# 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。

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 Haobor 仓库镜像扫描任务	28

# 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 场景说明一待扫主机信息

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

任务类型	资产发现一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	终端、服务器等目标 ■↓ 〒 ② ☆ ☆ 「 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
预置条件	扫描器与目标网段网络可达

Image:	2.	在"资	产管理	理"→	"资产发现	现"→	新建任务	,参数如	下:		
Image:											
*** *** *** ***** ***** ***** ***** ***** *****		任务类型	● IP发现	<ul> <li>子域名发</li> </ul>	<del></del> 灾现						
*** ***		* 任务名	测试				2 / 12	8			
★ Unit Unit Unit Unit Unit Unit Unit Unit		* IP	192,168,	0.1-254				支持输入格式:			
Image:								192.168.2.1,192.16	8.2.2		
<b>W O C C C C C C C C C C</b>								192.168.2.1-255 192.168.2.1-192.10	8.2.255		
W 10 101 1 10 101 101 101 101 101 101 10								192.168.2.0/24			
CZRQLAL BEER         LIDER THELIORS VERSE         LIDER VERSE         A UNGERSTERE VERSE								192.168.2.* 多个用英文逗号或法	英行分割		
CXR4±1       EBER#         BLDW       EREMPLOR											
A Links #Hikule##          #Links #Hikule###       ##Example         #Links #Hikule###       ##Example         #Links # Efails# @ #Hikule####       ##Example         #Links #       #Example         #Interface       @ SYN hor CPSYN(#Hiskig).connecthyTCP connect(#Exis)         #Example       @ Subschehelmendows, SY@Tib@*ub/KE         #Example       @ Subschehelmendows, SY@Tib@*ub/KE         #Example       #Example         #Example       @ Subschehelmendows, SY@Tib@*ub/KE         #Example       #Example         #Example		仅发现主机	- 是否启	用				11			
★THELLERY WEAKEN          BEZIGHT © RETHELLERY WEAKEN         BEZIGHT © STREIPHENERVICE         BEZIGHT		海口洗衣	○○田 ○○	()) () () () () () () () () () () () ()	一時時間	₩					
<ul> <li>■主文編口列葉 ● 台灣馬等特目編員主文的編口不目編編白總縣中的編日</li> <li>■社文編口列葉 ● 台灣馬等特目編員主文的編口不目編編白總縣中的編日</li> <li>■地工机規模 ● 台灣馬等地理是打磨的建築性的目子時編出所用的建築是他的是是myoqu用高管計開建度会比较增</li> <li>日調整要理 ● 台灣馬等與目時編出所用的建築是他的建築性的是新聞的建築的。Connect为TCP connect(全造場)</li> <li>日調整理 ● 台灣馬等與目時編出所用的建築是他的建築性的是新聞的建築的。</li> <li>第11個整理 ● 台灣馬等與目時編出所用的建築是他的建築性的是新聞的建築的。</li> <li>第11個整理 ● 台灣高等與目時編出所用的建築是他的建築性的。</li> <li>1日調整理 ● 台灣高等與目時編出所用的建築是他的建築性的。</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,扫描结果支持资产库。</li> </ul>		师山应洋	吊用晒口	1(1年1子)		<u>白</u>					
■ Middel @ Origine &		自定义端口列表	是否启》	用 🛛 启用后将挂	日描自定义的端口,7	不扫描端口模板中	的端口				
★□日頭欄試 「CP SVN 」 ● SYN 为TCPSYN(半连续),Connect/bTCP connect(全选统) 日編展秀型 ● 今边选标是好期目時端口所开始的服务是加快这是加快运用的服务中型 日編展章 ● 印题 ● 印		跳过主机发现	0 勾选	后不检查主机是	否在线,认为所有主	机都是在线的					
PI開發秀型 ● 今选后是U则目标调口所开启的服务是http还是myod/开启后目描通度会比较错。 PI描述论 ● 今选后会目到的undbus, S7等工论专业协议 PI描述论 ● 分选后会目到的undbus, S7等工论专业协议 PI描述 ● 印述 ● 12 ● 12 ● 12 ● 12 ● 12 ● 12 ● 12 ● 1		端口扫描模式	TCP SYN	N	✓ Ø SYN 为	oTCPSYN(半连接	);Connect为TCP c	connect(全连接)			
<ul> <li>Immersed Q Q Qualatative y at lange (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</li></ul>		ᆆᆕᄪᅒᆇᆂᆈ									
<ul> <li>I#Ⅲ世协议 ● 勾选后会扫描和mumubus, S79°工注专业协义</li> <li>I#Ⅲ速度 ● 自然 ● 快速 ● 避快速</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,扫描结果支持资产库。</li> </ul>		1711111117599至	<u>м</u> 🕡 Арт	のたたに、からないであり	니까기기여리개요ㅋㅋㅋㅋ	nupæænysqi,77/	그 여기 배조 순 조 나 부	XIE			
<text><list-item><list-item></list-item></list-item></text>		扫描工控协议	🗌 🛛 勾选	后会扫描如mudb	bus、S7等工控专业	业协议					
<ul> <li>第78 ● EEE ● TRUE ● TRU</li></ul>											
<ul> <li>●骤</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,扫描结果支持资产库。</li> </ul>		扫描速度	○ 白活成	0 快速	2 招快速						
	3.	印置完	○ <sup>自适应</sup> 【成后】	● <sup>快速</sup> 点击"伤	<sup>○ 超快速</sup> 呆存并执	行"按钮	],即可ヲ	开始进行任	E务。		
任务行         任务 欠配         送成         消成         消位         消位         消位         消位         消位           第24         戶225         第25         100         2024-01-24 16.49.47         2024-01-24 16.58.40         2024-01-24 16.49.47         746 40.47         74	3. 4.	<sup>扫描速度</sup> 配置完 査看结 资产库	○ ≋≝œ 〕成后」 〕果: 1 <sup>〕</sup> 。	● ♥≢ 点击"伊 扫描完成	○ <sup>超快速</sup> 呆存并执行 戊后点击付	行"按钮 任务右侧	[,即可 <del>]</del> ]的"结 <sup>!</sup>	开始进行住 果",查看	£务。 扫描结身	<b>果,</b> 扫	描结果支持
■ 読ん       ● P2版       ● D2K       ● D2K       0 20404246947       20404246947       20404246947       20404246947       ● D2404246947       ● D2404246947       ● D2404246947       ● D2404246947       ● D2404266947       ● D24042669478       ● D24042669478	3. 4.	日端連度 配置完 査看结 资产库	○ 目适应 (成后) 「果: 1 …。	● ♥ 点击"仍 扫描完成	○ 器快速 呆存并执行 戊后点击付	行"按钮 任务右倾	],即可∃ ]的"结∮	开始进行伯 果",查看	E务。 扫描结身	畏,扫	描结果支持
• waino.com       7463230       9263       100       202410.65 162.217       202410.65 16.10.21       2023-12.28 14.51.10       766 466 46.02 Mini 46.02 Mini 466 46.02 Mini 466.02 Mini	3. 4.	日前速度 配置完 査看结 资产库	○ 目透应 ;成后」 ;果: 3 :。	● 快速 点击" 你 扫描完成		行"按钮 任务右侧	1,即可う 1的"结身	开始进行作 果",查看	壬务。 扫描结身	<b>艮,扫</b>	描结果支持 1 EX 0 === 0 0
10x1 10x 14       10x2m       100       2023-12-20 13.4500       2023-12-20 13.47.35       2023-12-20 13.4500       开始 編集 換算         1       192.168.0*       炉笼银       902       2023-12-20 13.47.35       2023-12-20 13.47.35       2023-12-20 13.47.35       2023-12-20 13.45.00       开始 編集 換算         1       192.168.0*       炉笼银       204       10       2023-12-20 13.52.95       2023-12-20 13.52.05       2023-12-20 11.51.27       开始 編集 換算         1       1       100       2023-12-20 11.50.49       0       2023-12-20 11.51.27       开始 編集 換算         1       1       100       2023-12-20 11.50.49       0       2023-12-20 11.51.27       开始 編集 換算         1       1       100       2023-12-20 11.50.49       0       2023-12-20 11.51.27       开始 編集 換算	3. 4.	日端速度 配置完 査看结 资产库 (1986) (19	○ 目道应 派后」 课 <b>果:</b> 、	● 快速 点击" 你 扫描完成 (55年) (55+)		行"按钮 任务右侧 <sup>111</sup> 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	1,即可引 <b>1的"结</b> 身 M11 <b>3007</b>	开始进行住 果",查看 2021-01-24 16 58 40	<b>壬务。</b> 扫描结身 2024-01-24 16-4	<b>果,扫</b>	描结果支持 * KEE
192.166.0.*       192.086       192.086       10       2023.12.26 11.51.29       2023.12.26 11.51.27       756 ଲाй 65.8 189         1       1       192.086       1       2023.12.26 11.50.49       2023.12.27 10.45.53       756 ଲाй 65.8 189         上       -	3. 4.	扫描速度 配置完 査看结 资产库	<ul> <li>目透应</li> <li>派成后」</li> <li>(果: 寸)</li> <li>(</li></ul>	● 快速 点击"仍 扫描完成 <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup> <sup>(1)</sup>		行"按钮 任务右侧	1,即可引 <b>1的"结</b> <u>9</u> 941500896 204-01-24 16.49.47 204-01-05 42 07	中始进行作 果",查看 200401-24 1658-40 200401-65 16 10211	王务。 扫描结り 202401-24164 2023-1228164	<b>果,扫</b> 847 3 1110 3	抽结果支持
1     IP2短程     已停止     1     2023-12-26 11:50.49     2023-12-27 10.45.53     开始 備補 防理 動分       共合衆<<1	3. 4.	日前恵度 配置完 査看結 资产库 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	○ 目透应 〕成后〕 〕果: 寸 …。	<ul> <li>快速</li> <li>点击"6</li> <li>扫描完成</li> <li>日描完成</li> <li>日本完成</li> <li></li></ul>		行"按钮 任务右侧 <sup>100</sup>	L,即可引 <u>1的"结</u> 身 <u>M1300000</u> 222-01-24 16-48-47 222-01-24 16-48-47 222-12-28 13-46-00 222-12-28 13-46-00 222-12-28 11-01-29	中始进行作 果", 査看 2024-01-24 16.58.40 2024-01-05 16 10:211 2023-12.28 13.47.35	王务。 扫描结身 2024-01-24 164 2023-12-28 145 2023-12-28 145 2023-12-28 145	<b>東,扫</b> 947 第 11:10 第 500 第	
共6条 < <b>1</b> > 前往 1 页 10账页 >	3. 4.	扫描速度 配置完 査看结 资产库 (12168-4) 122168-4 122168-4	○ 目透应 :成后) :课: : : : : : : : : : : : : : :	<ul> <li>快速</li> <li>点击"份</li> <li>扫描完成</li> <li>日描完成</li> <li>(約束型)</li> <li>(10未1)</li> <li>(10+1)</li> <li></li></ul>		行"按钮 任务右侧 <sup>20</sup> 2 20 20 2 20 20 2 20 20 20 20 20 20 20 20 20 20 20 20 20	L,即可子 小的"结身 24401-2416-48-47 124401-2416-48-47 124401-2416-48-47 123412-2811345:00 123412-281131129	<b>平始进行住</b> 果",查看 2024-01-24 16:58-40 2024-01-28 16:10:21 2023-12-28 13:47:35	王务。 扫描结身 2024-01-24 164 2025-12-28 145 2025-12-28 145 2025-12-28 115 2025-12-28 115	<b>果,扫</b> 947 第 1110 第 500 第 128 第	描结果支持 + Rt2 0 899 0 0 Rt Rts act 0 899 Rts act
	3. 4.	扫描速度 配置完 査看结 资产库 (近): (近): (近): (近): (近): (近): (近): (近):	<ul> <li>目透应</li> <li>武成后」</li> <li>課果: 第</li> <li>(and the set of the</li></ul>	<ul> <li>快速</li> <li>点击"份</li> <li>扫描完成</li> <li>扫描完成</li> <li>(約二次)</li> <li>(11)</li> <li>(11)</li> <li>(11)</li> <li>(11)</li> <li>(11)</li> <li>(11)</li> <li>(11)</li></ul>		行"按钮 任务右侧 <sup>20</sup>	L, 即可子 小的"结身 244130000 24416.48.47 22416.48.47 22416.48.47 22416.48.49 22416.24811.45.00 22316.24811.45.00 22316.24811.45.129 22316.24811.45.129	<b>平始进行住</b> 果", 查看 2024-01-24 15:58-40 2024-01-26 15:47-25 2023-12-28 13:47:35	王务。 扫描结り 2024-01-24 16-4 2023-12-28 143 2023-12-28 143 2023-12-28 143 2023-12-28 143 2023-12-28 143 2023-12-27 10-4	<b>東,扫</b> 9.47 5 9.47 5 1110 5 800 5 128 5 127 5 853 5 853 5	描结果支持 またででのののののの またでのののののののののののののののののののののののののののののののののののの
	3. 4.	扫描速度 配置完 査看結 资产库 ( の) ( の) ( の) ( の) ( の) ( の) ( の) ( の	○ 目透应	<ul> <li>快速</li> <li>点击"份</li> <li>扫描完成</li> <li>日描完成</li> <li>日本</li> <li>日本</li></ul>		行"按钮 任务右侧 <sup>100</sup>	4, 即可子 们的"结身 224-01-24 16 48 47 224-01-24 16 48 47 224-01-24 16 48 47 224-228 11 30-22 223-12-28 11 30-29 223-12-28 11 50 49	<b> 中始进行住  ま 、                                 </b>	任务。 扫描结り 2024-01-24 16-4 2023-12-28 14-5 2023-12-28 14-5 2023-12-28 11-5 2023-12-28 11-5 2033-12-5	果, 扫 9.47 - 3 11.110 - 3 5.00 - 3 12.20 - 3 12.27 - 3 5.53 - 3 5.53 - 3 12 12.7 - 3 12 12.7 - 3 12 12.7 - 3 12 12.7 - 3 12 12.7 - 3 12.7	
	3. 4.	扫描速度 配置完 査看結 资产库 (新客) (192168.4) (192168.4) (192168.4) (192168.4) (192168.4) (192168.4) (192168.4) (192168.4)	○ 目透应	<ul> <li>快速</li> <li>点击"你</li> <li>扫描完成</li> <li>扫描完成</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> </ul>		行"按钮 任务右侧 <sup>20</sup>	4, 即可引 小的"结身 20401-24 16 49 47 20401-05 15 22 17 2042 3 12 3 12 3 60 23 12 28 11 31 29 23 12 28 11 31 29 23 12 28 11 31 29	<b>平始进行作</b> <b>果", 査看</b> 2024-01-24 16.58.40 2024-01-05 16 10:211 2023-12.28 13.47.25	<b>任务。</b> <b>打描结長</b> 2024-01-24 16.4 2023-12-28 14.5 2023-12-28 11.5 2023-12-28 11.5 2033-12-28 11.5 2023-12-28 11.5 2033-12-28 11.5 2033-12-15 2034-11.5 2034-12-15 2034-15 2034-15 2034-12-15 2034-15 2034-12-15 2034-12-15 2034-	<b>長,扫</b> 9.47 第 1110 第 128 第 127 第 12 第 12 第 12 第 12 第 12 第 12 第 12 第 12	
任务名: 現成 任务规型 17% 現 秋志: SGK 目动周期 🌑 三虎 💶 100%	3. 4.	日前恵度 配置完 査看結 资产库 (1) 22,168.4 1) 122,168.4 1) 124,168.4 1) 124,		<ul> <li>快速</li> <li>大击 " 份</li> <li>扫描完成</li> <li>日描完成</li> <li>「 25%</li> <li>「 25%</li> <li>「 12%</li> <li>「 12%</li> <li>「 12%</li> <li>「 12%</li> <li>「 12%</li> <li>( 12%)</li> <li>( 12%)&lt;</li></ul>		行"按钮 任务右侧 <sup>20</sup> 20 20 20 20 20 20 20 20 20 20 20 20 20	1, 即可子 小的"结身 <sup>100</sup> "结身 <sup>122401-241649-47</sup> <sup>122401-241649-47</sup> <sup>12241228113129</sup> <sup>12241228113129</sup> <sup>1224228115129</sup> <sup>12241228115129</sup>	<b>平始进行作</b> <b>果", 査看</b> 2024-01-24 1658.40 2024-01-24 1658.40 2024-01-65 16-10-21 2023-12-28 13.47-35	<b>住务。</b> <b>打描结</b> 2024-01-24 164 2023-1228 148 2023-1228 148 2023-1227 148 2035-1278 148 2035-1278 2035-1278 148 2035-1278 148 2035-1278 148 2035-1278 148 2035-1278 148 2035-128 205	<b>果,扫</b> 947 第 1110 第 128 第 127 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	描结果支持 1 PR2 0 899 0 0 0 HT 0 1 999 0 0 HT 0 1 999 0 0 1 页 1090页 v
(1594) <b>1884</b> (1599-182) Vot. <b>1995</b> Biologie Constant Co	3. 4.	扫描速度 配置完 査看結 资产库 (研究) ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( (		<ul> <li>快速</li> <li>点击"份 扫描完成</li> <li>日描完成</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> </ul>		行"按钮 任务右侧 <sup>20</sup> 20 20 20 20 20 20 20 20 20 20 20 20 20	1, 即可子 1的"结身 24413000 22441-2416.48-47 22441-2416.48-47 22342-281134500 22342-28113529 22342-28113529 22342-28113529	<b>F 始进行住</b> 果", 査看 200401-241658-40 200401-241658-40 200401-0516-10211 2003-12-2813-47-35	王务。 扫描结り 2024-01-24 f8-4 2023-12-28 f8-3 2023-12-28 f8-3 2023-12-28 f8-3 2023-12-28 f8-3 2023-12-28 f8-3 2023-12-27 f8-4 2023-12-27 f8-4 2023-12-27 f8-4 2023-12-27 f8-4 2023-12-27 f8-4 2023-12-28 f8-3 2023-12-28 f8-3 2033-12-28 f8-3 2035-12-28 f8-3 2035-12-1	<b>見</b> , 扫 9.47 第 128 第 127 第 553 第 127 第 553 第 127 第 12 1 12 1 12 1 12 1 1 1 1 1 1 1 1 1 1	
	3. 4.	日前恵度 配置完 査看結 资产库 (研究) ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( (		<ul> <li>快速</li> <li>点击"份 扫描完成</li> <li>扫描完成</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> <li>印2環</li> </ul>		行"按钮 任务右侧 20 20 20 20 20 20 20 20 20 20 20 20 20	1, 即可子 <u>1的"结</u> 身 24-01-24-16-48-47 24-01-24-16-48-47 24-01-24-16-48-47 22-12-28-11-30-29 22-12-28-11-30-49 22-12-28-11-30-49	<b>平始进行住</b> <b>果", 查看</b> 202401-241558-40 202401-261558-40 2023-12-2813-47-35	E务。 力描结与 20240124164 20240124164 2023-12.28145 2023-12.28145 2023-12.28145 2023-12.27164 共合策 《 《	長,扫   9.47   9.47   9.47   9.47   9.47   9.47   9.47    9.47   9.47   9.47   9.47    9.47   9.47   9.47   9.47    9.47   9.47   9.47   9.47   9.47   9.47   9.47    9.47    9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47   9.47    9.47   9.47   9.47   9.47    9.47   9.47    9.47   9.47    9.47   9.47   9.47   9.47    9.47   9.47   9.47    9.47   9.47    9.47    9.47    9.47   9.47   9.47   9.47    9.47    9.47    9.47   9.47    9.47   9.47    9.47   9.47    9.47   9.47    9.47    9.47    9.47   9.47    9.47    9.47   9.47    9.47   9.47    9.47    9.47   9.47    9.47   9.47    9.47   9.47    9.47    9.47    9.47    9.47    9.4	描结果支持 ■ KIE
	3. 4.	扫描速度 配置完 査看結 资产库 ・ 低彩 ・ 低彩 ・ 低彩 ・ いいの ・ いの ・ いいの ・ いいの ・ いいの ・ いいの ・ いの ・ いいの ・ いの ・ いいの ・ いの ・ いいの ・ いいの ・ いいの ・ いいの ・ いいの ・ いいの ・ いいの	<ul> <li>自适应</li> <li>(現人后)</li> <li>(現人)</li> </ul>	<ul> <li>快速</li> <li>快速</li> <li>片油</li> <li>竹油</li> <li>行加</li> <li></li></ul>			L, 即可子 1的"结与 10的"结与 24-01-24-16-18-27 12-12-22 11-52-9 12-12-22 11-52-9 12-12-22-9 12-12-22-9	中始进行係 果", 査看 2024-01-24 16:58-04 2023-12-28 13:47:35 2023-12-28 13:47:35 2023-12-28 13:47:35	ESCEWER	<ul> <li>キャ・扫</li> <li>キャ・扫</li> <li>キャ・カー</li> <li></li></ul>	
	3. 4.	扫描速度 配置完 変子存 変子存 である である である である。 152168.04		<ul> <li>快速</li> <li>快速</li> <li>「日 抽 完成</li> <li>日 抽 完成</li> <li>日 2 元</li> <li>日</li></ul>		行" 按钮 任务右( 2 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	<ol> <li>即可引</li> <li>加 "结只</li> <li>約 "结只</li> <li>約 "结只</li> <li>約 "结只</li> <li>約 "结只</li> <li>約 "结只</li> <li>約 "结只</li> <li>2 4 0 1 4 9 4 7 1 1 2 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 2 1 1 2 1 1 1 2 1 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 2 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</li></ol>	中始进行名 果", 査看 2024-01-24 16.58.40 2024-01-05 16 10.21 2023-12-28 13.47.35 2023-12-28 13.47.55 2023-12-28 13	E务。 力描结り 20240124164 20240124164 202240124164 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 20231228115 2023128116	長,扫	
Life     Mat     Life     Mat     Mat<	3. 4.	日面恵度 配置完 変产库 で、 「「「「」」 「」」 「」」 「」」 「」」 「」」 「」」	<ul> <li>自适应</li> <li>() 現代日</li> <li>() 現代日</li></ul>	● 快速           点击 " 伊           扫描完成           日 法           「 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法           」 日 法		行" 按钮 任务右() 200 2 201	1、即可う           1的 "结り           160 "结り           161 1680所           204 01-24 16 49 47           204 01-24 16 49 47           204 01-24 16 49 47           204 01-24 16 49 47           204 01-24 16 49 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 16 19 47           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 11 19 49           204 01-24 19 19 49           204 01-24 19 19 19 19 19 19 19 1	中始进行係 スパンパンパンパンパンパンパンパンパンパンパンパンパンパンパンパンパンパンパン	E分。 打描结長 202401-24 16.4 202401-24 16.4 2023-12-28 115	長、扫	
Image: Point of the point o	3. 4.	日面速度 配置完 変产库 で、 「「」、 「」、 「」、 「」、 「」、 「」、 「」、 「	<ul> <li>自适应</li> <li>() 最近</li> <li>(</li></ul>		○ 超快速       日本     日本 <t< td=""><td></td><td></td><td>中始进行名 果、、 査看 2024-01-24 16:58.40 2024-01-24 16:58.40 2024-01-24 16:58.40 2024-01-26 16:10:21 2023-12-28 13.47:35 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2024-01-26 16:10 2024-01-26 16:10 2024-01</td><td>ES . 13 H 4 5 . 2024 01-24 16.4 2023 - 12.28 14.5 2023 - 12.28 14.5 2024 - 12.48 14.58 14</td><td>1           9.47           1           9.47           1           1.10           1           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.29           1.20           1.20           1.21           1.22           1.23           1.29           1.20           1.21           1.22           1.23           1.24           1.25           1.25           1.20           1.20           1.21           1.22           1.23           1.24           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25      <t< td=""><td></td></t<></td></t<>			中始进行名 果、、 査看 2024-01-24 16:58.40 2024-01-24 16:58.40 2024-01-24 16:58.40 2024-01-26 16:10:21 2023-12-28 13.47:35 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2023-12-28 13.47:35 2024-01-26 16:10:21 2024-01-26 16:10 2024-01-26 16:10 2024-01	ES . 13 H 4 5 . 2024 01-24 16.4 2023 - 12.28 14.5 2023 - 12.28 14.5 2024 - 12.48 14.58 14	1           9.47           1           9.47           1           1.10           1           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.28           1.29           1.20           1.20           1.21           1.22           1.23           1.29           1.20           1.21           1.22           1.23           1.24           1.25           1.25           1.20           1.20           1.21           1.22           1.23           1.24           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25           1.25 <t< td=""><td></td></t<>	
Internet       Internet <th< td=""><td>3. 4.</td><td>日田恵度 配置完 変产年 (12:46.4 12</td><td></td><td><ul> <li>快速</li> <li>快速</li> <li>広击</li> <li>(4)</li> <li>(4)</li></ul></td><td>超快速         R存并执行         戊后点击/         戊后点击/         10         東京         11         東京         12         13         14         15         15         16         16         17         18         18         19         19         10         10         11         11         12         12         14         15         16         16         17</td><td>行" 按钮 任务右侧 20 20 20 20 20 20 20 20 20 20 20 20 20</td><td></td><td>中始进行名 果", 査看 2024-01-24 16:58-00 2024-01-24 16:58-00 2023-12-28 13.47.35 2023-12-28 13.47.35 日本部別次产庫 5378249</td><td></td><td><ul> <li>長, 扫</li> <li>9.47</li>     &lt;</ul></td><td></td></th<>	3. 4.	日田恵度 配置完 変产年 (12:46.4 12		<ul> <li>快速</li> <li>快速</li> <li>広击</li> <li>(4)</li> <li>(4)</li></ul>	超快速         R存并执行         戊后点击/         戊后点击/         10         東京         11         東京         12         13         14         15         15         16         16         17         18         18         19         19         10         10         11         11         12         12         14         15         16         16         17	行" 按钮 任务右侧 20 20 20 20 20 20 20 20 20 20 20 20 20		中始进行名 果", 査看 2024-01-24 16:58-00 2024-01-24 16:58-00 2023-12-28 13.47.35 2023-12-28 13.47.35 日本部別次产庫 5378249		<ul> <li>長, 扫</li> <li>9.47</li>     &lt;</ul>	
If SHE IN	3. 4.	田田 一 一 一 一 一 一 一 一 一 一 一 一 二 二 一 二 二 二 二 二 二 二 二 二 二 二 二 二				行" 按名 任务右() 20 20 20 20 20 20 20 20 20 20 20 20 20		中始进行名 果、、	ESS.	<ul> <li>長、白</li> <li>9.47</li> <l< td=""><td>描结果支持 ■ EXE</td></l<></ul>	描结果支持 ■ EXE
Instrume       Instrum       Instrum       Instrum       In	3. 4.	打研速度 配置: な子子体 次子・体 ・ 「あた」 ・ 「」 ・ 」 ・ 」 ・ 」 ・ 」 ・ 」 ・ 」 ・ 」 ・				行" 按名 任务右() 2 30 30 30 30 30 30 30 30 30 30 30 30 30	I, III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	中 始 送行 名  ス ・ バーモーン  、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	日本の111111111111111111111111111111111111	<ul> <li>人、日</li> <li>ターイ</li> <li>ターイ</li> <li>ターイ</li> <li>ターイ</li> <li>ス</li> <li>ス</li></ul>	
	3. 4.	日前恵度				行" 按名 任务右() 500 100 100 100 100 100 100 100 100 100	I, III III IIIIIIIIIIIIIIIIIIIIIIIIIII	中始: 进行 名 果 、 査希 2224 01-24 15.58 40 2224 01-24 15.58 40 2224 01-25 15 47 23 2223 - 12 28 13.47 23 223 - 12 28 13.47 23 224 - 13 28 13 224 - 13 28 13		<ul> <li>↓</li> <li>↓</li></ul>	

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 场景说明一扫描信息

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。

任务类型	资产发现一子域名猜解
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

	1. 使用 use	r 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
	* 域名	baldu.com         支持編入指式.
		example.com example.cn
		example.com.cn
		參个用英文這号或與行分割 
操作步骤		
	域名爆破字典	子域名爆破字典 > 模板配置
	域名并发数	5 ^ 范围: (1-10)
	单域名并发线程数	100 个 范围: (1-500)
	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 应用资产	生: 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 "库。
备注说明	资产发现任务 1.【系统首页	→发起方法有两种: 】>【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 场景说明一待扫主机信息

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。

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	目标IP: 192.168.0.66       交換机         単一       交換机
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

	1.	使用	user 账户或者 supera		登录紫光漏洞	扫描系统;		
	2.	<b>*</b> 在	【扫描管理】>【系统打	∃描】页面乁	、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	<b>◎数如下</b> :				
	编辑	目任务						
		•任务名称	192.168.0.66	12 / 128				
		描述		0/1024				
		目标	<b>手动输入IP</b> 手动输入域名 从网络资产库中选择 从文	4导入				
			192.168.0.66	IP示 192.1 8.2.0 e80;;	il: 68.2.1, 192.168.2.2, 192.168.2.1 24, 192.166.2.*, fe80::20c:29ff.fe 20c:29ff.fe9f:b7f1-fe80::20c:29ff.fe	-255, 192.168.2.1-192.168 9f:b7fe/126,fe80::20c:29ff:fi e9f:b7few	2.255, 192.16 9f:b7f1-b7ff, f	
				4				
操作步骤		任务优先级	默认	~				
		扫描节点	auto	✓ Ø aut	0表示自动负载均衡,将扫描任务下	下发到最优的扫描节点。单析	部署时下发到本机。	
		执行万式参数模板	手动 默认禮板(TCP Connect扫描常用籍简端口)	~~ 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	京記書			
			基础选项				高级道	与项
	3.	*配量	置任务扫描参数完成后	点击"保存	并执行"按钮	沮,即可开	始扫描任务	۰ م
	4.	查看 查看	结果:扫描完成后点击 扫描任务结果信息。	テ【扫描历史	2】页面,选打	译扫描任务	行,任务右	ī侧的 "结果",
	5.	生成	报表: 扫描完成后点:	テ【扫描历史	」页面,选	择扫描任务	;行,任务右	ī侧的 "报表",
		跳转	到报表管理生成系统排	3描报表页面	可,生成报表	成功后点	击下载即可。	)
	系 1	充扫描 (系统	插任务发起方法有三种: ;首页】>【快速入口】>	【系统扫描】	1			
其它	2.	【扫描	管理】、【系统扫描】、		•			
				新建				
	3.通	f 过资	产库直接对资产发起系	新建 统扫描任务				
	3.通 1 加	1 1 1 日 二 日 二 四 万 二 二 二 二 二 二 二 一 一 う 二 二 一 う 二 二 う 二 の う 二 の う 二 の う 二 の う 二 の う 二 の う 二 の う 二 の う 二 の う 二 の う 二 の コ 二 の つ 二 の つ 二 の コ 四 つ 二 の つ	产库直接对资产发起系	新建 统扫描任务 	"跳讨主机方	☑活检测";	先项	
	3.通 1.如	道过资 ————————————————————————————————————	产库直接对资产发起系 描目标是禁 ping 的主机	新建 统扫描任务 	"跳过主机存	Z活检测";	先项。	
备注说明	3.通 1.如 2.拒	道过资 可果扫 日描目	产库直接对资产发起系 描目标是禁 ping 的主机 标支持网段、支持 IPV	新建 统扫描任务 ., 需要开启 4、IPV6	"跳过主机存	☑活检测"i	先项。	

# 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 场景说明一待扫主机信息

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。

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	■标IP: 192.168.0.66 ■ ■ ■
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> <li>使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统;</li> <li>*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>*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>

	1		
	编	籍任务	
		*任务名称	<b>192.168.0.66 1</b> 2/128
		描述	0/1024
		目标	手动输入口 手动输入域名 从网络资产库中选择 从文件导入
			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, 192.16
			8.2.0/24, 192.168.2.*, 1680-20c-29ff.1e9ft.b7fe126,1e80::20c:29ff.1e9ft.b7f1-b7ff, 1 e80::20c:29ff.1e9ft.b7f1-1e80::20c:29ff.1e9ft.b7few
		任务优先级	
		扫描节点	auto v 🔮 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。
		执行方式	手动 >
		参数模板	繁认模板(TCP Connect扫描常用错简)) v 模板配置
			基礎決頭 高級洗頭
	4.	*在住	£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
		使证明	1002 1402 1402 1002
		发速	(1)時間 <p< th=""></p<>
		登录	主印扫描 💽
		登录	代任務様 「rod@192.166.0.66(ush:22) × ・
			Adulta C
			<u></u> ±−#
			ROH 045971194/5 0459
	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.	査看 査看	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", 扫描任务结果信息。
	7.	生成 跳转	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", 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。
	系	充扫描	任务发起方法有三种:
条注说明	1.	【系统	首贞】>【快速入口】>【系统扫描】
ᅖᅚᅭᄢᄭ	2.	【扫描	管理】>【系统扫描】>新建
	3.通	通过资	产库直接对资产发起系统扫描任务

# 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。

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

表 3-1 场景说明一待扫网站信息

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。



	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:
		* 任务名称 Intp://testphp.vulnweb.com/ 27 / 128 描述 0 / 1624_
操作步骤		Fise 小山(本) 从州省設置「第二十四法 从文件与入     IP所研:     IP所研:     IP所研:     IPの研研:     IPの研研:     IPの研研:     IPの研研:     IPの研研:     IPの研研:     IPの研研:     IPの研研研研研研研研研研研研研研研研研研研研研研研研研研研研研研研研研
		任务代先規     部は、        日面市倉     auto     ●       財石方式     手造
	4.	••••••     •••••     ••••     ••••     ••••     •••     •••     •••     •••     •••     •••     •••     •••     •••     ••     ••••     ••••     ••••     ••••     ••••     ••••     ••••     ••••
	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。
	应 1.	用扫描任务发起方法有三种: 【系统首页】>【快速入口】>【应用扫描】
备注说明	2.	【扫描管理】>【应用扫描】>新建
	3.ì	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。

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

表 4-1 场景说明一待扫目标信息

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。

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	目标: 192.168.0.7       交換机         ご       交換机

预置条件	扫描	i器与 扫Ⅱ	i目标 IP 网络可达, P 拉黑,否则扫不到	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 漏洞信息不全。
	1. 2.	使用 <b>*</b> 在   用系	user 账户或者 su 【扫描管理】>【数 统默认参数模板,	peradmin 账户 [据库扫描】页] 参考参数如下:	登录紫光漏洞扫描系统; 面下,点击"新建",进入任务新建页面,建议使
	*	任务名称	(時代) 次元本(株売) 以二(4号)	2 / 128 0 / 1024 <sub>/</sub>	
			192.168.0.7		<b>ド示例:</b> 192.168.2.1,192.168.2.2,192.168.2.1-255,192.168.2.1-192.168.2.255,192.168.2. 024,192.168.2.*,1680.:20c:29ff.fe9f.b7fev126,fe80::20c:29ff.fe9f.b7f1-b7ff,fe80:: 20c:29ff.fe9f.b7f1-fe80::20c:29ff.fe9f.b7few 多个用意义语号成编行分割
操作步骤	Æ	务优先级 扫描节点 执行方式	默认 auto 手动	~	● auto表示自动负载均衡,将扫描任务下发到最优的扫描节点。单机器署时下发到本机。
	[	参数模板	默认模板	~	模板配置
	3. 4.	*配置 查看 查看	1任务扫描参数完) 结果:扫描完成后 扫描任务结果信息	或后点击"保存 点击【扫描历9 。	并执行"按钮,即可开始扫描任务。 2】页面,选择扫描任务行,任务右侧的"结果",
	5.	生成 跳转	报表:扫描完成后 到报表管理生成数	点击【扫描历9 [据库扫描报表]	史】页面,选择扫描任务行,任务右侧的"报表", 页面,生成报表成功后点击下载即可。
其它	数据 1.【	3库扫 系统	描任务发起方法有 首页】>【快速入□	三种: 1】>【数据库扫	描】
	2.【 3.通	扫描	管理】>【数据库打 产库直接对资产发;	日描】>新建 起数据库扫描任:	务
备注说明	如果	見扫描	目标是禁 ping 的主	至机,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 场景说明一待扫目标信息

扫描目标数据库主机 IP	192. 168. 0. 7
数据库类型	Mysq1
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。

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	■标: 192.168.0.7
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】 田白夕 <u>家</u> 研	>【数据库资产】页面新建	数据库资产,录入 IP 就后保存	、数据库类型、端口、
	用尸名、密码、 	开后"扒打岔陆扫抽"远坝	。	
	数据库资产编辑页			
	* 名称 Mysql	5/128 * IP 192.10	8.0.7	11764
	描述			0 / 1024
	数据库关型 Mysql	→ 靖口 3306 -	用户名 root	4 / 128
	密码	Ø Database	0/128	
	登录验证			
	执行登录扫描 <b>○</b> 伊启后扫描时会使用上面输入的	助账号信息登录到数据库执行扫描		
	<ol> <li>*在【扫描管理】 目标里,选择" 参数模板,参考</li> <li>*任务任務 Mysql</li> </ol>	>【数据库扫描】页面下, 资产库",然后勾选上一步包 参数如下:	点击"新建",进入住 J建的数据库资产,参	£务新建页面,在扫描 診数模板使用系统默认
	目标 手动输入 资产库(推荐) 从文件导入			
	资产名			+ 新雄 C ⑧
	■ 资产名	IP 数据库类型 192.168.0.7 Mvsd	端口 3306	操作
	Mysql	192.168.0.4 Mysql	3306	编辑
	66	192.168.0.66 未知	0	婉雜
			共3条 <	1 > 前往 1 页 10余/页 >
	任务优先级默认	✓ ● auto表示自示表的影響機均能将有許不可能。●	发到最优的扫描节点,单机就靠时下没到本机。	
	执行方式 手动	<ul> <li>Onesolvenesolsevenes</li> </ul>	ACCOMMONANTALISE INTERNA I PENNERIPERINA I CARLEY-PENNA	
	参数模板 默认模板	<		
	<ol> <li>4. *配置任务扫描参</li> <li>5. 查看结果: 扫描 查看扫描任务结</li> </ol>	参数完成后点击"保存并执行 完成后点击【扫描历史】页ī 课信息。	亏"按钮,即可开始打 面,选择扫描任务行,	日描任务。 任务右侧的"结果",
	<ol> <li>6. 生成报表:扫描 跳转到报表管理</li> </ol>	完成后点击【扫描历史】页百 生成数据库扫描任务报表页	面,选择扫描任务行, 面,生成报表成功后	任务右侧的"报表", 点击下载即可。
	数据库扫描任务发起 1.【系统首页】>【特	方法有三种: ē速入口】>【数据库扫描】		
其它	2.【扫描管理】>【数	女据库扫描】>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 pi	ng 的主机,需要开启"跳过言	 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。

 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

表 5-1 场景说明一待扫目标信息

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。

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	目标: 192.168.0.66       交換机
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。

	网络波士德德东								
	Matt The address M								
	* 名称 服务	10 80			3/128 * IP	192.168.0.66			
	/M4622								
	设备编号		0/1	28 位	置 请选择 审 0 ^		/ 标签 法择组织架构	请选择	
	所属业务系统		0 / 1	28 网络区	城请选择		· 负责人		
	联系方式		07	64 <b>#</b>	箱	0/6	4		
	登录凭证选择 请选择	泽				Q目标自动识别			
		x	✓ Centos配置规范			~			
	配置规范 Linux								
3 步骤	▲##₹ ( @) ★在 ( 资) 协议、端 考参数如 编辑	产管理】 行口、用 1下: <sup>洗证</sup>	┃ >【凭证管 户名、密码	『理】〕 等信息	页面下,点i 』,然后可以	击"新建", 人点击登陆朝 〉	, 进入新 金证测ì	所增凭证〕 式是否能	页面,输 <i>入</i> 够登陆成现
3 步骤	▲##₩ (Ima *在【资) 协议、端 考参数如 编辑	产管理】 計口、用 1下: เK证	】>【凭证管 户名、密码	『理】〕 等信息	页面下,点i 』,然后可以	击"新建", 人点击登陆羽	→ 进入新 金证测ì	所增凭证〕 式是否能	瓦面,输 <i>入</i> 够登陆成功
3 步骤	<ul> <li>★在【资〕</li> <li>协议、端</li> <li>考参数如</li> </ul>	mit 产管理】 計口、用 1下: i洗证 - IP - biǔ	】>【凭证管 户名、密码 <sup>192.168.0.59</sup>	『理】〕 等信息	页面下,点i 【,然后可以	击"新建", 人点击登陆羽 〉	进入 进入 金证测 i	所增凭证] 武是否能	瓦面,输 <i>入</i> 够登陆成功
3	<ul> <li>▲霍【资〕</li> <li>◆在【资〕</li> <li>协议、端</li> <li>考参数如</li> </ul>	mii 产管理】 計口、用 ]下: : : : : : : : : : : : : : : : : : :	】>【凭证管 户名、密码 <sup>192.168.0.59</sup> smb 445	「理】〕 等信息	页面下,点i 【,然后可以	击"新建", 人点击登陆羽 〉	进入 进入 金证测 i	所增凭证] 武是否能	瓦面,输 <i>入</i> 够登陆成功
3	▲### ( uno	mi 产管理) 計口、用 計下: 読证 ・ 部议 ・ 調口 ・ 明 ・ 第 ・ 第 ・ 第 ・ ・ ・ 第 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	】>【凭证管 户名、密码 <sup>192.168.0.59</sup> smb 445	「理】〕 等信息	页面下,点i 【,然后可以	ま"新建",	进入新 金证测i	所增凭证〕 式是否能	瓦面,输 <i>入</i> 够登陆成功
3	▲##₩ (шо ★在【资) 协议、端 考参数如 编辑	mii 产管理) 計口、用 引下: 読证 * IP * 助议 ・ 端口 * 用户名 密码	■ >【凭证管 户名、密码 <sup>192,168,0,59</sup> smb 445 <sup>•</sup> TL	"理】〕 等信息	页面下,点i 【,然后可以	ま"新建",	进入 金证测 ·	所增凭证〕 式是否能	瓦面,输 <i>入</i> 够登陆成功
3	▲### ( uno *在【资) 协议、端 考参数如 编辑	mit 产管理) 「「「、用 「下: 読证 ・IP ・助议 ・端口 ・開中名 密码 nable 用中名	■ > 【凭证管 户名、密码 <sup>192,168,0.59</sup> smb 445 <sup>•</sup> TL	"理】〕 等信息	页面下,点i 』,然后可以	a:mee 击"新建", 人点击登陆到 → 2/128 ∞ 0/128	进入 金证测i	<b>所增凭证</b> 〕 式是否能	页面,输 <i>入</i> 够登陆成功
3	▲### (mo *在【资) 协议、端 考参数如 编辑	mit 产管理) 計口、用 1下: i洗证 ・IP ・协议 ・調口 ・用户名 密码 nable 用户名 enable 密码	■ >【凭证管 户名、密码 192.168.0.59 smb 445 <del>、</del> TL TL	「理】〕「等信息	页面下,点i 』,然后可以	± "新建", 人点击登陆朝 2/128 @ 0/128	进入 金证测i	所增凭证] 武是否能	页面,输 <i>入</i> 够登陆成功
步骤	▲### [ uno *在【资方 协议、端 考参数如 编辑	mit 产管理) 対口、用 す下: 詳证 ・IP ・抽议 ・調口 ・開户名 密码 enable 周户名 enable 密码 WebUrl	■ >【凭证管 户名、密码 192.168.0.59 smb 445 <sup>•</sup> TL TL 	7理】〕	页面下,点i 3,然后可以	anness 击"新建", 人点击登陆马 ~ 2/128 ◎ 0/128 0/128	进入 金证测 ( _ ] ] ]	所增凭证〕 式是否能	页面,输 <i>入</i> 够登陆成3

	• 任务名	192.168.0.66 14 / 128		
	描述			
	a Stervice	0/1024		
	- 30/**			
				~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
		<ul> <li>资产名</li> </ul>	IP	擬作
		windows 虚权机	192.168.200.128	编辑
		Esxi	192.168.0.106	頭相
	l	92.168.0.66	192.168.0.66	编辑
		92.168.0.59	192.168.0.59	编辑
			<del>,</del>	4条 < 1 > 前往 1 页 10余/页 >
		登录凭证 root@192.168.0.66(ssh:22) × ~		
	* 模板选择	默认 ~ 機振	配憲	
	采集方式	<ul> <li>本地采集(在线)</li> <li>即本采集(商法)</li> <li>第3時采集 ()</li> </ul>		
	一种后下于	"但专并抽答" 即可工场行尽		
	※ 加 从 田	「休什开执门 ,即可开始任务	°	
	5 本手は田		両面 洪塚扫世代タダ	- 仁夕士间的"姑耳"
		: 扫细元成府从市【扫细加文】	一贝国,见伴归捆任分1.	」,在另右侧的 结米,
	査看扫描	任务结果信息。		
	6. 生成报表	: 扫描完成后点击【扫描历史】	贝面,选择扫描任务作	」,任务石侧的"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。
	基线核查任务	发起方法有两种:		
甘它	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		
7 1 1 2 2 2 7 3				

## 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 场景说明一待扫目标信息

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。

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	目标: windows10 回路不通 の 銘不通
预置条件	目标主机支持运行 windows 离线检查脚本
操作步骤	<ul> <li>*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> <li>*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> </ul>

				4/128			
	* 任务	名 离线检查		41120			
	描	*					
				0 / 1024			
	* 资	产网络资产数据	国库资产				
		20100-02		<b>6</b> 30			C®
		жо н					
		<ul> <li>一 资产字</li> </ul>			IP	操作	
		windo	vs虚拟机		192.168.200.128	编辑	
		192 10	807		192 168 0 7	總續	
		- 102.1	9.9.1		102.100.0.1		
		Esxi			192.168.0.106	编辑	
		192.10	8.0.66		192.168.0.66	编辑	
		192.10	8.0.59		192.168.0.59	编辑	
						共5 ☆ < 1 > 前往 1 页 10 %	<i>и</i> д ∨
		登录凭证 请	选择	~			
	• 模板选	译 默认		~ 模板配置			
	采集方	式 () 本地妥集(在	維) 🟮 脚本平便(斎姓) 🔿 跳鉄平集 👩				
				_			
	松に」	=+ "/	日友光神仁" 印言	「今代にない	17=1		
	※ つん	रम १	朱仔开现1丁,即只	元风仕分型	J廷。		
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 M	记置规
	± 22 -	r 8	的几名里卡丁日本	비지미나는		0 7、1、二/二/一 明十月4	டி அட
	Ϋ́Ŀ _	L丹,	<b>然</b> 后符脚半上共招	「贝到日你」	EML (192.168.	0. () 上运行, 脚 平 名 核	≸刃:
	Windo	wsRvsA	gent exe.				
	" IIIGO	"DD 1 DI	Sent. exes				
			· · · · · · · · · · · · · · · · · · ·				
5.	<b>*</b> 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,等待半分锋	中后会
5.	<b>∗</b> 运行	脚本工	具:双击运行脚本	工具,然后	在弹出页面中点	<b>袁击开始检查,等待半分</b> 锋	中后会
5.	<b>*</b> 运行 提示核	脚本工 社在完成	具:双击运行脚本 戏,然后点击导出;	工具,然后 结果。	在弹出页面中点	京击开始检查,等待半分转	中后会
5.	<b>*</b> 运行 提示林	脚本工 社在完成	具:双击运行脚本 戏,然后点击导出约	工具,然后 结果。	在弹出页面中点	京击开始检查,等待半分转	中后会
5.	*运行 提示格	脚本工	具:双击运行脚本 成,然后点击导出统	工具,然后 结果。	在弹出页面中点	ā击开始检查,等待半分 <b>转</b>	中后会
5.	*运行 提示格	脚本工 全在完成 1886年1月	具:双击运行脚本 成,然后点击导出统	工具,然后 结果。	在弹出页面中点 - □ ×	ā击开始检查,等待半分转	中后会
5.	*运行 提示材		具:双击运行脚本 成,然后点击导出结	工具,然后 结果。	在弹出页面中点 - □ ×	ā击开始检查,等待半分转	中后会
5.	*运行 提示格 Windows22		具:双击运行脚本 成,然后点击导出结 GMH Window 10 Etterpris	工具,然后 结果。	在弾出页面中点 - □ ×	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 * Windowster #MicEatte #MicEatte #MicEatte #MicEatte #MicEatte		具:双击运行脚本 成,然后点击导出结 GMH Windows 10 Enterpris BalidLabEct17763.1 amd64ffrer.f5_refease.EB975	工具,然后 结果。 LISC 2019 4CurrentVersions 3, CurrentBuild(177	在弾出页面中点 - □ ×	ā击开始检查,等待半分转	中后会
5.	*运行 提示格 <sup>®</sup> Windows22 <sup>®</sup> Win	脚本工 全在完成 公式院61月 世期8 周A2 展作版6 展在5人(6)	具:双击运行脚本 成,然后点击导出 GMM GMM Windows 10 Entrpris BuildLabEx:17763.1 and64frers5_release.180914-14 1197 1197	工具,然后 结果。 + LTSC 2019 4.CurrentVersions.3, CurrentBuild(177	在弹出页面中点 - • ×	ā击开始检查,等待半分转	中后会
5.	*运行 提示格 * Windowsze * Windowsze * Windowsze * Windowsze * Windowsze * Windowsze * Windowsze * Windowsze * Windowsze * *	脚本工 立在完成 於當終を1月 <sup>11算約点</sup> 風中高 繁作系成版本 於音大小約) 電慮大小(6) 系成版金	具:双击运行脚本 成,然后点击导出。 (MM (MM Windows 10 Entry BuildLabEx:17763.1.amd64fre.r5_release.180914-14 12197 1168 C.Windows	工具,然后 结果。	在弾出页面中点 	ā击开始检查,等待半分转	中后会
5.	*运行 提示本 * Windows24 年代里世世 用代里世世 用代里世世 用代里世世	<b>脚本工</b> 全査完成	具:双击运行脚本 成,然后点击导出。	工具,然后 结果。	在弾出页面中点 	ā击开始检查,等待半分转	中后会
5.	*运行 提示相 * Windowstr ************************************	<b>脚本工</b> ななにも13 日本での 日本 日本での 日本での 日本での 日本での 日本での 日本での 日本での 日本での 日本	具:双击运行脚本 <b>战,然后点击导出</b>	工具,然后 结果。 HISC 2019 ACurrentVersion 6.3, CurrentBuild(177 ACurrentVersion 6.3, CurrentBuild(177	在弹出页面中点 ◎	ā击开始检查,等待半分转	中后会
5.	*运行 提示相 *Madawate *Madawate *Madawate *Madawate *Madawate *Madawate ************************************	<b>脚本工</b> <b>社会には 市場に 市場に 市場に 市場に 市場に 市場に 市場に 市場に</b>	具:双击运行脚本 成,然后点击导出。	工具,然后 结果。 ACurrentVersion5.3, CurrentBuild(177 AcurrentVersion5.3, CurrentBuild(177 AcurrentVersion5.3, CurrentBuild(177	在弹出页面中点 ••	意击开始检查,等待半分转	中后会
5.	*运行 提示林 * Windowssiz ##是面明 ###面明 ###面明 #### ##面明 #### ##面明 ##### #### #### ##### ##### ##### #####	<b>脚本工</b>	具:双击运行脚本 成,然后点击导出 (MH GMH GMH Windows 10 Enterpris BuildLabEct17763.1 and64fer:r5_refease.189014.1 12197 1196 C(Window OTO-91592) ADMINE-28282-4 C6-#0.149 OF-90.1492 C4-#0.149 C4-#0.	工具,然后 结果。 atts: 2019 ACurrentVersions.3, CurrentBuild(177 a taze ACurrentVersions.3, CurrentBuild(177 a taze ACurrentVersions.3, CurrentBuild(177 a taze ACurrentVersions.3, CurrentBuild(177	在弾出页面中点	ā击开始检查,等待半分转	中后会
5.	*运行 提示材 * Windowsse #H显示材 #H显示材 #H显示式 #H显示式 #H国 #H国示式 #H国示式 #H国 #H国 #H国 #H国 #H国 #H国 #H国 #H国 #H国 #H国	脚本工 全査完成 になられる13 になった。 ないので、 ななられる13 になった。 ないので、 ななられる13 になった。 ないので、 ななられる13 になった。 ないので、 ななられる13 になった。 ないので、 ななられる13 になった。 ないので、 ないのでで、 ないので、 ないので、 ないので、 ないので、 ないので、 ないので、 ないので、 ないので、 て	具:双击运行脚本 <b>战,然后点击导出</b> (MH GMH GMH GMH BuildLabEct177631.amd64frer.57.effaces.180914-01 12197 1199 C(Window C)GU-3829 ADMINE-32828-4 CRULAP D1BUILAP D1BUILAP D1-SULAP	工具,然后 古果。 出版 2019 ACurrentVersion 6.3, CurrentBuild(177 4, CurrentVersion 6.3, CurrentVersion 6.3, CurrentVersion 6.3, CurrentBuild(177 4, CurrentVersion 6.3, Curren	在弾出页面中点	ā击开始检查,等待半分转	中后会
5.	*运行 提示格 *Madass #Mada	脚本工 立査完長 に は 日本 に 日本 に 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	具:双击运行脚本 <b>拔,然后点击导出</b>	工具,然后 结果。 trsc 2019 4.CurrentVersion6.3, CurrentBuild(177 4. 4.CurrentVersion6.3, CurrentBuild(177 4. 4. 4. 4. 4. 4. 4. 4. 4. 4.	在弹出页面中点 。。	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 *Midowski #482 #482 #482 #488 #488 #488 #488 #488	脚本工 全 査 完 に	具:双击运行脚本 成,然后点击导出。 (MM (Mindows 10 Enterpris BuildLabEx:17763.1 amd64frer.5,release.180914-14 BuildLabEx:17763.1 amd64frer.5,release.180914-14 C(Windows BuildLabEx:17763.1 amd64frer.5,release.180914-14 C(Windows	正具,然后 古果。 はTSC 2019 4.CurrentVersionの6.3, CurrentBuild(177 4.CurrentVersionの6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4.CurrentVersion(6.3, CurrentBuild(177 4	在弾出页面中点 ◎	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 Windowski adda adda adda adda adda adda adda ad	脚本工 位在完成 和本 市場に 市場に 市場に 市場に 市場に 市場に 市場に 市場に	具: 双击运行脚本 发, 然后点击导出。 (MM GMH Windows 10 Enterpris BuildLabEx:1770.1.amd64frer.5_release.180914.14 12197 BuildLabEx:1770.1.amd64frer.5_release.180914.14 C1Windows 01500-05209 C1Windows 01	工具,然后 结果。 4.155.2019 4.CurrentVersion.6.3, CurrentBuild(177 4.CurrentVersion.6.3, CurrentBuild(177 4.Current	在 弹出页面中点	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 3. Windowski 8. Makasa 9. Ma	脚本工 な音にも13 11月に名 第7名にある 第7名にの 第一名にの 第一名にの 第一名にの 第一名 第一名 第一名 第一名 第一名 第一名 第一名 第一名	具:双击运行脚本 成,然后点击导出。 (MM (MM (Mm (Mm (Mm (Mm (Mm (Mm	工具,然后 结果。 	在弹出页面中点 。。	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 *////////////////////////////////////	脚本工	具: 双击运行脚本 发, 然后点击导出。	工具,然后 名果。	在 弹 出 页 面 中 点	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 ***********************************	脚本工 <b>社会に</b>	具: 双击运行脚本 发, 然后点击导出。 GMH CMH Windows 10 Enterprise BuildLabEc17763.1.amd64fre.r5_release.180914.14 12197 BuildLabEc17763.1.amd64fre.r5_release.180914.14 12197 BuildLabEc17763.1.amd64fre.r5_release.180914.14 12197 BuildLabEc17763.1.amd64fre.r5_release.180914.14 CUMindow OK50514525 AMMIN-GEBER CUMING OK5051455 AMMIN-GEBER CUMING OK5051455 AMMIN-GEBER CUMING CUMING OK5051455 AMMIN-GEBER CUMING CUMIN	正具,然后 古果。 は155 2019 4.CurrentVersionら.3, CurrentBuild(177 4.CurrentVersionら.3, CurrentBuild(177 4.CurrentVersion) 4.CurrentVersion 4.Cu	在 弹 出 页 面 中 点	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 2 Windowstr 248度在日 448度 946度日 746度日5 456度日 456度日 456度日 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566度日(148) 566 566 566 566 566 566 566 566 566 56	<b>脚本工</b> 社会完成	具: 双击运行脚本 成, 然后点击导出。	正具,然后 古果。 生15C 2019 4.CurrentVersionら.3.CurrentBuild(177 4.CurrentVersion) 4.CurrentVersion 4.Curren	<b>在弾出页面中点</b> ◎	ā击开始检查,等待半分转	中后会
5.	*运行 提示林 2 Windows22 248至22 248至22 248至22 248至2 248至2 248至2 248至2 248至2 248至2 248至2 248至2 248至2 248至2 248至2	脚本工	具: 双击运行脚本 龙, 然后点击导出。 (MH GMH GMH GMH Windows 10 Entropis BuildubEc17763.1.amd64fer15_refeaer.18091141 12197 1188 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMindows 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS 055518529 ADMIN-25888 CUMMINDOWS CUM	エ具,然后 古果。 はTSC 2019 A CurrentVersion 5.3, CurrentBuild(177 4 4 420 	在 弹 出 页 面 中 点	ā击开始检查,等待半分钟	中后会
5.	*运行 提示林 2 Vindowski 2 Mindowski 2 Mindowski Mindowski Mindowski Mindowski Mindowski Mindowski Mindows	<b>脚本工</b> な 金字に成 中 に 日本 中 日本 日本 中 日本 中 日本 中 日本	具: 双击运行脚本 龙, 然后点击导出。 (MH (MH (MH (MH)) BuildLabEct17763.1 amd64fers52 refeater.189314.41 12197 1100 (C)(Weidow (0550-31925) ADMINI-25883- (C-5-80,137 (C) 905-5-2019 (C) 188224D-18	工具,然后 名果。 名王子2019 4.4CurrentVersion6.3, CurrentBuild(177 4.4CurrentVersion6.3, CurrentBuild(177		ā击开始检查,等待半分钟	中后会
ō.	*运行 提示林 5.4000000000000000000000000000000000000	<b>脚本工</b> な 在 完成 に 本 に は 市 系 系 系 本 た に た 、 、 た に 、 、 、 、 、 、 、 、 、	具: 双击运行脚本 龙, 然后点击导出。 (Mi GMi GMi BuildubEc17763.1am64ffers75_refeace.189314.1 12197 1196 CC/Window 0550-91555 ADMIN-世界電子 CC-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C-#30,149 Dotto-1501度可愛用。 (C- State	エ具,然后 古果。 はTSC 2019 4.4CurrentVersionの5.3, CurrentBuild(177 4.4CurrentVersionの5.3, CurrentBuild(177 4.4CurrentVersion 5.3, CurrentBuild(177 4.4CurrentVe		ā击开始检查,等待半分转	中后会
5.	*运行 提示林 3.48年間3 9658 7.648 7.6487 7.6487.	<b>脚本工</b> ななたまま 一 かなたいの 本の時代 市の時代 の時代いの 本の時代 市の時代 の時代いの 本の時代 一 の時代いの 一 、 、 、 、 、 、 、 、 、	具: 双击运行脚本 支, 然后点击导出 。 。 。 。 。 。 。 。 。 。 。 。 。	エ具,然后 古果。 は155 2019 4. CurrentVersionの5.3, CurrentBuild(177 4. CurrentVersionの5.3, CurrentBuild(177 4. CurrentVersionの5.3, CurrentBuild(177 4. CurrentVersionの5.3, CurrentBuild(177 4. CurrentVersionの5.3, CurrentBuild(177 5. CurrentVersionの5.3, CurrentBuild(177 5. CurrentVersionの5.3, CurrentBuild(177 5. CurrentVersionの5.3, CurrentBuild(177 5. CurrentVersion 5.3, CurrentBuild(177 5. CurrentVe		(古井山市)	中后会
ō.	*运行 提示林 3. Windowski 2. Windowski Windowski 2. Windowski 2. Windowski 2. Windowski Millish Vindowski Windowski Windowski Windowski Windowski Windowski Windowski		具:双击运行脚本 成,然后点击导出。 (MH (Mindows 10 Enterpris BuildLabEx:1708.1.amd64frer.5.release.180914.14 12197 BuildLabEx:1708.1.amd64frer.5.release.180914.14 12197 C(Windows 007000/08529 ADMINE-EBER 01-501.47 01-501.47 01-501.47 (2) (2) (2) (2) (2) (2) (2) (2)	工具,然后 结果。 	在弾出页面中点	ā击开始检查,等待半分转 可建的离线检查任务,点 <del>ī</del>	中后会
5.			具:双击运行脚本 成,然后点击导出。 (MM (Md (Md (Md (Md (Md (Md (Md	工具,然后 结果。 	在弾出页面中点	電击开始检查,等待半分转 可建的离线检查任务,点面	中后会
		脚本工 社 生	具:双击运行脚本 成,然后点击导出。 (MH () () () () () () () () () ()	工具,然后 结果。 	在弾出页面中点 ◎ ◎ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	電击开始检查,等待半分转 可建的离线检查任务,点音 查结果文件即可。	中后会
<b>5</b> .	*运行 提示林 */提示林 */###8 ###8 ###8 ###8 ###8 ###8 ###8 ##	脚本工 全	具:双击运行脚本 龙,然后点击导出。 (MH ( ) (MH ( ) (MH ( ) (MH ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	工具,然后 结果。 *1552019 4.CurrentVersions.3.CurrentBuild(177 4.CurrentVersions.3.CurrentB	在弾出页面中点 ③ ③ 〕页面,找到创 上传第 5 步的检	電击开始检查,等待半分转 可建的离线检查任务,点音 查结果文件即可。	中后会
			具:双击运行脚本 成,然后点击导出。 (MH (C)	工具,然后 结果。 	在弾出页面中点	武击开始检查,等待半分钟 可建的离线检查任务,点击 查结果文件即可。 行,任务右侧的"结果".	中 后 会 街 石 倒 看
ō. ;.			具:双击运行脚本 成,然后点击导出。 (MH Common Com	工具,然后 结果。 *1552019 4.4CurrentVersion 5.3. CurrentBuild(177 ***********************************	在弾出页面中点 。 、 、 、 、 、 、 、 、 、 、 、 、 、	武击开始检查,等待半分转 可建的离线检查任务,点击 查结果文件即可。 行,任务右侧的"结果",	中后会 右侧 查看
5. 3. 7.			具:双击运行脚本 成,然后点击导出。 (MH (MH (MH (MH (MH (MH (MH (MH	工具,然后 结果。 * 155 2019 4 ACurrentVersion 5.3. CurrentBuild(177 * 4 * 4 * 4 * 4 * 4 * 4 * 4 * 4 * 4 * 4	在弾出页面中点 。 。 〕 页面,找到创 上传第5步的检 选择扫描任务:	電击开始检查,等待半分转 可建的离线检查任务,点面 查结果文件即可。 行,任务右侧的"结果",	中后会 石 石 香
5. 6. 7.			具:双击运行脚本 成,然后点击导出。 (MH (MH (MH (MH (MH (MH (MH (MH	工具,然后 结果。 4.155 2019 4.4CurrentVersion 5.3, CurrentBuild(177 4.4CurrentVersion 5.4CurrentVersion 5.4CurrentVersion 5.4CurrentBuild(177 4.4CurrentVersion 5.4CurrentBu	在弾出页面中点 。 。 〕 页面,找到创 上传第5步的检 选择扫描任务:	基于始检查,等待半分转 可建的离线检查任务,点面 查结果文件即可。 行,任务右侧的"结果",	中后会 石 石 個
<ol> <li>6.</li> <li>7.</li> <li>8.</li> </ol>			具:双击运行脚本 成,然后点击导出。 (MH (MH (MH (MH (MH (MH (MH (MH	工具,然后 结果。 *155 2019 4.CurrentVersion 5.3, CurrentBuild(177 4.CurrentVersion 5.3, CurrentBuild(177 4.CurrentVersion 5.3, CurrentBuild(177 5. **** **** ************************	在弾出页面中点	電开始检查,等待半分转 可建的离线检查任务,点面 查结果文件即可。 行,任务右侧的"结果", 面物 "报表", 跳转到料	中后会 右 査 覆
<ol> <li>6.</li> <li>7.</li> <li>8.</li> </ol>	*运行根 *运示格 */运示格 *////////////////////////////////////		具:双击运行脚本 成,然后点击导出。 (MH)	工具,然后 结果。 155 2019 4.CurrentVersion 5.3. CurrentBuild(177 4.CurrentVersion 5.3. CurrentBuild(1	在弾出页面中点	高击开始检查,等待半分转 可建的离线检查任务,点司 查结果文件即可。 行,任务右侧的"结果", 右侧的"报表",跳转到打	中后会 石 石 個 五 香 表 管
<b>6.</b> <b>7.</b> 8.	*       提出         #       基         #       基         #       基         #       基         #       基         #       基         #       # <td< td=""><td>脚查</td><td>具:双击运行脚本 成,然后点击导出线 (Mit))))))))))))))))))))))))))))))))))))</td><td>工具,然后 结果。 1155 2019 4.CurrentVersion 6.3. CurrentBuild(17 4.CurrentVersion 6.3. CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.Curren</td><td>在弾出页面中点 一 * - * - * - * - * - * - * - * -</td><td>高击开始检查,等待半分转 可建的离线检查任务,点音 查结果文件即可。 行,任务右侧的"结果", 右侧的"报表",跳转到打 即可。</td><td>中 后 会 石 て て て て て て て て て て て て て て て て の で の し て の し て の し て の し て の し て の し の の の の</td></td<>	脚查	具:双击运行脚本 成,然后点击导出线 (Mit))))))))))))))))))))))))))))))))))))	工具,然后 结果。 1155 2019 4.CurrentVersion 6.3. CurrentBuild(17 4.CurrentVersion 6.3. CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.CurrentBuild(17 4.Curren	在弾出页面中点 一 * - * - * - * - * - * - * - * -	高击开始检查,等待半分转 可建的离线检查任务,点音 查结果文件即可。 行,任务右侧的"结果", 右侧的"报表",跳转到打 即可。	中 后 会 石 て て て て て て て て て て て て て て て て の で の し て の し て の し て の し て の し て の し の の の の

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。

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

表 6-1 场景说明一待扫目标信息

在线爆破指的是通过在线方式对目标主机讲行字典猜解。

任务类型	口令猜解一在线爆破
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	目标: windows10 夏東
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	<ol> <li>使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统;</li> <li>*在【扫描管理】&gt;【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"。</li> </ol>
	5. 直有结果: 元成冶点山【汕油历文】 火山,远洋汕油社分门,社分石 网的 结果 ,直 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 场景说明一待扫目标信息

扫描目标数据库主机 IP	192. 168. 0. 66
目标操作系统类型	Cent0S7
爆破类型	Linux
用户名	root
密码	T1@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。。

任务类型	口令猜解一离线 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。

	1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统;
	<ol> <li>*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> </ol>
操作步骤	<ul> <li>3. 在新建页面下发点击新建, 在弾出框中输入 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。</li> </ul>
	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。
바순	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】
<u>央</u> 匕 	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	场意况明一符扫目标信息
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。



预置条件	apk 包未加密加壳,大小不超过 300Mb		
1. 使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统;			
	<ol> <li>*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。</li> </ol>		
操作步骤	新建任务 × 应用类型 ● Android ○ IOS * 应用上传 + 将文件拖到此处 威 点由上传		
	Dase apk 上传进度 0%		
	<ol> <li>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。</li> </ol>		
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 场景说明一待扫目标信息

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。

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	目标: centosiatest 正映 で 換机		
预置条件	扫描器与目标网络可达;扫描器需配置好 DNS。		

	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。
		新增任务
操作步骤		*任务名 公共镜像 4/128
		<ul> <li>* 扫描目标 ● (像)扫描 ● 仓库扫描</li> <li>仓库送型 ● 公共仓库 ● 私有仓库</li> </ul>
		镇像标签 <u>centos latest</u>
		取消 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。
	镜 <sup>/</sup>	像扫描任务发起方法有两种: 【系统首页】、【快速λ口】、【镜像扫描】
<u> </u>	1. 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 场景说明一待扫目标信息

仓库类型	Haobor 仓库		
版本	V2		

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

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	目标: Haobor		
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	<ol> <li>使用 user 账户或者 superadmin 账户登录紫光漏洞扫描系统;</li> <li>*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>		
	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		