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

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

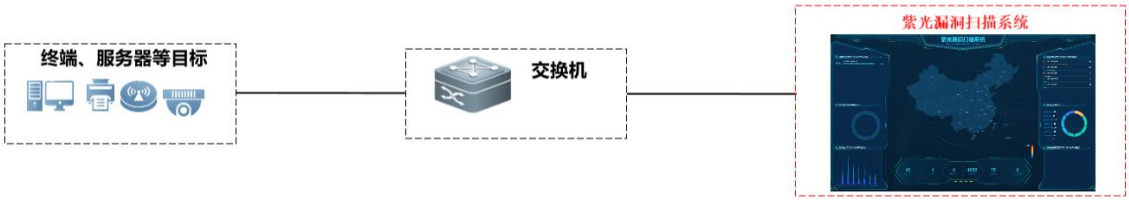
扫描探测发现网段中存活 IP、端口、服务信息。

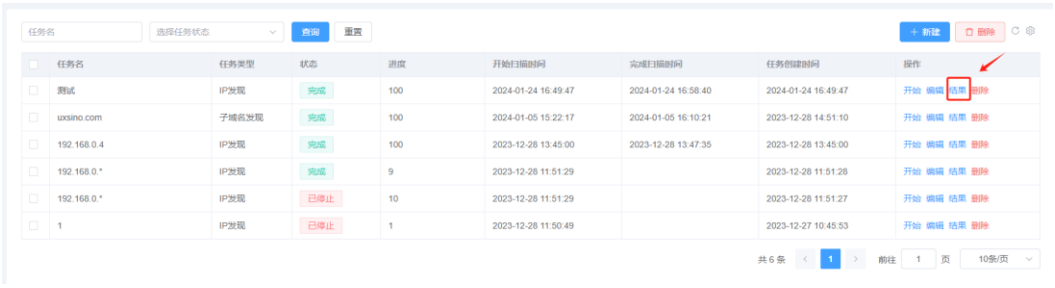
在本场景中，待扫网段和扫描方式的信息参见下表。

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

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”->“资产发现”-> 新建任务，参数如下：  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。  

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

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”->“资产发现”-> 新建任务，参数如下：**  **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应用资产库。**
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

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。

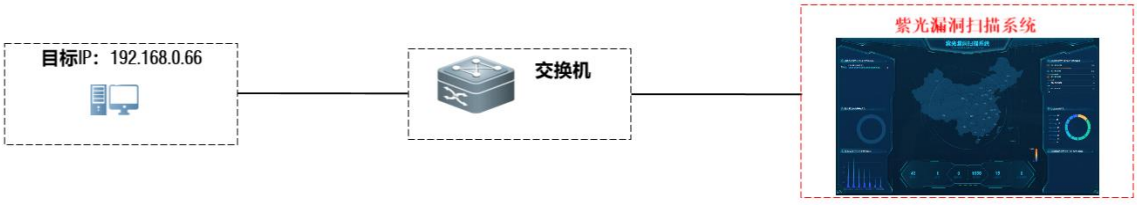
表 2-1 场景说明—待扫主机信息

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	
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

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【扫描管理】>【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：  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。 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。 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。
其它	系统扫描任务发起方法有三种： 1.【系统首页】>【快速入口】>【系统扫描】 2.【扫描管理】>【系统扫描】>新建 3.通过资产库直接对资产发起系统扫描任务
备注说明	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。 2.扫描目标支持网段、支持 IPV4、IPV6 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

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。

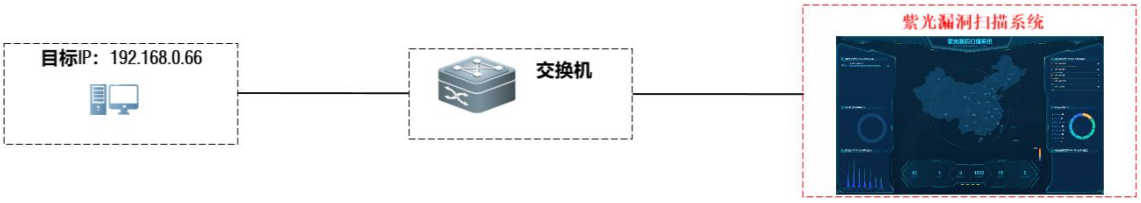
表 2-2 场景说明—待扫主机信息

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

□ □ □

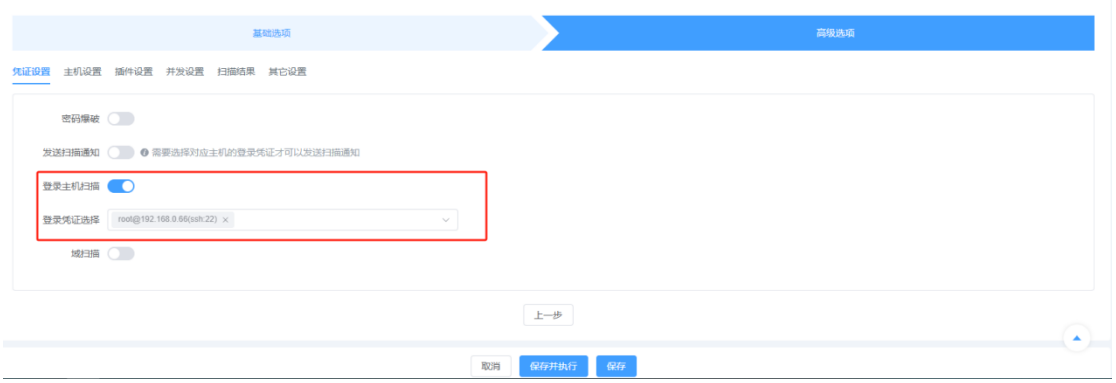
登陆扫描指的是通过录入目标主机的凭证信息，扫描任务结合凭证登录目标主机，扫描目标主机存在的端口服务和漏洞信息，登陆扫描扫描到的信息会更多。

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	
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	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】>【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。** 3. ***在【扫描管理】>【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：**

<table>
<tr>
<td></td>
<td>


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

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。

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。

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。</td>
</tr>
<tr>
<td>备注说明</td>
<td>系统扫描任务发起方法有三种：
1.【系统首页】>【快速入口】>【系统扫描】
2.【扫描管理】>【系统扫描】>新建
3.通过资产库直接对资产发起系统扫描任务</td>
</tr>
</table>

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。

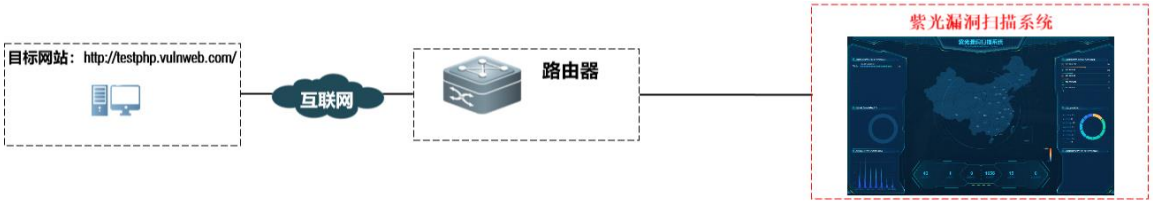
表 3-1 场景说明—待扫网站信息

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。

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【系统管理】>【设备管理】中编辑网卡，配置 DNS 地址。 3. *在【扫描管理】>【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：  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应用扫描报表页面，生成报表成功后点击下载即可。
备注说明	应用扫描任务发起方法有三种： 1.【系统首页】>【快速入口】>【应用扫描】 2.【扫描管理】>【应用扫描】>新建 3.通过资产库直接对资产发起应用扫描任务

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。

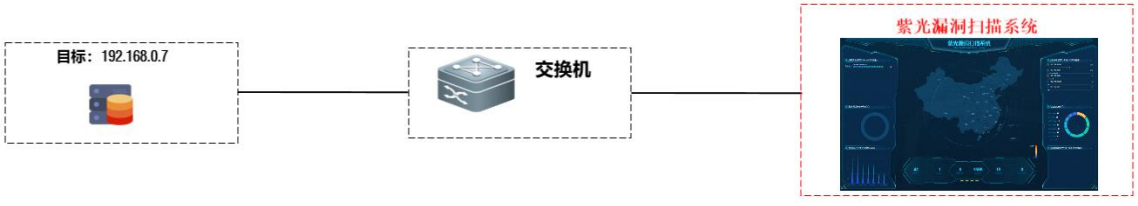
表 4-1 场景说明—待扫目标信息

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	**1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；** **2. *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，建议使用系统默认参数模板，参考参数如下：**  **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。** **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。** **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。**
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。

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。

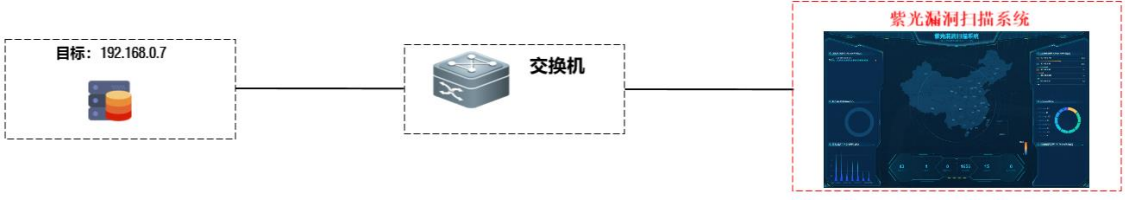
表 4-2 场景说明—待扫目标信息

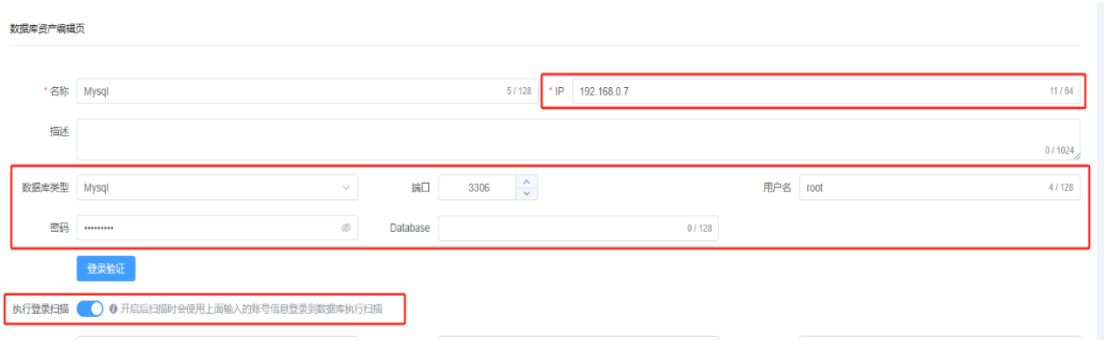
扫描目标数据库主机 IP	192.168.0.7
数据库类型	Mysql
参数模板	默认模板
端口模板	数据库端口
漏洞模板	全部漏洞模板
端口扫描方式	TCP SYN
执行方式	手动执行扫描

□ □ □

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	
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；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：  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。

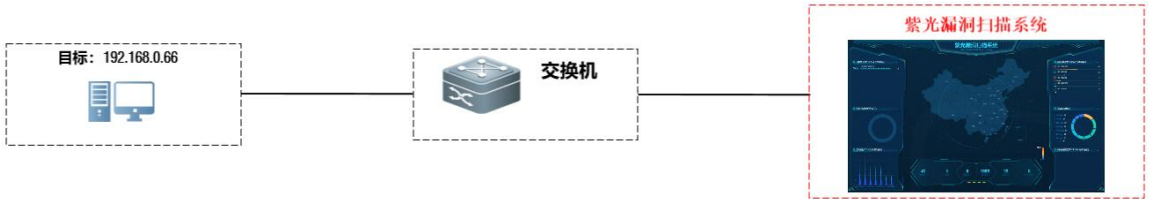
表 5-1 场景说明—待扫目标信息

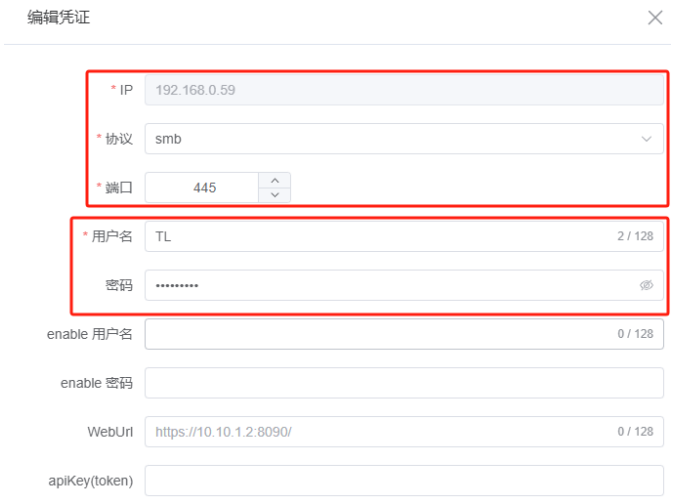
扫描目标数据库主机 IP	192.168.0.66
目标操作系统类型	CentOS7
远程登陆协议	ssh
基线检查模板	默认模板
采集方式	在线检查
执行方式	手动执行扫描

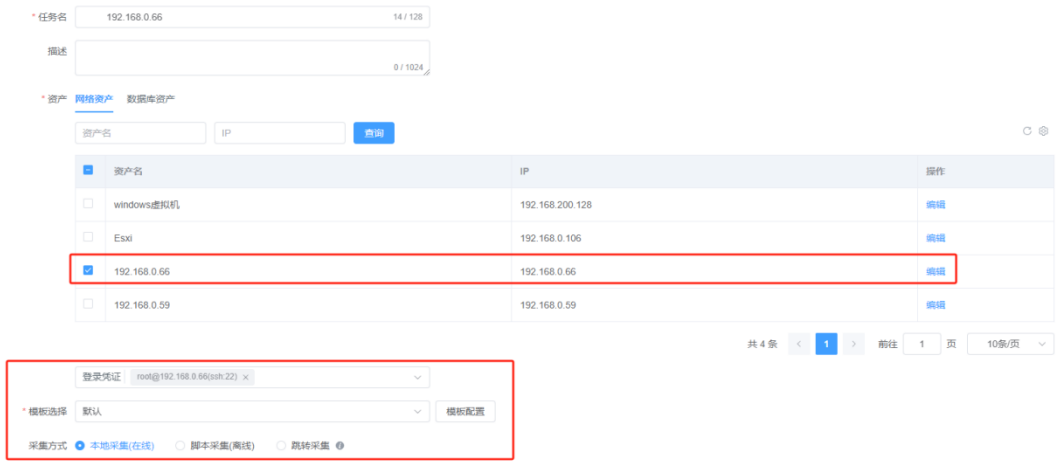
□ □ □

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。

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】>【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。  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：  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）”。

	 **然后点击“保存并执行”，即可开始任务。** **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基线核查扫描报表页面，生成报表成功后点击下载即可。**
其它	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
备注说明	基线核查结果为未知项的，需要人工判定

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

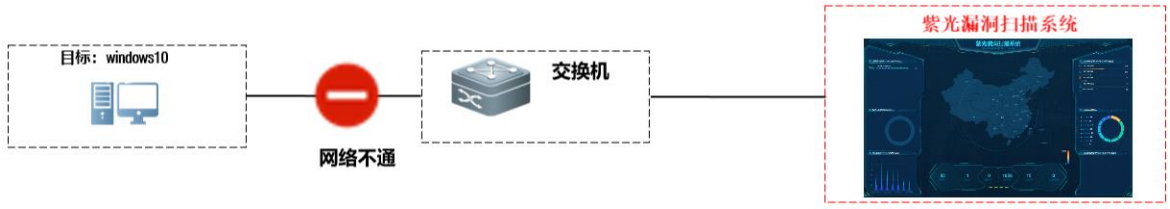
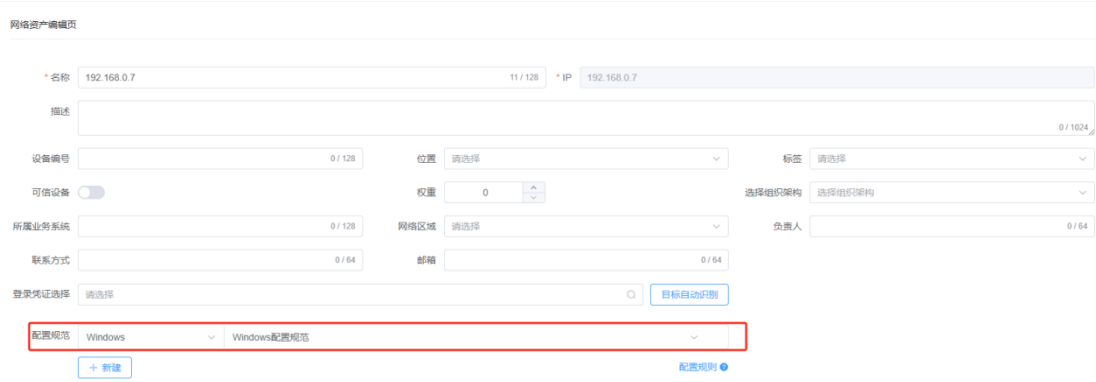
扫描目标数据库主机 IP	192.168.0.7
目标操作系统类型	Windows10
基线检查模板	默认模板

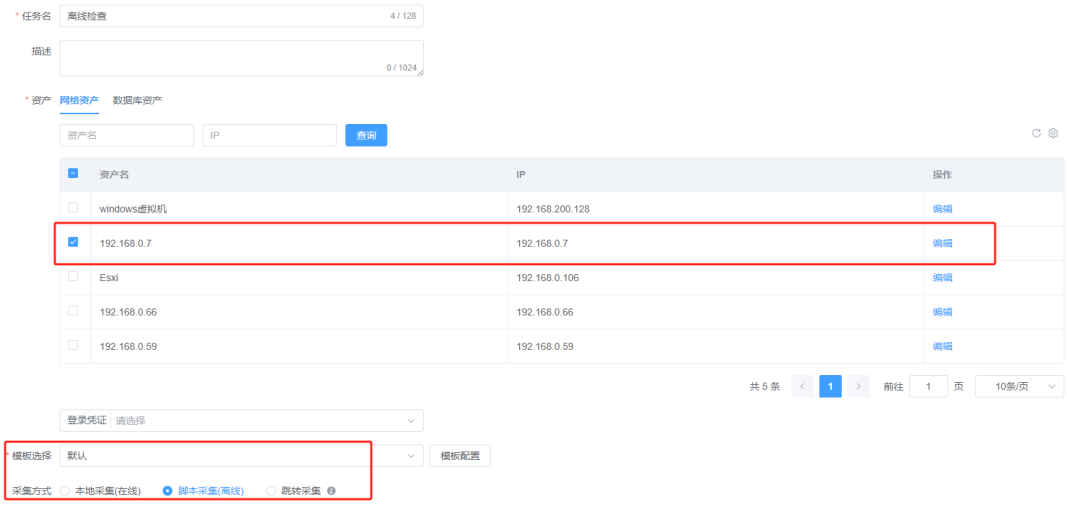
采集方式	离线检查
执行方式	手动执行扫描

□ □ □

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	
预置条件	目标主机支持运行 windows 离线检查脚本
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【扫描管理】>【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。  3. *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)，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)”。



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。

其它	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
备注说明	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

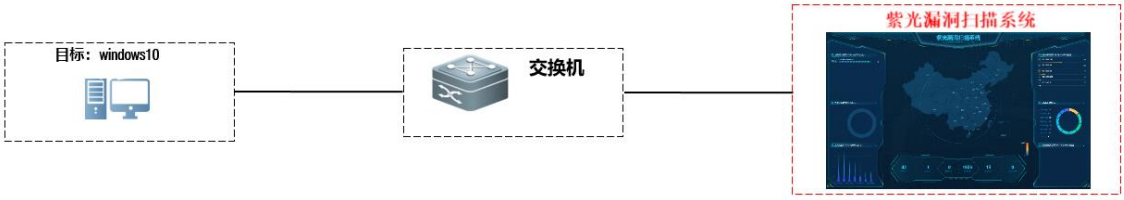
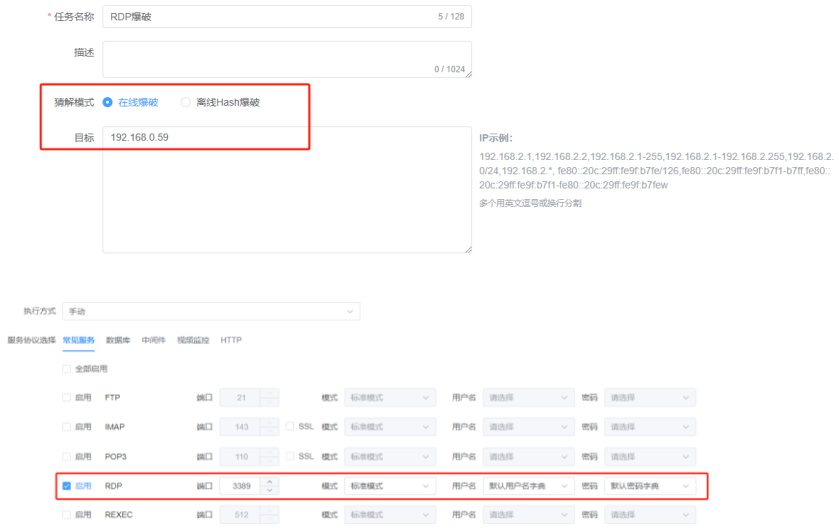
扫描目标数据库主机 IP	192.168.0.59
目标操作系统类型	Windows10
爆破协议	RDP
用户名	administrator
密码	123456
猜解模式	在线爆破
用户名/密码字典	默认用户名/密码字典
执行方式	手动执行扫描

□ □ □

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

拓扑示意	
预置条件	扫描器与目标主机网络可达，可正常访问 RDP 协议，字典模板中需要能够匹配上弱口令
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【扫描管理】>【口令猜解】页面新建任务，然后猜解模式选择“在线爆破”，输入目标 IP，在常见服务中勾选 RDP，模式标准模式，用户名选择“默认用户名字典”，密码选择“默认密码字典”。**  **然后点击“保存并执行”，即可开始扫描。** **3. 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。**
其它	口令猜解任务发起方法有两种： 1.【系统首页】>【快速入口】>【口令猜解】 2.【扫描管理】>【口令猜解】>新建
备注说明	可以根据自己的实际需求，在【模板管理】>【字典管理】页面创建字典模板。

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

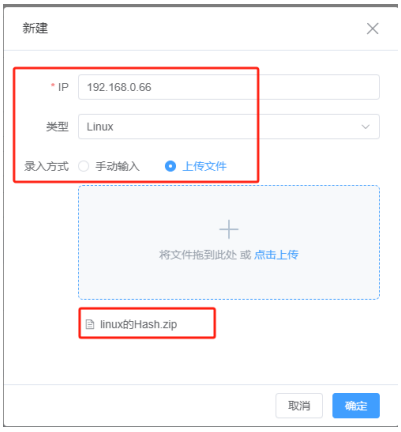
扫描目标数据库主机 IP	192.168.0.66
目标操作系统类型	CentOS7
爆破类型	Linux
用户名	root
密码	Tl@123456
猜解模式	离线 Hash 爆破
密码字典	自建密码字典
执行方式	手动执行扫描

□ □ □

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。

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【扫描管理】>【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）。  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。  然后确定，点击“保存并执行”，即可开始任务。 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。
其它	口令猜解任务发起方法有两种： 1.【系统首页】>【快速入口】>【口令猜解】 2. 【扫描管理】>【口令猜解】>新建
备注说明	可以根据自己的实际需求，在【模板管理】>【字典管理】页面创建字典模板。

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

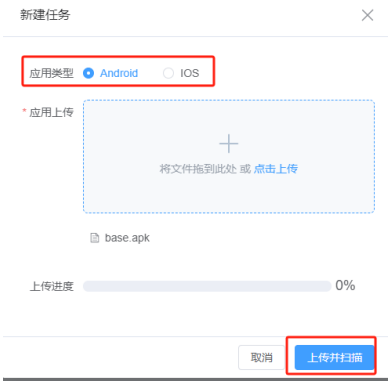
扫描目标安装包操作系统	安卓
安装包加密加壳情况	未加密
安装包类型	apk
安装包大小	1.85 MB

□ □ □

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	1. **使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统；** 2. ***在【扫描管理】>【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。**  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。**
其它	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
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。

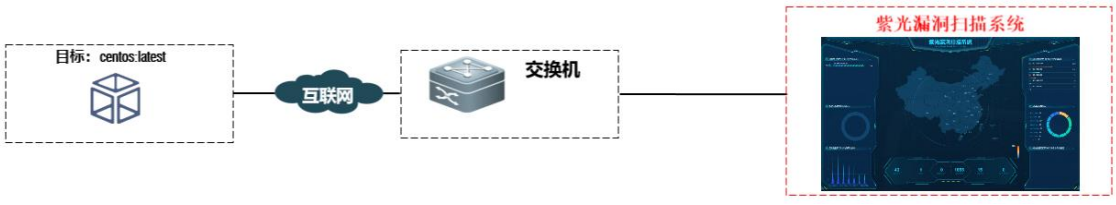
表 8-1 场景说明—待扫目标信息

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	
预置条件	扫描器与目标网络可达；扫描器需配置好 DNS。

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【扫描管理】>【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。  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。
其它	镜像扫描任务发起方法有两种： 1.【系统首页】>【快速入口】>【镜像扫描】 2.【扫描管理】>【镜像扫描】>新建
备注说明	无

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。

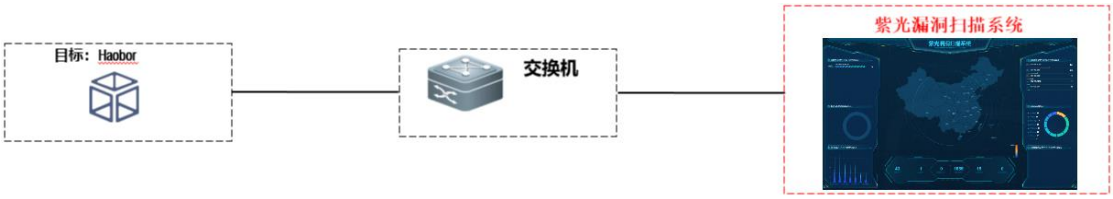
在本场景中，待扫信息参见下表。

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	
预置条件	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	1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统； 2. *在【扫描管理】>【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。  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。
其它	镜像扫描任务发起方法有两种： 1.【系统首页】>【快速入口】>【镜像扫描】 2.【扫描管理】>【镜像扫描】>新建
备注说明	无