

# UNIS X1000-12T12F-G2 紫光漏洞扫描系统

## 快速开始指南

---

Copyright © 2024 紫光恒越技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除紫光恒越技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 新建资产发现任务 .....	1
1.1 IP 发现 .....	1
1.2 子域名猜解 .....	3
2 新建系统扫描任务 .....	5
2.1 非登陆扫描 .....	5
2.2 登陆扫描 .....	6
3 新建应用扫描任务 .....	9
3.1 应用扫描 .....	9
4 新建数据库扫描任务 .....	11
4.1 非登陆数据库扫描 .....	11
4.2 登陆数据库扫描 .....	13
5 新建基线核查任务 .....	15
5.1 在线检查任务 .....	15
5.2 离线检查任务 .....	17
6 新建口令猜解任务 .....	21
6.1 在线爆破任务 .....	21
6.2 离线 Hash 爆破任务 .....	23
7 新建移动扫描任务 .....	25
7.1 扫描任务 .....	25
8 新建镜像扫描任务 .....	27
8.1 公开远程镜像扫描任务 .....	27
8.2 Haabor 仓库镜像扫描任务 .....	28

# 1 新建资产发现任务

本章节将基于具体场景，引导您快速创建资产发现任务。

## 1.1 IP 发现

### 1.1.1 场景说明

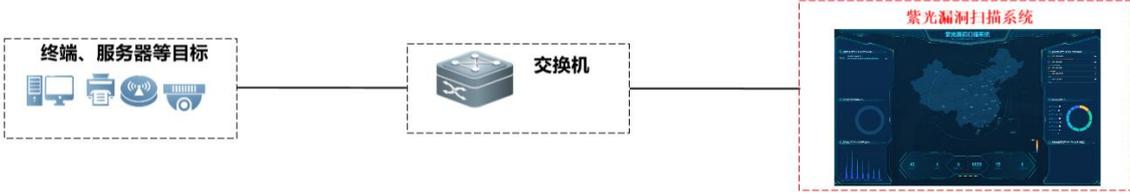
扫描探测发现网段中存活 IP、端口、服务信息。

在本场景中，待扫网段和扫描方式的信息参见下表。

表 1-1 场景说明—待扫主机信息

扫描网段主机	192.168.0.1-254
主机存活检测	只扫描存活主机
扫描服务类型	是
扫描速度	快速
端口扫描方式	TCP SYN

### 1.1.2 操作步骤

任务类型	资产发现—IP 发现
描述	发现目标网段中存活的主机，开放的端口号、服务和协议等信息
拓扑示意	
预置条件	扫描器与目标网段网络可达

1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；
2. 在“资产管理”->“资产发现”->新建任务，参数如下：

任务类型  IP发现  子域名发现

\* 任务名 测试 2 / 128

\* IP 192.168.0.1-254

支持输入格式:  
192.168.2.1,192.168.2.2  
192.168.2.1-255  
192.168.2.1-192.168.2.255  
192.168.2.0/24  
192.168.2.\*  
多个用英文逗号或换行分割

仅发现主机  是否启用

端口选择 常用端口(推荐) 模板配置

自定义端口列表  是否启用  启用后将扫描自定义的端口,不扫描端口模板中的端口

跳过主机发现   勾选后不检查主机是否在线,认为所有主机都是在线的

端口扫描模式 TCP SYN  SYN 为TCPSYN(半连接),Connect为TCP connect(全连接)

扫描服务类型   勾选后是识别目标端口所开启的服务是http还是mysql,开启后扫描速度会比较慢

扫描工控协议   勾选后会扫描如modbus、S7等工控专业协议

扫描速度  自适应  快速  超快速

操作步骤

3. 配置完成后点击“保存并执行”按钮，即可开始进行任务。
4. 查看结果：扫描完成后点击任务右侧的“结果”，查看扫描结果，扫描结果支持添加到资产库。

任务名 选择任务状态 保存 重置

任务名	任务类型	状态	进度	开始扫描时间	完成扫描时间	任务创建时间	操作
测试	IP发现	完成	100	2024-01-24 16:49:47	2024-01-24 16:58:40	2024-01-24 16:49:47	开始 编辑 结果 删除
uxsino.com	子域名发现	完成	100	2024-01-05 15:22:17	2024-01-05 16:10:21	2023-12-28 14:51:10	开始 编辑 结果 删除
192.168.0.4	IP发现	完成	100	2023-12-28 13:45:00	2023-12-28 13:47:35	2023-12-28 13:45:00	开始 编辑 结果 删除
192.168.0.*	IP发现	完成	9	2023-12-28 11:51:29		2023-12-28 11:51:28	开始 编辑 结果 删除
192.168.0.*	IP发现	已停止	10	2023-12-28 11:51:29		2023-12-28 11:51:27	开始 编辑 结果 删除
1	IP发现	已停止	1	2023-12-28 11:50:49		2023-12-27 10:45:53	开始 编辑 结果 删除

共 6 条 < 1 > 前往 1 页 10条/页

基础信息

任务名: 测试 任务类型: IP发现 状态: 完成 自动扫描: 开启 进度: 100%

IP 端口 服务 操作

IP 192.168.0.220 端口 161 协议 udp 服务 snmp 操作 添加资产 删除

IP 192.168.0.220 端口 8081 协议 tcp 服务 http-proxy 操作 添加资产 删除

IP 192.168.0.220 端口 8080 协议 tcp 服务 http-proxy 操作 添加资产 删除

IP 192.168.0.220 端口 4002 协议 tcp 服务 java-ssi 操作 添加资产 删除

IP 192.168.0.220 端口 4001 协议 tcp 服务 newcaik 操作 添加资产 删除

IP 192.168.0.220 端口 443 协议 tcp 服务 https 操作 添加资产 删除

IP 192.168.0.220 端口 22 协议 tcp 服务 ssh 操作 添加资产 删除

IP 192.168.0.210 端口 443 协议 tcp 服务 https 操作 添加资产 删除

IP 192.168.0.210 端口 22 协议 tcp 服务 ssh 操作 添加资产 删除

IP 192.168.0.209 端口 10012 协议 tcp 服务 unknown 操作 添加资产 删除

共 120 条 < 1 2 3 4 5 6 ... 12 > 前往 1 页 10条/页

备注说明	资产发现任务发起方法有两种： 1. 【系统首页】>【快速入口】>【资产发现】 2. 【资产管理】>【资产发现】>新建
------	--

## 1.2 子域名猜解

### 1.2.1 场景说明

通过字典猜解扫描发现存在的子域名信息。

在本场景中，待扫域名的信息参见下表。

表 1-2 场景说明—扫描信息

域名	Baidu.com
域名爆破字典	子域名爆破字典（系统内置）
域名并发数	5
单域名并发线程数	100



子域名指二级域名，二级域名是顶级域名（一级域名）的下一级，比如 `http://a.com` 是个顶级域名，`http://bbs.a.com`、`http://mail.a.com` 这类的域名就是子域名，子域名又叫多级域名。

### 1.2.2 操作步骤

任务类型	资产发现—子域名猜解
描述	发现猜解存在的子域名信息
拓扑示意	无
预置条件	扫描器与目标域名网络可达，扫描器配置 DNS；猜解字典模板里能够匹配上目标

<p>操作步骤</p>	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统;</li> <li>2. 在“资产管理”-&gt;“资产发现”-&gt;新建任务，参数如下： <div data-bbox="363 344 1123 788" data-label="Form"> <p>任务类型 <input type="radio"/> IP发现 <input checked="" type="radio"/> 子域名发现</p> <p>* 任务名 <input type="text" value="测试"/> 2 / 128</p> <p>* 域名 <input type="text" value="baidu.com"/> <small>支持输入格式: example.com example.cn example.com.cn 多个用英文逗号或换行分割</small></p> <p>域名爆破字典 <input type="text" value="子域名爆破字典"/> <input type="button" value="模板配置"/></p> <p>域名并发数 <input type="text" value="5"/> <small>范围: (1-10)</small></p> <p>单域名并发线程数 <input type="text" value="100"/> <small>范围: (1-500)</small></p> </div> </li> <li>3. 配置完成后点击“保存并执行”按钮，即可开始进行任务。</li> <li>4. 查看结果：扫描完成后点击任务右侧的“结果”，查看扫描结果，扫描结果支持添加到应用资产库。</li> </ol>
<p>备注说明</p>	<p>资产发现任务发起方法有两种：</p> <ol style="list-style-type: none"> <li>1. 【系统首页】&gt;【快速入口】&gt;【资产发现】</li> <li>2. 【资产管理】&gt;【资产发现】&gt;新建</li> </ol>

## 2 新建系统扫描任务

本章节将基于具体场景，引导您快速创建系统扫描任务。

### 2.1 非登陆扫描

#### 2.1.1 场景说明

远程扫描目标主机存在的漏洞信息、端口服务信息。

在本场景中，待扫主机和扫描方式的信息参见下表。

表 2-1 场景说明—待扫主机信息

扫描目标主机	192.168.0.66
扫描端口	常用端口模板
端口扫描方式	TCP Connect
漏洞模板选择	全部漏洞
是否扫描工控漏洞	不扫描
执行方式	手动执行扫描



非登陆扫描指的是不登录目标主机，直接输入目标进行远程扫描。

#### 2.1.2 操作步骤

任务类型	系统扫描
描述	系统扫描用于发现目标主机存在的漏洞信息
拓扑示意	
前置条件	扫描器与目标域名网络可达，中间不要有安全防护设备作访问策略限制，否则扫不到漏洞信息或者漏洞信息不全

<p style="text-align: center;"><b>操作步骤</b></p>	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</li> <li>2. *在【扫描管理】&gt;【系统扫描】页面下，点击“新建”，进入任务新建页面，建议使用系统默认参数模板，参考参数如下： <div data-bbox="338 353 1444 884" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>编辑任务</p> <p>*任务名称 <input type="text" value="192.168.0.66"/> 12 / 128</p> <p>描述 <input type="text" value=""/> 0 / 1024</p> <p>目标 <span style="border-bottom: 1px solid #00aaff; text-decoration: underline;">手动输入IP</span> 手动输入域名 从网络资产库中选择 从文件导入</p> <div style="border: 2px solid red; padding: 5px; display: inline-block; margin: 5px 0;">192.168.0.66</div> <div style="font-size: 0.8em; margin-left: 10px;">           IP示例:            192.168.2.1, 192.168.2.2, 192.168.2.1-255, 192.168.2.1-192.168.2.255, 192.168.2.0/24, 192.168.2.*, fe80::20c:29ff:fe9f:b7f1:126:fe80::20c:29ff:fe9f:b7f1-b7f1, fe80::20c:29ff:fe9f:b7f1-fe80::20c:29ff:fe9f:b7f1ew         </div> <p>任务优先级 <input type="text" value="默认"/></p> <p>扫描节点 <input type="text" value="auto"/> <small>● auto表示自动负载均衡,将扫描任务下发到最优的扫描节点,单机部署时下发到本机。</small></p> <p>执行方式 <input type="text" value="手动"/></p> <div style="border: 2px solid red; padding: 5px; display: inline-block; margin: 5px 0;">           参数模板 <input type="text" value="默认模板(TCP Connect扫描常用漏洞端口)"/> <input type="button" value="模板配置"/> </div> </div> </li> <li>3. *配置任务扫描参数完成后点击“保存并执行”按钮，即可开始扫描任务。</li> <li>4. 查看结果：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。</li> <li>5. 生成报表：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“报表”，跳转到报表管理生成系统扫描报表页面，生成报表成功后点击下载即可。</li> </ol>
<p style="text-align: center;"><b>其它</b></p>	<p>系统扫描任务发起方法有三种：</p> <ol style="list-style-type: none"> <li>1.【系统首页】&gt;【快速入口】&gt;【系统扫描】</li> <li>2.【扫描管理】&gt;【系统扫描】&gt;新建</li> <li>3.通过资产库直接对资产发起系统扫描任务</li> </ol>
<p style="text-align: center;"><b>备注说明</b></p>	<ol style="list-style-type: none"> <li>1.如果扫描目标是禁 ping 的主机，需要开启“跳过主机存活检测”选项。</li> <li>2.扫描目标支持网段、支持 IPV4、IPV6</li> <li>3.扫描工控目标需要在参数中开启相关配置：基础选项—通用设置——扫描工控漏洞</li> </ol>

## 2.2 登陆扫描

### 2.2.1 场景说明

远程登陆扫描目标主机存在的漏洞信息、端口服务信息。

在本场景中，待扫主机和扫描方式的信息参见下表。

表 2-2 场景说明—待扫主机信息

扫描目标主机	192.168.0.66
目标操作系统	CentOS
扫描端口	常用端口模板
端口扫描方式	TCP Connect
漏洞模板选择	全部漏洞
是否扫描工控漏洞	不扫描
执行方式	手动执行扫描



登陆扫描指的是通过录入目标主机的凭证信息，扫描任务结合凭证登录目标主机，扫描目标主机存在的端口服务和漏洞信息，登陆扫描扫描到的信息会更多。

## 2.2.2 操作步骤

任务类型	系统扫描
描述	系统扫描用于发现目标主机存在的漏洞信息
拓扑示意	<p>目标IP: 192.168.0.66</p> <p>交换机</p> <p>紫光漏洞扫描系统</p>
预置条件	扫描器与目标域名网络可达，中间不要有安全防护设备作访问策略限制，否则扫不到漏洞信息或者漏洞信息不全，目标的登陆凭证可以远程登陆成功。
操作步骤	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</li> <li>2. *在【资产管理】&gt;【凭证管理】中新增录入目标主机的登陆凭证并验证是否成功。</li> <li>3. *在【扫描管理】&gt;【系统扫描】页面下，点击“新建”，进入任务新建页面，建议使用系统默认参数模板，参考参数如下：</li> </ol>

	<div data-bbox="338 224 1445 748"> <p>编辑任务</p> <p>* 任务名称 <input type="text" value="192.168.0.66"/> 12 / 128</p> <p>描述 <input type="text" value=""/> 0 / 1024</p> <p>目标 <a href="#">手动输入IP</a> <a href="#">手动输入域名</a> <a href="#">从网络资产库中选择</a> <a href="#">从文件导入</a></p> <p><input type="text" value="192.168.0.66"/> IP示例: 192.168.2.1, 192.168.2.2, 192.168.2.1-255, 192.168.2.1-192.168.2.255, 192.168.2.0/24, 192.168.2.*, fe80::20c:29ff:fe9f:b71e/126, fe80::20c:29ff:fe9f:b711-b7ff, fe80::20c:29ff:fe9f:b711-fe80::20c:29ff:fe9f:b71e</p> <p>任务优先级 <input type="text" value="默认"/></p> <p>扫描节点 <input type="text" value="auto"/> <small>● auto表示自动负载均衡,将扫描任务下发到最优的扫描节点。单机部署时下发到本机。</small></p> <p>执行方式 <input type="text" value="手动"/></p> <p>参数模板 <input type="text" value="默认模板(TCP Connect扫描常用扫描端口)"/> <input type="button" value="模板配置"/></p> <p><a href="#">基础选项</a> <a href="#">高级选项</a></p> </div> <p>4. *在任务参数中，在“高级选项”里，开启登陆主机扫描，选择录入的主机凭证</p> <div data-bbox="363 882 1458 1245"> <p><a href="#">基础选项</a> <a href="#">高级选项</a></p> <p><a href="#">凭证设置</a> <a href="#">主机设置</a> <a href="#">插件设置</a> <a href="#">并发设置</a> <a href="#">扫描结果</a> <a href="#">其它设置</a></p> <p>密码爆破 <input type="checkbox"/></p> <p>发送扫描通知 <input type="checkbox"/> <small>● 需要选择对应主机的登录凭证才可以发送扫描通知</small></p> <p>登录主机扫描 <input checked="" type="checkbox"/></p> <p>登录凭证选择 <input type="text" value="root@192.168.0.66(ssh.22) x"/></p> <p>域扫描 <input type="checkbox"/></p> <p><input type="button" value="上一步"/></p> <p><input type="button" value="取消"/> <input type="button" value="保存并执行"/> <input type="button" value="保存"/></p> </div> <p>5. 配置任务扫描参数完成后点击“保存并执行”按钮，即可开始扫描任务。</p> <p>6. 查看结果：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。</p> <p>7. 生成报表：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“报表”，跳转到报表管理生成系统扫描报表页面，生成报表成功后点击下载即可。</p>
备注说明	<p>系统扫描任务发起方法有三种：</p> <ol style="list-style-type: none"> <li>1.【系统首页】&gt;【快速入口】&gt;【系统扫描】</li> <li>2.【扫描管理】&gt;【系统扫描】&gt;新建</li> <li>3.通过资产库直接对资产发起系统扫描任务</li> </ol>

# 3 新建应用扫描任务

本章节将基于具体场景，引导您快速创建应用扫描任务。

## 3.1 应用扫描

### 3.1.1 场景说明

远程扫描测试互联网网站目标存在的漏洞信息。

在本场景中，待扫网站和扫描方式的信息参见下表。

表 3-1 场景说明—待扫网站信息

扫描目标 URL	http://testphp.vulnweb.com/
网络访问	互联网访问
参数模板	默认模板
漏洞模板	默认漏洞模板
执行方式	手动执行扫描



应用漏扫一般是两个流程，先是通过爬虫爬取对应的 URL，然后执行漏洞扫描。

### 3.1.2 操作步骤

任务类型	应用扫描
描述	应用扫描用于发现目标网站应用存在的漏洞信息
拓扑示意	
预置条件	扫描器与目标域名网络可达，目标没有 WAF 拦截访问；扫描器需配置好 DNS。



# 4 新建数据库扫描任务

本章节将基于具体场景，引导您快速创建数据库扫描任务。

## 4.1 非登陆数据库扫描

### 4.1.1 场景说明

远程扫描目标主机中数据库应用存在的漏洞信息。

在本场景中，待扫数据库信息参见下表。

表 4-1 场景说明—待扫目标信息

扫描目标数据库主机 IP	192.168.0.7
数据库类型	Mysql
参数模板	默认模板
端口模板	数据库端口
漏洞模板	全部漏洞模板
端口扫描方式	TCP SYN
执行方式	手动执行扫描



非登陆扫描指的是不登录目标数据库，直接远程扫描目标数据库。

### 4.1.2 操作步骤

任务类型	数据库扫描
描述	数据库扫描用于发现目标数据库存在的漏洞信息
拓扑示意	

预置条件	扫描器与目标 IP 网络可达，中间不要有安全防护设备作访问策略限制，同时数据库不要把漏扫 IP 拉黑，否则扫不到漏洞信息或者漏洞信息不全。
操作步骤	<p>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</p> <p>2. *在【扫描管理】&gt;【数据库扫描】页面下，点击“新建”，进入任务新建页面，建议使用系统默认参数模板，参考参数如下：</p>  <p>3. *配置任务扫描参数完成后点击“保存并执行”按钮，即可开始扫描任务。</p> <p>4. 查看结果：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。</p> <p>5. 生成报表：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“报表”，跳转到报表管理生成数据库扫描报表页面，生成报表成功后点击下载即可。</p>
其它	<p>数据库扫描任务发起方法有三种：</p> <ol style="list-style-type: none"> <li>1.【系统首页】&gt;【快速入口】&gt;【数据库扫描】</li> <li>2.【扫描管理】&gt;【数据库扫描】&gt;新建</li> <li>3.通过资产库直接对资产发起数据库扫描任务</li> </ol>
备注说明	如果扫描目标是禁 ping 的主机，需要开启“跳过主机存活检测”选项。

## 4.2 登陆数据库扫描

### 4.2.1 场景说明

远程登陆扫描目标数据库应用存在的漏洞信息。

在本场景中，待扫数据库信息参见下表。

表 4-2 场景说明—待扫目标信息

扫描目标数据库主机 IP	192.168.0.7
数据库类型	Mysql
参数模板	默认模板
端口模板	数据库端口
漏洞模板	全部漏洞模板
端口扫描方式	TCP SYN
执行方式	手动执行扫描



登陆扫描指的是扫描器录入数据库的登录凭证信息后，结合登录凭证进行深入的扫描，所以扫描前要获取数据库类型、凭证等信息，同时数据库支持第三方远程登陆。

### 4.2.2 操作步骤

任务类型	数据库扫描
描述	登录数据库扫描用于发现目标数据库存在的漏洞信息
拓扑示意	<p>The diagram illustrates the network setup for the scan. On the left, a box labeled '目标: 192.168.0.7' contains a MySQL database icon. A line connects this to a central box labeled '交换机' (Switch) with a switch icon. Another line connects the switch to a box on the right labeled '紫光漏洞扫描系统' (Purple Light Vulnerability Scanning System) containing a screenshot of the system's interface.</p>
预置条件	扫描器与目标 IP 网络可达，中间不要有安全防护设备作访问策略限制，同时数据库不要把漏洞 IP 拉黑，否则扫不到漏洞信息或者漏洞信息不全；数据库支持第三方远程登陆
操作步骤	1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；

2. \*在【资产管理】>【数据库资产】页面新建数据库资产，录入 IP、数据库类型、端口、用户名、密码、开启“执行登陆扫描”选项。然后保存。

3. \*在【扫描管理】>【数据库扫描】页面下，点击“新建”，进入任务新建页面，在扫描目标里，选择“资产库”，然后勾选上一步创建的数据库资产，参数模板使用系统默认参数模板，参考参数如下：

资产名	IP	数据库类型	端口	操作
<input checked="" type="checkbox"/> Mysql	192.168.0.7	Mysql	3306	编辑
<input type="checkbox"/> Mysql	192.168.0.4	Mysql	3306	编辑
<input type="checkbox"/> 66	192.168.0.66	未知	0	编辑

4. \*配置任务扫描参数完成后点击“保存并执行”按钮，即可开始扫描任务。
5. 查看结果：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。
6. 生成报表：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“报表”，跳转到报表管理生成数据库扫描任务报表页面，生成报表成功后点击下载即可。

其它

- 数据库扫描任务发起方法有三种：
- 1.【系统首页】>【快速入口】>【数据库扫描】
  - 2.【扫描管理】>【数据库扫描】>新建
  - 3.通过资产库直接对资产发起数据库扫描任务

备注说明

如果扫描目标是禁 ping 的主机，需要开启“跳过主机存活检测”选项。

# 5 新建基线核查任务

本章节将基于具体场景，引导您快速创建数据库扫描任务。

## 5.1 在线检查任务

### 5.1.1 场景说明

远程使用默认模板对目标进行基线核查。

在本场景中，待查目标主机信息参见下表。

表 5-1 场景说明—待扫目标信息

扫描目标数据库主机 IP	192.168.0.66
目标操作系统类型	CentOS7
远程登陆协议	ssh
基线检查模板	默认模板
采集方式	在线检查
执行方式	手动执行扫描



在线检查指的是通过远程登陆目标主机进行基线配置核查。

### 5.1.2 操作步骤

任务类型	基线配置核查
描述	在线远程对目标主机进行基线配置核查，发现目标主机不合规的配置项
拓扑示意	
预置条件	扫描器与目标 IP 网络可达，扫描器能够通过 ssh 协议远程用户访问目标主机，用户权限需要等同于 root 用户权限。

1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；
2. \*在【资产管理】>【网络资产】页面新建资产，录入/导入资产名称、资产 IP、选择配置规范为：Linux—Centos 配置规范。然后保存。

网络资产编辑页

\* 名称 服务器 3 / 128 \* IP 192.168.0.66 12 / 64

描述 0 / 1024

设备编号 0 / 128 位置 请选择 标签 请选择

可信设备  权重 0 选择组织架构 选择组织架构

所属业务系统 0 / 128 网络区域 请选择 负责人 0 / 64

联系方式 0 / 64 邮箱 0 / 64

登录凭证选择 请选择  目标自动识别

配置规范 Linux - Centos配置规范

+ 新建 配置规则

3. \*在【资产管理】>【凭证管理】页面下，点击“新建”，进入新增凭证页面，输入 IP、协议、端口、用户名、密码等信息，然后可以点击登陆验证测试是否能够登陆成功，参考参数如下：

编辑凭证

\* IP 192.168.0.59

\* 协议 smb

\* 端口 445

\* 用户名 TL 2 / 128

密码 .....

enable 用户名 0 / 128

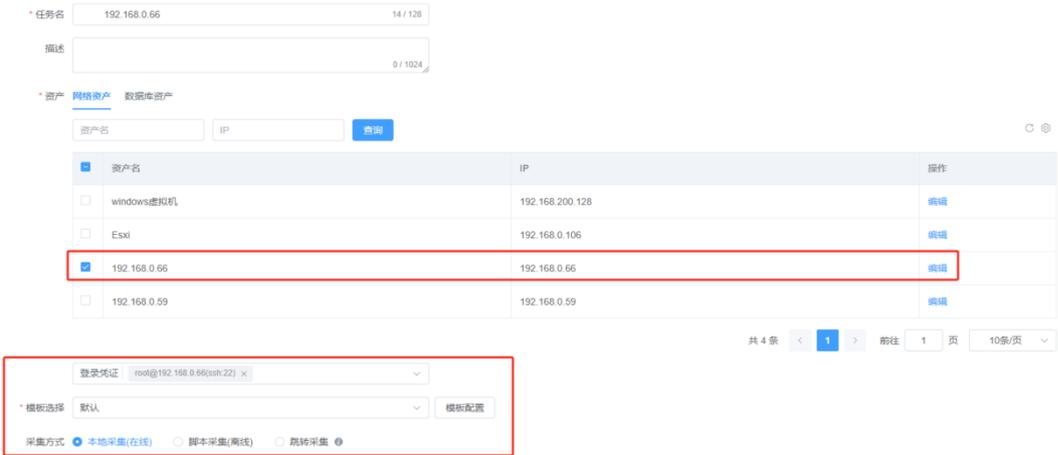
enable 密码

WebUrl https://10.10.1.2:8090/ 0 / 128

apiKey(token)

4. \*在【扫描管理】>【基线核查】页面下新建基线核查任务，配置任务参数：选择网络资产，勾选第 2 步创建的资产，登陆凭证选择 3 步创建的凭证，模板选择“默认”，采集方式选择“本地采集（在线）”。

操作步骤

	 <p>然后点击“保存并执行”，即可开始任务。</p> <p>5. 查看结果：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。</p> <p>6. 生成报表：扫描完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“报表”，跳转到报表管理生成基线核查扫描报表页面，生成报表成功后点击下载即可。</p>
其它	<p>基线核查任务发起方法有两种：</p> <ol style="list-style-type: none"> <li>1.【系统首页】&gt;【快速入口】&gt;【基线核查】</li> <li>2.【扫描管理】&gt;【基线核查】&gt;新建</li> </ol>
备注说明	<p>基线核查结果为未知项的，需要人工判定</p>

## 5.2 离线检查任务

### 5.2.1 场景说明

远程使用等保三级模板对 windows 主机目标进行基线核查。

在本场景中，待查目标主机信息参见下表。

表 5-2 场景说明—待扫目标信息

扫描目标数据库主机 IP	192.168.0.7
目标操作系统类型	Windows10
基线检查模板	默认模板

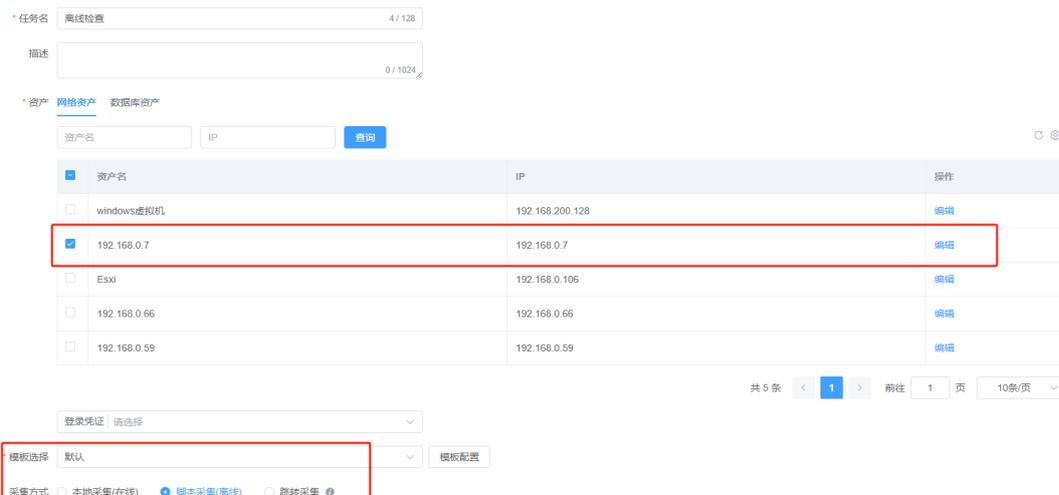
采集方式	离线检查
执行方式	手动执行扫描



离线检查一般用于扫描系统无法与检查目标主机网络通信，需要人为下载离线工具到目标主机运行，将运行结果导出到扫描系统中分析结果。

## 5.2.2 操作步骤

任务类型	基线配置核查
描述	通过离线工具对目标主机进行基线配置核查，然后将结果导入漏扫系统，发现目标主机不合规的配置项
拓扑示意	
前置条件	目标主机支持运行 windows 离线检查脚本
操作步骤	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</li> <li>2. *在【扫描管理】&gt;【基线核查】页面新建资产，录入/导入资产名称、资产 IP、选择配置规范为：Windows—Windows 配置规范。然后保存。</li> </ol> <ol style="list-style-type: none"> <li>3. *在【扫描管理】&gt;【基线核查】页面下新建基线核查任务，配置任务参数：选择网络资产(勾选第 2 步创建的资产)，无须选择登陆凭证选择，模板选择“默认”，采集方式选择“脚本采集（离线）”。</li> </ol>



然后点击“保存并执行”，即可完成任务创建。

4. \*在【模板管理】>【离线检查工具】页面中，操作系统下，点击下载“Windows 配置规范”工具，然后将脚本工具拷贝到目标主机（192.168.0.7）上运行，脚本名称为：WindowsBvsAgent.exe。
5. \*运行脚本工具：双击运行脚本工具，然后在弹出页面中点击开始检查，等待半分钟后会提示检查完成，然后点击导出结果。



6. \*上传结果文件：在漏扫系统中【扫描历史】页面，找到创建的离线检查任务，点击右侧的“导入脚本检查结果”按钮，在弹出框上传第5步的检查结果文件即可。
7. 查看结果：完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。
8. 生成报表：在【扫描历史】页面，选择扫描任务行，任务右侧的“报表”，跳转到报表管理生成基线核查扫描报表页面，生成报表成功后点击下载即可。

<b>其它</b>	基线核查任务发起方法有两种： 1. 【系统首页】>【快速入口】>【基线核查】 2. 【扫描管理】>【基线核查】>新建
<b>备注说明</b>	离线检查结果上传一定要上传到创建的任务里，离线目标的 IP 要与任务所选资产一致。

# 6 新建口令猜解任务

本章节将基于具体场景，引导您快速创建口令猜解扫描任务。

## 6.1 在线爆破任务

### 6.1.1 场景说明

通过字典库模板在线方式对目标进行弱口令扫描。

在本场景中，待查目标主机信息参见下表。

表 6-1 场景说明—待扫目标信息

扫描目标数据库主机 IP	192.168.0.59
目标操作系统类型	Windows10
爆破协议	RDP
用户名	administrator
密码	123456
猜解模式	在线爆破
用户名/密码字典	默认用户名/密码字典
执行方式	手动执行扫描



在线爆破指的是通过在线方式对目标主机进行字典猜解。

### 6.1.2 操作步骤

任务类型	口令猜解—在线爆破
描述	通过字典库模板在线方式对目标进行弱口令扫描，发现目标主存在的弱口令信息



## 6.2 离线 Hash 爆破任务

### 6.2.1 场景说明

通过字典库模板对离线 Hash 文件进行字典爆破。

在本场景中，待查目标主机信息参见下表。

表 6-2 场景说明—待扫目标信息

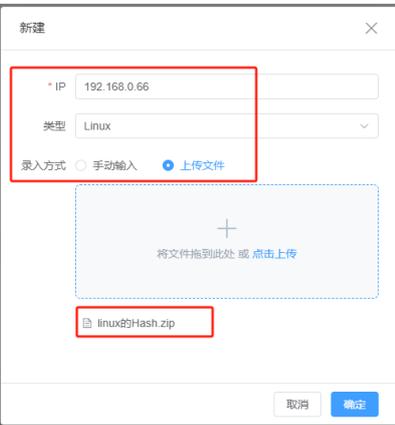
扫描目标数据库主机 IP	192.168.0.66
目标操作系统类型	CentOS7
爆破类型	Linux
用户名	root
密码	Tl@123456
猜解模式	离线 Hash 爆破
密码字典	自建密码字典
执行方式	手动执行扫描



Hash 函数常用于密码的保存,离线 Hash 爆破即使用字典中的密码经过 Hash 后与目标 Hash 对比,如果相同则成功。所以前提需要拿到密码保存的 hash 值。。

### 6.2.2 操作步骤

任务类型	口令猜解—离线 Hash 爆破
描述	结合字典库模板将 Hash 文件还原成明文
拓扑示意	无
预置条件	将目标主机中/etc/passwd 和 /etc/shadow 文件下载到本地后,压缩为.zip;同时密码字典库需要能够匹配对应的密码。

<p>操作步骤</p>	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</li> <li>2. *在【扫描管理】&gt;【口令猜解】页面新建任务，然后猜解模式选择“离线 Hash 爆破”，密码选择“离线测试密码字典”（自建的密码字典）。  </li> <li>3. 在新建页面下发点击新建，在弹出框中输入 IP 信息，类型选择“Linux”，录入方式选择“上传文件”，将 Hash 文件压缩包上传。  <p>然后确定，点击“保存并执行”，即可开始任务。</p> </li> <li>4. 查看结果：完成后点击【扫描历史】页面，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。</li> </ol>
<p>其它</p>	<p>口令猜解任务发起方法有两种：</p> <ol style="list-style-type: none"> <li>1. 【系统首页】&gt;【快速入口】&gt;【口令猜解】</li> <li>2. 【扫描管理】&gt;【口令猜解】&gt;新建</li> </ol>
<p>备注说明</p>	<p>可以根据自己的实际需求，在【模板管理】&gt;【字典管理】页面创建字典模板。</p>

# 7 新建移动扫描任务

本章节将基于具体场景，引导您快速创建移动扫描任务。

## 7.1 扫描任务

### 7.1.1 场景说明

采用静态的方式，对安卓、IOS 上的 APP 安装包进行离线扫描，发现 app 存在的风险漏洞信息。

在本场景中，待扫信息参见下表。

表 7-1 场景说明—待扫目标信息

扫描目标安装包操作系统	安卓
安装包加密加壳情况	未加密
安装包类型	apk
安装包大小	1.85 MB



目前只支持未加密的安装包进行检查。

### 7.1.2 操作步骤

任务类型	移动扫描
描述	通过静态扫描方式，发现 app 存在的风险漏洞信息
拓扑示意	

预置条件	apk 包未加密加壳，大小不超过 300Mb
操作步骤	<p>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</p> <p>2. *在【扫描管理】&gt;【移动扫描】页面新建任务，应用类型选择“Android”，上传 apk 包，然后点击“上传并扫描”后,扫描任务会自动开始。</p>  <p>3. 查看结果：完成后在页面任务栏，选择扫描任务行，任务右侧的“扫描结果”，查看扫描任务结果信息。同时可根据需要下载对应格式的扫描报告。</p>
其它	<p>基线核查任务发起方法有两种：</p> <p>1. 【系统首页】&gt;【快速入口】&gt;【基线核查】</p> <p>2. 【扫描管理】&gt;【基线核查】&gt;新建</p>
备注说明	扫描报告中只显示有风险的项。

# 8 新建镜像扫描任务

本章节将基于具体场景，引导您快速创建镜像扫描任务。

## 8.1 公开远程镜像扫描任务

### 8.1.1 场景说明

对 Docker 公开仓库容器镜像进行扫描，发现其存在的漏洞信息。

在本场景中，待扫信息参见下表。

表 8-1 场景说明—待扫目标信息

扫描目标（镜像标签）	centos:latest
仓库类型	公共仓库
镜像类型	互联网远程镜像



目前只支持未加密的安装包进行检查。

### 8.1.2 操作步骤

任务类型	镜像扫描
描述	使用扫描器对 Docker 公开仓库容器镜像进行扫描，发现其存在的漏洞信息
拓扑示意	<p>目标: centos:latest</p> <p>互联网</p> <p>交换机</p> <p>紫光漏洞扫描系统</p>
预置条件	扫描器与目标网络可达；扫描器需配置好 DNS。

<p>操作步骤</p>	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</li> <li>2. *在【扫描管理】&gt;【镜像扫描】页面新建任务，扫描目标选择“镜像扫描”，仓库类型选择“公共仓库”，输入要扫描的镜像公共标签，点击“开始”按钮后扫描任务会自动开始。</li> </ol>  <ol style="list-style-type: none"> <li>3. 查看结果：完成后在页面任务栏，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。同时可根据需要下载 doc 格式的扫描报告。</li> </ol>
<p>其它</p>	<p>镜像扫描任务发起方法有两种：</p> <ol style="list-style-type: none"> <li>1. 【系统首页】&gt;【快速入口】&gt;【镜像扫描】</li> <li>2. 【扫描管理】&gt;【镜像扫描】&gt;新建</li> </ol>
<p>备注说明</p>	<p>无</p>

## 8.2 Haobor 仓库镜像扫描任务

### 8.2.1 场景说明

登陆 Harbor 仓库拉取镜像列表，扫描镜像存在的漏洞信息。

在本场景中，待扫信息参见下表。

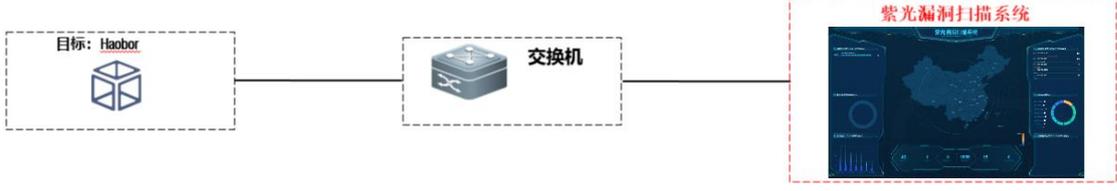
表 8-2 场景说明—待扫目标信息

仓库类型	Haobor 仓库
版本	V2



Harbor 是一个用于存储和分发 Docker 镜像的企业级 Registry 服务器。

## 8.2.2 操作步骤

任务类型	镜像扫描
描述	使用扫描器登陆 Haobor 仓库，选择仓库中的镜像进行扫描，发现其存在的漏洞信息
拓扑示意	 <p>The diagram illustrates the network setup for the scan. On the left, a scanner is connected to a switch labeled '交换机'. This switch is then connected to the '紫光漏洞扫描系统' (Purple Light Vulnerability Scanning System) on the right.</p>
前置条件	扫描器与 Haobor 仓库网络可达，获取 Haobor 仓库的登陆凭证。
操作步骤	<ol style="list-style-type: none"> <li>1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；</li> <li>2. *在【扫描管理】&gt;【镜像扫描】页面新建任务，扫描目标选择“仓库扫描”，然后输入 Haobor 仓库的地址、版本、用户名密码信息，点击“获取镜像列表”勾选要扫描的镜像标签。点击“开始”按钮进行任务扫描。</li> </ol>  <p>The screenshot shows the '新增任务' (Add Task) form. The '扫描目标' (Scan Target) is set to '仓库扫描' (Repository Scan). The '仓库地址' (Repository Address) is 'http://192.168.0.80', the '版本' (Version) is 'V2', the '用户名' (Username) is 'admin', and the '密码' (Password) is masked. The '获取镜像列表' (Get Image List) button is highlighted. Below, the '镜像列表' (Image List) shows three entries with checkboxes: '镜像标签', '192.168.0.80/tuling/dvwa v2.1.1', and '192.168.0.80/xinan/hbase v66.666'. The '开始' (Start) button is also visible.</p> <ol style="list-style-type: none"> <li>3. 查看结果：完成后在页面任务栏，选择扫描任务行，任务右侧的“结果”，查看扫描任务结果信息。同时可根据需要下载 doc 格式的扫描报告。</li> </ol>
其它	<p>镜像扫描任务发起方法有两种：</p> <ol style="list-style-type: none"> <li>1. 【系统首页】&gt;【快速入口】&gt;【镜像扫描】</li> <li>2. 【扫描管理】&gt;【镜像扫描】&gt;新建</li> </ol>
备注说明	无