资产
OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	低	22/ssh	7.2	192.168.8.168	低	192.168.8.168
HTTP安全返回头Strict-Transport-Security	低	1	1	443/www	5.0	192.168.8.168
HTTP响应头X-Content-Options: nsniff	中	1	1	443/www	4.0	192.168.8.168
HTTP请求走私检测	低	1	1	443/www	4.0	192.168.8.168
HTTP响应头未设置X-Frame-Options	低	1	1	443/www	4.0	192.168.8.168
SSL证书不信任	中	1	1	443/www	6.4	192.168.8.168
服务器断大信息泄露	低	1	1	http://192.168.7.97:5357/	1	http://192.168.7.97:5357/

>



>

HTML WORD PDF EXCEL XML



# Contents


> /

1

2

3

FTP

版本/特征库升级

特征库自动升级    版本/特征库手动升级    版本/特征库本地升级

系统服务器地址:  \* 例如: http://update.example.com:8080/

执行周期: 每天执行一次    02:47

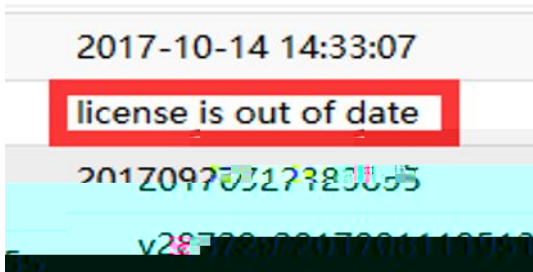
通过设置时代理地址上网获取服务器地址的升级包

代理服务器用户名:

代理服务器密码:

保存    立即升级

特征库升级任务	系统升级时间	系统升级结果	当前系统版本
635	20201106091	升级成功	当前系统版本
		V1.0(4.0.1-R2-v68710-20201010)	



license is out of date

1

admin

account

account/account

>

>

账号管理   用户管理   用户权限模板								编辑	删除	解除锁定	重置	新增	刷新	搜索[回车/TAB]	⚙
<input type="checkbox"/>	admin	[默认用户]	高级管理员功能组	2018-01-17 11:58:58	启用	否	30								
<input type="checkbox"/>	audit	[默认用户]	审计管理员功能组	2018-01-16 13:52:45	启用	否	30								
<input type="checkbox"/>	ren	[默认用户]	报表管理员功能组	2018-01-16 13:46:52	启用	否	30								
<input checked="" type="checkbox"/>	test		普通管理员功能组	2018-01-17 09:42:13	启用	否	30								
<input type="checkbox"/>	scan		普通管理员功能组	2018-01-16 17:19:32	启用	否	30								
<input type="checkbox"/>	xixi		普通管理员功能组	2018-01-17 10:50:02	启用	否	30								
<input type="checkbox"/>	zzzz		普通管理员功能组		启用	否	30								
<input type="checkbox"/>	minii		普通管理员功能组	2018-01-17 11:44:33	禁用	否	30								
<input type="checkbox"/>	teet		普通管理员功能组		启用	否	30								

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

