UNIS XScan-G 系列漏洞扫描系统 典型配置举例

Copyright © 2020 紫光恒越技术有限公司及其许可者版权所有,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。本文档中的信息可能变动,恕不另行通知。

目 录
-----

1 简介1
2 配置前提
3 主机扫描配置举例1
3.1 组网需求1
3.2 配置步骤2
3.3 验证配置4
4 主机弱口令扫描配置举例5
4.1 组网需求5
4.2 配置步骤6
<b>4.3</b> 验证配置8
5 WEB cookie 录制扫描配置举例8
5.1 组网需求8
5.2 配置步骤9
5.3 验证配置11
6 WEB 手动爬行扫描配置举例12
6.1 组网需求12
6.2 配置步骤13
6.3 验证配置15
7 WEB 被动爬行扫描配置举例16
7.1 组网需求16
7.2 配置步骤16
7.3 验证配置19
8数据库扫描配置举例20
8.1 组网需求20
8.2 配置步骤20
8.3 验证配置23

# 1 简介

本文档介绍 UNIS 漏洞扫描系统典型配置举例

# 2 配置前提

本文档不严格与具体硬件版本对应,如果使用过程中与产品实际情况有差异,请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证,配置前设备的所有参数均采用出厂时的缺 省配置。如果您已经对设备进行了配置,为了保证配置效果,请确认现有配置和以下举例中的配置 不冲突。

# 3 主机扫描配置举例

3.1 组网需求

图1 配置组网图



**UNIS** 漏洞扫描系统属于网络旁路设备,可以部署在核心交换机上(原则上可达即可扫),并对应不同的网络分配不同的网口地址,定期地对网络中多个不同的网段的主机进行全面、深入的检测,同时生成相应的漏洞解决方案,用户根据这些解决方案来对目标系统和应用做相应的加固和防护,及时将网络的安全风险降到最低。

# 3.2 配置步骤

通过【扫描】>【新增任务】创建一个主机扫描任务。

图2 新建任务

扫描		呆存 返回
<ul> <li>         · 基本配置         ·         ·         ·</li></ul>	<b>扫描 &gt; 任务编辑</b>	
量本参数 主机扫描	任務名称:     [王原太郎(中の小学校 / 太昭和) 東田江名文を()、72~~)     太阳(中の / 上原太郎(中の小学校 / 太昭和) 東田江名文を()、72~~)	
☆ ±013曲参数 ∧ 常規参数		
靖□参数 破解参数	• 扫描典型:  • 注析扫描 () Web扫描 () 数据率扫描	
☑ 主机通知参数 ∧ 扫描通知	• 戌先版: ○ 焉 ⑧ 中 ○ 低	
wsus通知	<ul> <li>         • 排行计划: 立即执行</li> <li>         · 任約的执行计划:可选择任务的执行时间与周期等     </li> </ul>	
	最否开启: 🗋 自动原始到资产	
	是否开启: ○ 发送结果到邮桶 ○ 上传给果到FTP	
	授業成型: htm/授業 ✓	
	And an and a second sec	

基本参数,配置任务名称,其他参数默认。

配置路径:【扫描】>【新增任务】>【基本配置】>【基本参数】。

图3 配置基本参数

0
~
~

主机扫描,输入扫描目标,显示认证设置配置功能。 配置路径:【扫描】>【新增任务】>【基本配置】>【主机扫描】。

### 图4 配置主机扫描

扫描									√ 保存	返回
◎ 基本配置 /	扫描 > 任务编辑									
基本参数										
主机扫描	* 扫描目标	标: 19	192.168.161.158				0	は増振导入		
Q、主机扫描参数										
□ 主机通知参数								从资产导入		
							11	模板下载		
	认证设置	置: 目	目标	协议	端口	用户名	密码	操作		
		导	导入认证 手动漆	加认证下载						
	* 策略模仿	板: 完	完全扫描					~		
	拳数模拟	板: 默	默认参数					~		
		注意	:意:重新选择参数模板将算	<u>車置所有已设置</u> 好的参数						

点击【手动添加】,弹出新增认证界面窗口。

### 图5 新增认证

新增认证		×
* 目标:	:	
* 协议:	:	
★ 靖口:	: 地口空間头,4 error	
* 用户名:	JML)2립/J: 1-05635	
密码:		
	論:	- 取当
	4H /	

配置扫描认证参数,选择目标、协议(支持 SMB、SSH、TELNET 三种协议认证)、端口、用户名、 密码。

#### 图6 新增认证

新增认证	×
* 目标:	192.168.161.158 $\vee$
* 协议:	smb v
* 端口:	<b>445</b> 端口范围为:1-65535
* 用户名:	administrator
密码:	8888888
	确定 取消

#### 点击确定,完成新增认证配置

#### 图7 完成配置

扫描								~	保存 返
<ul> <li>基本配置</li> <li>基本配置</li> </ul>	^	扫描 > 任务编辑							
主机扫描		* 扫描目标	192.168.161.158				0	从模板导入	
Q 主机油描参数 ☑ 主机通知参数								从资产导入	
		认证设置	目标	协议	端口	用户名	密码	操作	
			192.168.161.158	smb	445	administrator	*****	劃除	
			导入认证 手动添加 认证	下载					
		* 策略模板	完全扫描					~	
		參数模板	默认参数 注意:重新选择参数模板将重置所有已设	置好的参数				~	

点击右上角【保存】按钮,即完成主机递进扫描任务创建

## 3.3 验证配置

- (1) 新建主机扫描任务,未配置认证参数,其他参数与主机递进扫描任务一致。
- (2) 扫描结束, 2个任务扫描结果, 进行对比分析。
- (3) 正常情况下扫描出来的主机递进扫描任务结果比未配置认证参数的扫描任务多。

#### 图8 验证配置



# 4 主机弱口令扫描配置举例

4.1 组网需求

图9 配置组网图



弱口令检测可以使用系统默认的模板也可以自定义弱口令模板,弱口令破解协议支持大部分常用协议如 SSH/SMB 等。

# 4.2 配置步骤

新建自定义用户和密码字典。

配置路径:【模板】>【数据字典】>【新建字典】。

图10 新建字典

模板						✓ 保存 返回
模板 > 字典模板						
× 字典名称	t: test1	★ 描述信息:	test	* 字典类型:	用户字典 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
Administrator administrator Guest guest admin system	<b>≱典容称不为空目不能过30个学</b> 符		順送做見不为 <u>空目不</u> 超过200个手符			
字典内容长度不超过ds	386个字符					

#### 通过【扫描】>【新增任务】创建一个主机扫描任务。

#### 图11 新增任务

扫描		√ 保存	返回
<ul> <li>② 基本配置 ^</li> </ul>	13篇 > 任务编辑		
基本参数 主机扫描	• 任务名称: 任务名称:		
Q、主机扫描参数 ^ 常规参数	- 不知力が「た法で加加が「チャノイを認識人運転生活会社/不能知道!」/ <>		
端口参数 破解参数	• 扫描完型: ● 主机扫描 ○ Web扫描 ○ 数据年扫描		
主机通知参数 ~ 扫描通知	<ul> <li>• 优先版: ○ 湾 ⑧ 中 ○ 低</li> </ul>		
WSUS通知	• 94/31738: TB95412		
	最高升高: ○ 自动添加到资产		
	最高开程: 〇 波波地東到邮箱 〇 上台地東到FTP		
	Reader and Anniese	~	
	报表模版: 按卡工程师	×	

基本参数,配置任务名称,其他参数默认。 配置路径:【扫描】>【新增任务】>【基本配置】>【基本参数】。

#### 图12 配置基本参数

扫描		✓ 保存 返回
<ul> <li>● 基本配置 ^</li> </ul>	扫描 > 任务编辑	
基本参数		
主机扫描	*任务名称: 主机扇口令扫描	0
Q、主机扫描参数 ~	不能为空/长度不超过30个字符/不能输入重复任务名称/不能包含/:*?*<>	
☑ 主机通知参数 ∨	任务分组:未分组	
	<ul> <li>         ・ 扫描時間:         ・ 主机 当編         ・ ○ 数据 年 当備         ・ 該        、          ・</li></ul>	
	• 优先级: 〇 竜 ④ 中 〇 低	
	<ul> <li>・执行计划: 立規規行 ✓ ・任务的执行计划,可选择任务的执行时期间期期等</li> </ul>	
	是否开启: □ 自动添加到资产	
	最否开台: ○ 发送结果到邮箱 ○ 上传结果到FTP	
	报表到型: htm/服表	~
	报泰模版: 技术工程师	Ψ.

主机扫描,输入扫描目标,策略模板选择<账户密码检测>。 配置路径:【扫描】>【新增任务】>【基本配置】>【主机扫描】。 图13 主机扫描

<ul> <li>③ 基本配置 ^</li> </ul>	扫描 > 任务编辑					
基本参数						
主机扫描	* 扫描目标:	192.168.161.158			٢	从模板导入
Q、主机扫描参数 ~						从资产导入
☑ 主机通知参数 ∨						横板下裁
					4	DEBX THAN
	认证设置:	目标 协议	端口	用户名	密码	操作
			1177740			
		导入队驻 于刻添加	以脏下载			
	★策略模板:	账户密码检测				~
	参数模板:	默认参数				~
		注意: 重新远择参数模板将重置所	有已设置好的参数			

破解参数,勾选 SMB 密码破解,密码字典和用户字典选择步骤(1)创建的字典。 配置路径:【扫描】>【新增任务】>【主机扫描参数】>【破解参数】。

图14 破解参数

扫描							√ 保存	30
<ul> <li>         基本配置         基本参数     </li> </ul>	扫描 > 任务编辑							
主机扫描			* 🗌 令破解时间: 🔡	250				
常规参数		破解项目:	76					
端□参数 破解参数		✓ SMB密码破解	密码字典:	test2	✓ 用户字典:	test1 ~		
☑ 主机通知参数		□ SSH密码破解	密码字典:	SSH密码字典	✓ 用户字典:	SSH用户字典		
		Telnet密码破解	密码字典:	TELNET密码字典	✓ 用户字典:	TELNET用户字典		

点击右上角【保存】按钮,即完成主机弱口令扫描任务创建

## 4.3 验证配置

在账户页面可以看到弱口令账户密码信息。

### 图15 验证配置

扫描			
扫描>任务详情:账户	主机目标 主机漏洞 服务 账户		
服务	用户名	密码	次数
+ SMB/445	admin	#test-123	1
+ SMB/445	Administrator	© test123	1
+ SMB/445	Guest	未知	1

# 5 WEB cookie 录制扫描配置举例

5.1 组网需求

图16 配置组网图



WEB cookie 录制后可以记录页面授权信息, 扫描结果更详细全面, 可用于扫描需要登录验证的 web 网页。

# 5.2 配置步骤

通过【扫描】>【新增任务】创建一个 WEB 扫描任务。

图17 新增任务

扫描			√ 保存	返回
<ul> <li>④ 基本配置 ^</li> </ul>	扫描 > 任务编辑			
基本参数 主机扫描 Q、主机扫描参数 ^ 空报参数	<ul> <li>任务在称:</li> <li>任务公福:</li> </ul>	(15)当該第 不能力定/ 长意不能过30个字符 / 不能输入重复任务名称/不能包含 /;*?*<>  ★分類 ✓ 新売分組		
端□参数 破解参数 ☑ 主机通知参数 ^	<ul> <li>扫描供型:</li> <li>/作牛店:</li> </ul>			
扫描通知 WSUS通知	* 执行计划:	立刻执行 ✓ *任务总约/行计划,司法即任务总约,行司利与周期等等		
	是否开启:	目前通知到第一		
	是否开启:	<ul> <li>&gt; 发送结束到邮箱 () 上标结束到FTP</li> <li>BROTBYARMS</li> </ul>		
	报表类型:	html招表 V		
	报表磁板:	18:41800 V		

基本参数,配置任务名称,扫描类型选择 WEB 扫描,其他参数默认。 配置路径:【扫描】>【新增任务】>【基本配置】>【基本参数】。

图18 配置基本参数

◎ 基本配置	~	扫描>任祭编辑	
基本参数			
Web扫描		* 任务名称: cook	kiege#H2HA
Q Web扫描参数		不能为	为空 / 长度不超过80个字符 / 不能输入重复任务名称/不能包含 /: " ? " <>
		任务分组:未分	3組 ・ 新増分組
		★ 扫描岗型: ○ 主	主机扫描    Web扫描
		* 优先级: 〇 百	高 • 中 ○ 底
		* 执行计划: 立即	UAF > "任务的执行计划。可选择任务的执行时间与周期等
		是否开启: 〇 首	3-10-51031分7 <sup>22</sup>
		是否开启: 🗌 发	±送結果到邮稿 □ 上作給結果到FTP
		报表类型: html	服表 >
		报表模板: 技术	*王母市

WEB 扫描,输入扫描目标,点击添加。 配置路径:【扫描】>【新增任务】>【基本配置】>【WEB 扫描】。

## 图19 Web 扫描

<ul> <li>◎ 基本配置 ^</li> </ul>	扫描 > 任务编辑			
基本参数				
Web扫描	扫描目标:	http://192.168.161.119/bWAPP/aim.php	0	
Q Web扫描参数 ~		添加 从资产导入 模板下载 目标导入		
		目标地址	优先级 cookie录制 🕹 🔞	操作
		http://192.168.161.119/bWAPP/aim.php	中 v 右键粘贴已录的cookie	× ≓
	* 扫描类型:	<ul> <li>主动扫描</li> <li>被动扫描</li> </ul>		
	* 策略模板:	快速扫描		~
	参数模板:	默认参数		~
		注意: 重新选择参数模板将重置所有已设置好的参数		

打开内置浏览器,在地址栏输入要录制 cookie 的目标 URL,回车并在网页上输入正确用户名密码 登录。

图20 录制 cookie

💽 bWAPP - Login - 内置浏览器	
文件(E)编辑(E)视图(M)历史(S)书签(B)窗口(M) 工具(I) 帮助(H)	
🔾 🕶 💭 🛩 🕵 👽 http://192.168.161.119/bWAPP/login.php	o 🔅 🙆 🖶 👄
百度 必应	
😻 bWAPP - Login 🛛	Cookie录制 被动扫描 手动爬行
an extremely bugay web app	URL: http://192.168.161.119/
an extremely raggy wer app.	完成并复制 清空
Login       New User       Info       Talks & Training       Blog <ul> <li>Login</li> <li>Login:</li> <li>bee</li> <li>Password:</li> <li>Image: Control of the standard standa</li></ul>	
Set the security level: Web Security Scanner	属性
Security Audits & Training	名称
Login	值
	域名
	路径
	过期时间 2018/03/12 20:29:03 崇
OVVAPP IN ICEINEER URBER ((0) IN-INDI W 2014 MIME OVDA 7 POIDW COMMENT ON I WHEE AND ARK FOR OUR CHEAT SHEET, CONTAINING	isHttpOnly isSecure SessionCook

点用户登录目标站点进行扫描录制,点击【完成并复制】按钮。

#### 图21 完成并复制



将保存好的录制粘贴到下表对应的 cookie 录制项下。

#### 图22 粘贴到 cookie 录制项

扫描				✓ 保存 返回
◎ 基本配置 ^ 其大会教	扫描 > 任务编辑			
web扫描 Q. Web扫描参数 ✓	扫描目标:	http://192.168.161.119/bWAPP/aim.php	۲	
		添加 从资产导入 模板下载 目标导入 目标地址	优先级 cookie录制 🕹 😧	操作
	* 扫描类型:		中 v 已最制 Q ×	* =
	* 第略模板 :	快速扫描		~
	參数模板:	默认参数 注意: 重新选择参数模板将重置所有已设置好的参数		~

点击右上角【保存】按钮,即完成扫描任务创建,注意:扫描过程不要关闭内置浏览器,关闭会影响扫描结果

## 5.3 验证配置

- (1) 新建 WEB 扫描任务,未进行 cookie 录制,其他参数与 cookie 录制扫描任务一致。
- (2) 扫描结束, 2个任务扫描结果, 进行对比分析。

3、查看 2 个任务对比结果,正常情况下扫描出来的 cookie 录制扫描任务结果比未配置 cookie 录制 扫描的扫描任务多。

#### 图23 验证配置



# 6 WEB 手动爬行扫描配置举例

6.1 组网需求

图24 配置组网图



对手动点击提交的 URL 以及爬虫引擎爬取到的 URL 进行扫描,主要用于对爬虫引擎做补充。

# 6.2 配置步骤

通讯配置,设置扫描器与产品提供内置端浏览器通信地址,使用当前访问的扫描器 IP 地址 配置路径:【其它】>【系统配置】>【通讯配置】

### 图25 通讯配置

🗲 🛈 🐔 https://183.1.3.21/#/main/m	isc/system_config/comm?_k=bhbjkv C Q 度宏	
紫光漏洞扫描系统	& 资产 Q 扫描 図 楔板 ▶ 工具	
其他		
式は新聞		
系统配直 ^	其他 > 系统配置:通讯设置	
网络设置		
路由设置	<ul> <li>適用地址: 183.1.3.21</li> </ul>	
时间配置	扫描器与产品提供內置端浏览器通信,需要使用当前访问的扫描器P地址,实现手动爬行和被动扫描	ŧ
通讯设置		

通过【扫描】>【新增任务】创建一个 WEB 扫描任务。

### 图26 新建任务

扫描		√ 强存	返回
<ul> <li></li></ul>	扫描 > 任务编辑		
基本参数 主机扫描	* 任务名称: 任务名称:		
○ 王初日田御参叔 ^ 常规参数	不能力型/ 长服小地过307 子孙 / 不 任务分组: 未分组	BBA人業点仕労合約小部51章(ジーゲート) / 新聞分組	
蹒□参数 破解参数	<ul> <li>★ 扫描美型: ● 主机扫描 ○ Web扫描 ○</li> </ul>	数据专归编	
☑ 主机通知参数 ∧ 扫描通知	• 优先级: ○ 裔 ● 中 ○ 低		
WSUS通知	*执行计划: 立即执行	<ul> <li>"任約60%/行針,但,可因用年任約60%/行約時時,而期間編</li> </ul>	
	是否开启: 🗌 自动添加到资产		
	是否开启: 〇 发送结果到邮箱 〇 上传结果3	JETP	
	接收报告邮箱		
	按表读版- 技术工程间	v 	
	Second terms		

基本参数,配置任务名称,扫描类型选择 WEB 扫描,执行计划选择"暂不执行",其他参数默认。 配置路径:【扫描】>【新增任务】>【基本配置】>【基本参数】

#### 图27 配置基本参数

<ul> <li>③ 基本配置 ^</li> </ul>	扫描 > 任务编辑	
基本参数 Web扫描 Q. Web扫描参数	• 任务名称: 任务分组:	手动扫描任务        不能为空/长度不超过30个字符/不能输入重复任务名称/不能包含/:*?*<>        未分組
	* 扫描类型:	○ 主机扫描 ● Web扫描 ○ 数编传扫描
	* 优先级:	○ 裔 ● 中 ○ 低
	* 执行计划:	<b>暂不执行</b> > *任务的执行计划,可选择任务的执行时间与周期等
	是否开启:	□ 目动轰加到资产
	是否开启:	□ 发送结果到邮箱 □ 上传结果到FTP
	报表关型:	html报表
	报表模板:	技术工程师

WEB 扫描,输入扫描目标,点击【添加】 配置路径:【扫描】>【新增任务】>【基本配置】>【WEB 扫描】

图28 Web 扫描

扫描					[	√ 保存 返回
<ul> <li>② 基本配置 ^</li> <li>基本参数</li> </ul>	扫描 > 任务编辑					
Web扫描	扫描目标:	http://192.168.161.153/		0		
Q Web扫描参数 V		添加 从资产导入 模板下载	目标导入			
		目标地址	优先级	cookie录制 🕹 💡	操作	
		http://192.168.161.153/	ф ×	右键粘贴已录的cookie	× =	
	★ 扫描类型:	<ul> <li>主动扫描 (</li></ul>				
	* 策略模板:	快速扫描			~	
	4. 35. (****	The second se				
	參取模似:	默认参数 注意:重新选择参数模板将重置所有已设置好的参数				

点击右上角【保存】按钮,查看扫描任务列表,点击该扫描任务右侧的【手动爬行】按钮,弹出手 动爬行窗口

### 图29 手动爬行

扫描 > 任务列表: 普通任务					
任务名称:	手动	状态:	请选择任务状态	~	用户名: 请选择对应的用户 >
开始时间:	请选择日期 凿	结束时间:		ė a	<b>描关型:</b> 请选择任务类型 >
					搜索 清粉条件
名称	扫描类型	创建时间	用户名	状态	操作 手动爬行
+ 手动扫描任务	Web	2018-03-13 10:21:21	admin	未扫描	
					共1条 〈 1 〉 跳至 1 页

#### 点击【复制】按钮,复制 URI 内容到剪贴板(一次只限一条)

手动爬行列表		×
手动爬行工具: 📩 🕑 (如何使用?)		
目标URL	URI 年期	
http://192.168.161.153/	https://192.168.167.102/auxiliary/?token=&action=mancrawler&rvas_task_uuid           =5eeb38674f634900b23a31e7bb8d7e9a⌖_uuid=5aa18964332b47e083           283d739e3321a8⌖_url=http://192.168.161.153/	
	共1条 〈 1 〉 跳至 1	页

将复制好的 URI 内容粘贴到内置浏览器的地址栏,并回车;通过内置浏览器用户进行手动点击想要 检测页面的 URL,点击【提交】按钮,扫描器自动保存所有手动爬行的 URL,开始扫描任务。

#### 图30 开始扫描

• PentesterLab » Web for Pentester II - 内置浏点器	
文件(D编辑(E)视图(V)历史(S)书签(B) 窗口(W) 工具(T) 帮助(H)	
🔾 🗸 🔊 🖉 Mttp://192.168.161.153/sqlinjection/example1/	o 🔅 👩 🔅
百度 必应	
🔗 ab » Web for Pe 🔽	Cookie录制 被动扫描 手动爬行
Pentesteri ab com	URL: http://192.168.161.153/
	提交 清空任务数据
	选择 过滤 已提交 属性
Username: Password: 提交	http://192.168.161.153/
	http://192.168.161.153/sqlinjection/example1/
© PentesterLab 2013	

# 6.3 验证配置

查看扫描结果,目录树显示不只提交的链接扫描,任务在提交链接的基础上,爬行出其他链接进行 扫描。

图31 验证配置



# 7 WEB 被动爬行扫描配置举例

7.1 组网需求

图32 配置组网图



对手动提交的 URL 进行扫描,只扫描提交的 URL,不扫描其余 URL。

## 7.2 配置步骤

通讯配置,设置扫描器与产品提供内置端浏览器通信地址,使用当前访问的扫描器 IP 地址。 配置路径:【其它】>【系统配置】>【通讯配置】。

### 图33 通讯配置

🔶 🛈 🛍   https://183.1.3.21/#/main/misc/	/system_config/comm?_k=bhbjkv
紫光漏洞扫描系统	& 资产 Q、扫描 回 模板 ▶ 工具
其他	
系統配置へ	其他 > 系统配置:通讯设置
网络设置	
路由设置	* 週讯地址: 183.1.3.21
时间配置	扫描器与产品提供内置端浏览器通信,需要使用当前访问的扫描器IP地址,实现手动爬行和被动扫描
通讯设置	

通过【扫描】>【新增任务】创建一个WEB扫描任务。

#### 图34 新建任务

扫描		保存 返回
<ul> <li>◎ 基本配置 ^</li> </ul>	1篇 > 任労綱領	
基本参数 主机扫描	• <b>任務名称</b> : 任務名称:	
<ul> <li>Q. 主机扫描参数 ^</li> <li>常规参数</li> </ul>	不能防空 / K重不超过00个字符 / 不能输入重算任务名物/不能包含 / * ? * <>  く 新電分割 任务分组: 未分組 く 新電分割	
請□参数 破解参数	• 月開開題: ● 主机扫描 ○ Web扫描 ○ 数编阵扫描	
主机通知参数 へ 扫描通知	<ul> <li>优先段:○ 高 ● 中 ○ 低</li> </ul>	
WSUS通知	<ul> <li>执行计划: 立即执行 ショード(注意的执行计划,可选择任意的执行时间与同同等)</li> </ul>	
	显否开启: 📄 自动体站2005年	
	是否开启: 🗍 发送结束到邮箱 🗋 上传结束到FTP	
	招表改型: html积末	
	技術構成: 技术上程/6 ∨	

基本参数,配置任务名称,扫描类型选择 WEB 扫描,执行计划选择"暂不执行",其他参数默认。 配置路径:【扫描】>【新增任务】>【基本配置】>【基本参数】。

#### 图35 配置基本参数

<ul> <li>◎ 基本配置 ^</li> </ul>	扫描 > 任务编辑	
基本参数		
Web扫描	* 任务名称:	被助扫描任务
Q Web扫描参数 v		不能为空 / 长度不超过30个字符 / 不能输入重复任务名称/不能包含 /:*?*<>
	任务分组:	未分组 イント 新増分組
	• 扫描 <del>光</del> 刑 -	
	• 口頂天王 .	micham 💿 micham 🔿 micham
	* 优先级:	○ 窩 ● 中 ○ 低
	* 执行计划:	暂不执行 ✓ "任务的执行计划」可选择任务的执行时间与周期等
	是否开启:	目 申助液加到资产
	是百廾启:	发送请来到醉雨 上传给来到FTP
	报表类型:	html提表
	报表横板:	技术工程师

WEB 扫描,输入扫描目标,点击【添加】;扫描类型选择"被动扫描"。 配置路径:【扫描】>【新增任务】>【基本配置】>【WEB 扫描】。

#### 图36 Web 扫描

扫描						√保存	返回
◎ 基本配置 ^ 基本条款	扫描 > 任务编辑						
web扫描 Q web扫描参数 ✓	扫描目标:	http://192.108.101.153/ 添加 从资产导入 模板下载	目标导入	9			
		目标地址 http://192.168.161.153/	优先级 中 ~	cookie 录制 🛓 💿 右键和贴已录的cookie	操作 ★ =		
	* 扫描类型:	○ 主动扫描 • 被动扫描					
	* 策略横扳:	快速扫描			×		
	参数模板:	默认参数 注意:重新选择参数模板将重置所有已设置好的参数			~		

点击右上角【保存】按钮,查看扫描任务列表,点击该扫描任务右侧的【被动爬行】按钮,弹出被动爬行窗口。

#### 图37 被动爬行

扫描 > 任务列表 : 普通代	<del>I</del> 务						
任务名称:	被动	状态:	请选择任务状态	~	用户名:	请选择对应的用户	~
开始时间:	请选择日期	结束时间:			扫描类型:	请选择任务类型	~
						搜索	清除条件
名称	扫描类型	创建时间	用户名	状态	操	作被动扫描	
+ 被动扫描任务	Web	2018-03-13 10:12:06	admin	未扫描		≙ ► ☞ × ≛	
						共1条 〈 1 〉 ;	眺至 1 页

#### 点击【复制】按钮,复制 URI 内容到剪贴板(一次只限一条)。

### 图38 复制信息

被动扫描		×
被动扫描工具 ᆇ 💡 (如何使用?)		
目标URL	URI (144)RI	
http://192.168.161.153/	https://192.168.167.102/auxiliary/?token=&action=passive&rvas_task_uuid=64           cd6e32cc1a4792be935088b14fba6a⌖_uuid=e852ba2954f74940972701           1a1eb8025a⌖_url=http://192.168.161.153/	
	共1条 〈 1 〉 跳至 1	页

将复制好的 URI 内容粘贴到内置浏览器的地址栏,并回车;通过内置浏览器,用户手动点击要检测页面的 URL,既可以多次点击【提交】按钮进行提交 URL,也可以最后一次性提交 URL,点击【完成】按钮,扫描器将对所有提交的 URL 进行漏洞检测。

#### 图39 漏洞扫描

🧕 PentesterLab » Web for Pentester II - 内置浏览器		
文件(E) 编辑(E) 视图(V) 历史(S) 书签(B) 窗口(W) 工具(T)	報助(日)	
🕒 🗸 🕤 – 😴 🖉 http://192.168.161.153/sqlinjection/examp	141/	o 🔅 👩 🔅 💿
百度 必应		
🔗 ab » Web for Pe 🔀		Cookie录制 被动扫描 手动爬行
PentesterLab.com		URL: http://192.168.161.153/
		提交 完成 清空任务数据
laornama	Recovered:	选择 过滤 已提交 属性
Usemanie.	Passworu	http://192.168.161.153/
© Pentesteri ab 2013		http://192.168.161.153/sqlinjection/example1/
er chicatoreab zoro		
		请求 响应
		GRT / HTTP/1 1
		accept: text/html, application/xhtml tyml application/web.c=0.9 */*.c=0.8
		host: 192.168.161.153 user-sent: Marilla/5.0 (Windows NT 6 1: Win64)
		x64) AppleWebKit/538.1 (KHTML, like Gecko) Built-in Browser/1 0 Safari/538.1

# 7.3 验证配置

查看扫描结果,目录树只显示了提交的链接,扫描任务不进行其他爬行,只对提交的链接进行扫描。 图40 验证配置



# 8 数据库扫描配置举例

8.1 组网需求

图41 配置组网图



配置认证的数据库扫描结果更加具体详细,扫描的漏洞更全面。

# 8.2 配置步骤

通过【扫描】>【新增任务】创建一个数据库扫描任务。

### 图42 新建任务

扫描				√ 保存	返回
◎ 基本配置	^	扫描 > 任务编辑			
<ul> <li>重+&gt;⇒</li> <li>主机扫描</li> <li>○、主机扫描参数</li> </ul>		* 任务名称:	任资名称 不能为空 / 长武不磁过30个字符 / 不能输入重其任务名称/不能包含 /: * ? * <>		
常规参数		任务分组:	未分组 🗸 新聞分組		
端□参数 破解参数		* 扫描类型:	● 主机扫描 ○ Web扫描 ○ 数据库扫描		
☑ 主机通知参数 121世通知		* 优先级:	○ 篇 ● 中 ○ 低		
WSUS通知		* 执行计划:	立期执行 ✓ "任务会执行计划、可这种任务会执行时间与期间等		
		是否开启:			
		是否开启:	□ 发送给果到邮箱 □ 上传给果到FTP		
		报表类型:	hmiR表 V		
		报表模版:	技术工程的 >> >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		

基本参数,配置任务名称,扫描类型选择"数据库扫描",其他参数默认。 配置路径:【扫描】>【新增任务】>【基本配置】>【基本参数】。

### 图43 配置基本参数

◎ 基本配置	^	扫描>任务编辑	
基本参数			
数据库扫描		* 任务名称: 数据库递进扫描	0
Q、数据库扫描参数		不能为空/长度不超过30个字符/不能输入重复任务名称/不能包含/:*?*<>	
		任務分組: 未分組 🗸 🔰	新增分组
		• 扫描英型: ○ 主机扫描 ○ Web扫描 ④ 数据库扫描	
		★优先级: ○ 高 ● 中 ○ 低	
		<ul> <li>执行计划: 立即执行</li> <li>✓ "任务的执行计划,可选择任务的执行时间与周期等</li> </ul>	
		是否开启: 🗋 自动体加到资产	
		是否开启: 🗋 发送给果到邮箱 🗋 上传给果到FTP	
		报表选型: htm/报表	~
		报表模板: 技术工程师	~

数据库扫描,输入扫描目标,显示认证设置配置功能。

配置路径:【扫描】>【新增任务】>【基本配置】>【数据库扫描】。

图44 数据库扫描

<ul> <li>基本配置</li> </ul>	^	扫描 > 任务编辑									
基本参数 数据库扫描 Q 数据库扫描参数			* 扫描目标:	192.168.162.136	3				e		从模板导入 从资产导入 模板下载
			认证设置:	目标 导入认证	协议 手动添加 认订	端口 E下载	用户名	密码	其他参数	撞	作
			★策略模板:	数据库完全检测							~
			参数模板:	默认参数 注意:重新选择参数	牧模板将重置所有已设	置好的参数					~

点击【手动添加】,弹出新增认证界面窗口。

#### 图45 手动添加

新增认证	x
* 目标:	~
* 协议:	v
* 端□:	端口花闺为 · 1.85535
* 用户名:	JIN H, CE273 - 190300
密码:	
	确定取消

配置扫描认证参数,选择目标、协议、端口、用户名、密码。

新增认证		×
* 目标:	192.168.162.136 V	
* 协议:	mysql $\vee$	
★ 端口:	3306	
* 用户名:	源后12日初73:1-06535 root	
密码:	•••••	
数据库名称:		
配置路径:		
	测试链接	

点击【测试连接】,提示"连接成功"。

#### 图47 测试连接

新增认证	提示	×	×
* 目标	连接成功		
* 协议			
* 端口:	3306		
* 用户名:	root		
密码:	*******		
数据库名称:			
配置路径:			
	测试链接		
		确定	取消

### 点击【确定】,完成新增认证配置。

图48 完成配置											
扫描										√ 保存	返回
<ul> <li>③ 基本配置 ^</li> </ul>	扫描 > 任务编辑										
基本参数 数据库扫描 Q、数据库扫描参数 ~	* (3)	描目标: 19	2.168.162.196					G	从模板导入 从资产导入 模板下载		
	λί	正设置: 目	标 2.188.162.136	协议 mysql	端口 3306	用户名	密码 	其他参数	操作 删除 连接测试		
		<b>9</b>	入认证 手动添加 认	证下载							
	* 100	略模板: 数:	据库完全检测						~		
	\$¢	数模板: 默; 注意	<b>认参数</b> 1. 重新选择参数模板将重置所有已;	2置好的参数					~		

点击右上角【保存】按钮,即完成数据库递进扫描任务创建。

## 8.3 验证配置

- (1) 新建数据库扫描任务,未配置认证参数,其他参数与数据库递进扫描任务一致。
- (2) 扫描结束, 2个任务扫描结果, 进行对比分析。
- (3) 正常情况下扫描出来的数据库递进扫描任务结果比未配置认证参数的扫描任务多。

### 图49 验证配置

▼ 1.3 数据库主机漏洞风险分布 紧急 高风险 低风险 中风险 信息 ॖ 数据库无认证-2018-03-13 10:40:00 数据库递进扫描-2018-03-13 10:37:50 紧急 任务名称 高风险 中风险 低风险 信息 总数 数据库无认证-2018-03-13 10:40:00 0 0 з 9 16 4 34 数据库递进扫描-2018-03-13 10:37:50 0 0 8 17 9