# UNIS XSCAN-CN60 漏洞扫描系统 用户 FAQ

Copyright © 2022 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。

1 常	常用配置类 FAQ	·1
	浏览器打开地址链接后显示证书存在安全问题。	1
	admin 账户登录密码忘记,账户被锁定。	1
	内网的地址无法管理设备,可 Ping 通, Web 界面和 SSH 均不能登录。	· 1
	邮件告警或短信告警接收人无法添加。	2
	SSH 登录的 admin 账户如何修改密码?	2
	添加多个任务后,部分任务处于排队阶段。	3
	系统检测结果中无检测详情	3
	选择特定模板后,系统扫描结果中仍存在其它类别的漏洞。	4
2 \	业务功能类 FAQ ······	.4
	添加扫描任务有几种方式?	4
	添加扫描地址后,任务几秒钟就结束,扫描结果无信息。	5
	Web 靶机确实存在此漏洞,但是扫描不出来该漏洞。	5
	漏洞模版上显示的漏洞数量少,没有要查询的规则名称。	5
	主机确认存在扫描无结果,扫描结束。	5
	规则库升级失败,提示升级失败。	8
	如何进行升级。	9
	口令猜解无法添加任务问题。1	1
	对系统扫描的个别主机信息和漏洞信息报告不准确。1	2
	web 扫描结果较少, Web 站点需要登录扫描问题。1	2
	Web 扫描扫不到页面。1	5
	Ping 不通,但是主机存活,系统扫描扫不到主机。1	5
	Web 扫描有页面数,没漏洞。1	5
	正常扫描和系统登录扫描(验证已登录成功),扫描结果没区别。	6
	Web 扫描结束后,怎样可以看到单个站点的页面数。1	6

## 目 录

本文档介绍 UNIS XSCAN-CN60 漏洞扫描系统中用户常见问题及解答。

## 1 常用配置类 FAQ

浏览器打开地址链接后显示证书存在安全问题。

解决方法:

点击继续浏览此网站即可。

图1 点击继续浏览此网站



#### admin账户登录密码忘记,账户被锁定。

#### 解决方法:

登录 account 账户,在用户管理找到 admin 进行编辑,解除锁定或重置密码。

#### 图2 解锁账号

0	账号管理	督用户管理 ≡ 用户权限相	莫板	编辑 / 删除	× 解除锁定 ■ 重置	日 新増+ 刷新 3	搜索[回车]
	用户名	A	用户权限模板	最近登录日期	状态	是否锁定	登录超时 (分钟)
<b>v</b>	admin	[默认用户]	高级管理员功能组	2019-05-13 18:13:27	启用	是	30
	audit	[默认用户]	审计管理员功能组		启用	否	30
	report	[默认用户]	报表管理员功能组		启用	否	30

## 内网的地址无法管理设备,可Ping通,Web界面和SSH均不能登录。

解决办法:

一般此类情况是某些用户添加了对应信任 IP 导致,只允许特定网段 IP 访问,需要直连设备,使用 默认的 192.168.0.1 地址登录,删除信任 IP 或者添加 0.0.0.0/0 的信任 IP 即可解决该问题。

图3 配置信任 IP

Q         信任IP         新理 +         講空 X         期新 C					
□ IP地址/编码	Https	Shell			
0.0.0.0/0	允许	允许			

#### 邮件告警或短信告警接收人无法添加。

原因:系统针对任务建立告警信息,不支持添加固定的告警信息接受人。 解决办法:添加多目标任务,可选择批量导入或者回车换行导入,选择检测结束发送邮件或发送短 信,并添加告警接收人(接收人邮箱建议加白,否则漏洞结果告警太多容易被拉黑)。

图4 告警接收人配置

1個や土規則(1土規則)時後,多个之同以定交辺県(1)組織行分構 付: 192.168.1.100 世可使用地名: www.example.com 00/fectba25xd1fdcb1:101092244088 192.168.1.0/24.192.168.2.1-254.192.168.3.1-192.168.3.254 192.168.1.0/24192.168.1.100		
阳务名称,长度在[1-40]字符之间		
完整的安全扫描		
默认: 系統時代提明]際的负载情況, <b>智能</b> 选择工作引擎。 local: 系統時令选择 <b>本地引擎</b> 。		
置中配置了邮件网关,多个邮箱可用英文逗号()分隔		
置中配置了短信网关,多个手机号码可用英文逗号()分隔		
6537.6MB/7860MB 硬盘使用率: 9.0G/44G へ		

#### SSH登录的admin账户如何修改密码?

解决办法:

使用 SSH 连接工具,连接主机 IP 地址后,登录 admin 账户,使用键盘输入用户身份验证方式,点 击确定后输入 admin 用户的密码,此时登录到 admin 账户,可以通过 changepass 命令更改 admin 账户的密码。修改后,下次 SSH 登录 admin 账户的密码为修改后的密码。(注意: admin 账户 Web 登录密码与录密码可不一致,请注意保存密码,以免遗忘 SSH 方式登)。

#### 图5 SSH 登录 admin 用户

SSH 用户:	名	x
远程主机 服务器类	机: 183.1.0.168:22 (%default%) 类型: SSH2, OpenSSH_7.5p1	3
请输入登 admin	登录的用户名(E):	
	・	
SSH用户身	息份验证 - Keyboard Interactive	x
2	Password:	*
	*****	Ŧ

图6 修改 admin 用户的密码

welcome to UNIS-OS Welcone to UNIS-OS
Last login: Wed Mar 14 09:24:22 2018 from 101.1.21.2 [unis -os]\$ changepass
Input the new password:
Input the password again: [unis -os]\$

确定

## 添加多个任务后,部分任务处于排队阶段。

解决办法:

系统为了防止同时多个任务执行影响设备性能导致系统异常,对并发任务数有限制,此情况一般由于正在运行的任务总数或 IP、站点总数达到了并发上限,导致平台新的任务出于排队等待状态,待执行的任务结束后,排队的任务会被执行。

取消

#### 系统检测结果中无检测详情

解决办法:

部分漏洞检测详情内容较多,导致报表内容冗长,故默认不保存漏洞检测详情,如需保存,在任务 中心>新建任务>系统扫描>检测选项>开启保存漏洞检测详情。

#### 图7 开启保存漏洞检测详情

→ 任务中心 →	□ 系统扫描 ④ WEB扫描 目 安全基线检测 □ 数据	库检测 🔷 口令猜解
新建任务	扫描基本配置 自主选择插件 探测选项 检测选项	引擎选项 登录信息选项
任务列表	最大限度报告漏洞 🗸	若选择开启,扫描结果中不是所有漏洞都经过原理扫描得出,会有一些根据版本信息推测出来的漏洞。
探测未知站点	执行所有规则检测	若选择开启:检测耗时越久、对检测目标的覆盖面更广。
会话录制	执行相关联漏洞	若选择开启:某些已例外的漏洞将加入到归描结果当中。
◎ 资产管理	呆存漏洞检测详情 🗙	若选择开启:漏洞的详细打印信息将加入到扫描结果当中。
┢ 策略模板 <	自适应网络 🗙	根据网络的反应速度,适当调整发包的速率,从而不至于将网络扫瘫痪,但会影响扫描速度
→ 报表管理 <	危险测试 🗙	包含一些危险的测试方法,如:拒绝服务检测,导致扫描目标的拒绝服务,因此慎用
高 系統管理	停止探测无响应主机 🗙	如果扫描过程中发现扫描目标没有反应,停止对该目标的探测
	随机顺序扫描	
	启用口令破解	使用默认字典对系统或服务的口令进行猜解
	测试Oracle账号 X	
	启用Web检测 ×	
	SMB信息探測	

## 选择特定模板后,系统扫描结果中仍存在其它类别的漏洞。

解决办法:

系统扫描选定指定模板后,为保证扫描效果,默认会检测相关联的其它漏洞。如不必要,可在任务 中心>新建任务>系统扫描>检测选项>开启执行相关联漏洞,关闭该功能。

#### 图8 开启执行相关联漏洞

□ 系统扫描 • WEB扫描 目 安全基线检测 □ 数据	库检测 ◆ 口令猜解
扫描基本配置 自主选择插件 探测选项 检测选项	引擎选项 登录信息选项
最大限度报告漏洞	若选择开启,扫描结果中不是所有漏洞都经过原理扫描得出,会有一些根据版本信息推测出来的漏洞。
执行所有规则检测	若选择开启:检测耗时越久、对检测目标的覆盖面更广。
执行相关联漏洞	若选择开启:某些已例外的漏洞将加入到扫描结果当中。
保存漏洞检测详情	若选择开启:漏洞的详细打印信息将加入到扫描结果当中。
自适应网络	根据网络的反应速度,适当调整发包的速率,从而不至于将网络扫瘫痪,但会影响扫描速度
危险测试 🗙	包含一些危险的测试方法,如:拒绝服务检测,导致扫描目标的拒绝服务,因此慎用
停止探测无响应主机	如果扫描过程中发现扫描目标没有反应,停止对该目标的探测
随机顺序扫描	
启用口令破解	使用默认字典对系统或服务的口令进行猜解
测试Oracle账号 X	
启用Web检测 ×	
SMB信息探测	

## 2 业务功能类 FAQ

## 添加扫描任务有几种方式?

三种:

• 手动输入:可一次输入单个或多个主机。

- 使用资产列表。
- 批量导入:下载 Excel 表格,按照模板填写上传。

添加扫描地址后,任务几秒钟就结束,扫描结果无信息。

解决方法:

当主机不存在或者地址不可达,导致扫描不到信息。在提交任务前请仔细核对任务地址。

图9 扫描任务异常

任务名称 🔻	检测周期	开始时间	结束时间	检测耗时	进度	操作
WEB扫拼	手动执行			12分39秒	发现漏洞数:0 检测网页数:1	立即执行▶ 禁用 Ů
WEB指	手动执行	2		36分18秒	<b>漏洞数:0 网页数:3029 剩余</b> 时间:大于1小时	暂停 ▋▌ 停止 ▋
系统扫描-sa	手动执行	2	ون،	16秒	发现漏洞数:0 发现主机数:0	立即执行▶ 禁用 🙂
系统扫描	手动执行		0	30分37秒	发现漏洞数:54 发现主机数:1	立即执行▶ 禁用 Ů
系统扫描	手动执行	2 )2	04 05 1/4110.20	18秒		立即执行 ▶ 禁用 🙂
WEB扫描	手动执行			1小时44分	发现漏洞数:33 检测网页数:5000	立即执行▶ 禁用 🙂
系统扫描-84	手动执行	26		7分27秒	发现漏洞数:24 发现主机数:1	立即执行 ▶ 禁用 🙂
系统扫描	手动执行			.秒	发现漏洞数:25 发现主机数:1	立即执行▶ 禁用 Ů
口令猜解	手动执行	2		2秒	发现弱口令:0	立即执行 ▶ 禁用 🙂
系统扫描-	手动执行			1分1秒		立即执行▶ 禁用也

Web靶机确实存在此漏洞,但是扫描不出来该漏洞。

解决方法:

- (1) Web 靶机存在的漏洞链接通过 IP 或域名访问不到,或者不可跳转该链接,通过直接添加存在问题的域名和 URL 来扫描。
- (2) 规则库内没有该条漏洞的规则,需要升级最新规则库后重新扫描。

漏洞模版上显示的漏洞数量少,没有要查询的规则名称。

解决方法:

规则库版本较老,升级到最新的规则库后即可。

#### 主机确认存在扫描无结果,扫描结束。

原因:地址不可达;主机防火墙开启;(主要为 Windows 防火墙)。

解决办法:

(1) 地址不可达,可能是由于扫描器本身的网络配置原因导致,或者扫描器所在网络禁止访问被扫描主机,更换到对应主机网络区,重新配置网络后即可。

#### 图10 业务地址配置

≓IP管理配置 A接口配置 ♂路由配置 ■ DNS配置			I DNS配置			新增・	▶ 刷新 2 搜索[回车]
VLAN名称	1	IP地址		子网掩码	Mtu	状态	操作
MngtVlan		192.168.0.1 192.168.13.73		255.255.255.0 255.255.255.0	1500	启用	编辑✔ 删除×

#### 图11 路由配置

≓ IP管理配置	▲ 接□配置	☞ 路由配置	I DNS配置		新增十月	動新 2 捜索
目的地址				子网掩码/子网前缀长度	下一跳	Metric
0.0.0.0				0.0.0.0	192.168.13.1	0

(2) 关闭主机防火墙。

Linux 防火墙

开启: service iptables start 关闭: service iptables stop

图12 Windows 防火墙





#### 图13 启用或关闭 Windows 防火墙

🛞 🌛 👻 ↑ 🔐 > 控制面板 >	所有控制面板项 → Windows 防火墙	▼ ひ 搜索控制… ♪	
控制面板主页 分许应用或功能通过 Windows	使用 Windows 防火墙来帮助保护你的医 Windows 防火墙有助于防止黑客或恶意软件通过 In	电脑 ternet 或网络访问你的电脑。	
防火墙	专用网络(R)	已连接 🕥	
更改通知设置			
启用或关闭 Windows 防火墙	你知道且信任的用户和设备所在的家庭或工作网络		
还原默认值	Windows 防火墙状态:	启用	
高级设置	传入连接:	阻止所有与未在允许应用列表中的应用的连接	
对网络进行疑难解答	活动专用网络:	🔮 Support	
	通知状态:	Windows 防火墙阻止新应用时通知我	
	● 秋宾或公用网络(P)	未连接 🕑	

另请参阅
操作中心
网络和共享中心

#### 图14 关闭防火墙

🔄 ⋺ マ ↑ 🍻 > 控制面板 > 所有控制面板项 > Windows 防火墙 > 自定义设置	~	Ç	搜索控制.
白宁以友光网络的沿黑			
日准义古关州知时以且			
你可以修改使用的每种类型的网络的防火墙设置。			
专用网络设置			
〇 启用 Windows 防火墙			
✓ Windows 防火墙阻止新应用时通知我			
🔯 💿 关闭 Windows 防火墙(不推荐)			
公用网络设置			
⑦ ○ 启用 Windows 防火墙			
■ 阻止所有传入连接,包括位于允许应用列表中的应用			
✔ Windows 防火墙阻止新应用时通知我			
◎ 关闭 Windows 防火墙(不推荐)			

## 规则库升级失败,提示升级失败。

图15 规则库升级失败

▲ 版本/特征库升4	ž	Ċ
特征库自动升级	版本/特征库手动升级 版本/特征库本地升级	
升级服务器地址	https://	* @\$Q: http://update.example.com:8090/
执行周期	每天执行一次 🔻 05:52 0	•
Proxy代理服务器		通过设置的代理地址上网获取服务器地址的升级包
代理服务器用户名		
代理服务器密码		
保存	立即升级	
		^
柱灯库北级时间		
特征库开级时间		
当前特征库版本		
系统升级时间		
系统升级结果		升级成功
当前系统版本		1 March 1 Marc
		● 部件 ×

原因:网络地址不可达;升级服务器地址错误。

解决办法:

- (1) 网络地址不可达:测试其它外网地址是否可达,如 www.baidu.com 或者 www.sina.com.cn,确定网络地址可达,并对升级地址进行可用性验证。
- 图16 诊断工具

🖵 任务中心	<	▶ 诊断工具
◎ 资产管理		PING命令 WEBGET命令 靖口探測工具 Tcpdump抓包工具 故歸信息收集
★ 策略模板	<	PING 🔸 www.baidu.com 激流
→ 报表管理	<	注: 限制字符输入: '` \$;\\n < > /?:*()
系統管理	~	PING www.wshifen.com (103.235.46.39) 56(84) bytes of data. 64 bytes from 103.235.46.39: icmp_req=1 ttl=47 time=319 ms
账号管理		64 bytes from 103.235.46.39: icmp_req=2 ttl=47 time=327 ms 64 bytes from 103.235.46.39: icmp_req=3 ttl=47 time=336 ms 64 bytes from 103.235.46.39: icmp req=4 ttl=47 time=335 ms
外发配置告警配置		www.wshifen.com ping statistics
系统告警日志		rtt min/avg/max/mdev = 319.612/329.840/336.224/6.822 ms
日期/时间		
漏洞检测备份		
版本/特征库升级		
诊断工具		

(2) 升级服务器地址填写错误:检查填写的升级服务器地址是否正确,填写正确的升级服务器地址。 默认升级服务器地址为: https://47.92.55.33/。

## 如何进行升级。

解决方法:

(1) 自动升级规则库

在 admin 账户下登录,选择系统管理>版本/版本库升级>版本/版本库升级。

#### 图17 自动升级规则库

Ģ	任务中心	<	▲ 版本/特征库升级	及					
0	资产管理		特征库自动升级	版本/特征库手;	动升级 版本/特征库本地升线	§.			
ġ.	策略模板	<	升级服务器地址		https://47.92.55.33/				* 例如:http://update.example.com:8090/
	报表管理	<	执行周期		每天执行一次	Ŧ	05:52	0	*
٥	系统管理	~	Proxy代理服务器						通过设置的代理地址上网获取服务器地址的升级包
	账号管理		代理服务器用户名						
	外发配置		代理服务器密码						
	告警配置								
	系统告警日志		保存	立即升级					
	日期/时间								
	漏洞检测备份		特征库升级时间						
	版本/特征库升级		特征库升级结果						规则库已经是最新版本
	诊断工具		当前特征库版本						
	验证丁旦		系统升级时间						
			系统升级结果						升级成功
		$\equiv$	当前系统版本						

(2) 界面手动升级规则库和系统版本

在本地搭建 Ftp(3CDaemon 软件)环境,关闭本地主机防火墙,选择对应的升级路径和文件,进行升级。

命令: ftp://user:pass@ip:port/包名.img

## 图18 搭建 Ftp(3CDaemon 软件)环境

文件 至著 報助         TTT 服务器         「TT 服务器         「UT III (IT III ) (IT IIII ) (IT IIIII ) (IT IIIII ) (IT IIIIII ) (IT IIIIII ) (IT IIIIII ) (IT IIIIIII ) (IT IIIIIII ) (IT IIIIII ) (IT IIIIIIIIII	3CDaemon						
TTT 服务器       展初时间       位置       字子 1 秋志         Aug 25, 2017 10:20:08       本地       0       正在监听 FTP 请求于 IP 地址: 192.168.8.207, 領口 21            ·····························	文件 查看 帮助						
TT 服务部       Aug 25, 2017 10:20:08 本地       0 正在监听 FTP 请共于 P地址: 192.168.8.207, 端口 21         送着 TT 服务部       3CDaemon 设置       ×         正確       第二日       3CDaemon 设置       ×         市市 加速       第二日       第二日       第二日         「「」」       第二日       3CDaemon 设置       ×         「「」」       第二日       第二日       第二日       ※         「「」」       第二日       第二日       ※       第二日       ※         「「」」」       第二日       第二日       ※       第二日       ※       ※         「「」」       第二日       第二日       ※       第二日       ※<	TFTP 服务器	启动时间	位置	字节	状态		
3CDaemon 设置       ×         3CDaemon 设置       ×         第717 服务器已经自动(点击)2里停止很导)       第第合公室 FTP用户 (Sysleg 设置)         12次至 Ftyd Joe (点击)2里停止很导)       用户信息         13(存止 (点击)2里停止很导)       用户目息         13(存止 (点击)2里停止很导)       用户目息         13(存止 (点击)2里停止很导)       用户目息         13(存止 (点击)2里停止很早)       用户目息         13(存止 (点击)2里停止很早)       用户目息         13(存止 (点击)2里停止(注)       11(市)         13(存止((点击)2里停止((□))       11(市)         13(存止((□))       11(市)         14(市)       11(市)         15(百日)       11(市)         15(百日)       11(市)         15(百日)       11(市)         15(百日)       11(市)         15(百日)       11(市)         15(日日)       11(市)         15(日日)       11(市)         15(日)       11(市)         15(日)       11(市)         15(日)       11(市)         16(日)       11(市)	FIF 服务器	Aug 25, 2017 10:20:08	本地	0	正在监听	FTP 请求于 IP 地址: 192.168.8.207, 端口 21	
<ul> <li>設置 TET 旅客器</li> <li>(通道定置 TETP 设置 FTP用户 Syslog 设置)</li> <li>(通信定置 LETP 设置 FTP用户 Syslog 设置)</li> <li>用户信息</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定里信以用)</li> <li>(通信定理信以用)</li> <li>(通信定理信以用)</li> <li>(通信定理信以用)</li> <li>(通信定理信以用)</li> <li>(通信定信用)</li> <li>(通信定理信URCA)</li> <li>(通信定理信URCA)</li> <li>(通信定证理信URCA)</li> <li>(通信定证理信URCA)</li> <li>(通信定证证证信URCA)</li> <li>(通信定证信用)</li> <li>(通信定证信URCA)</li> <li>(通信定证信LETP)</li> <li>(通信定证信LETP)</li> <li>(通信定LETP)</li> <li>(通信定LETP)</li> <li>(通信定LETP)</li> <li>(通信LETP)</li> <li></li></ul>			3CDa	emon i	受置		×
PTT 服务器已经自动 (点击这里停止服务)       PACOTYMOUS       用户信息         ILT 服务器已经自动 (点击这里停止纪录)       ILT 服务器已经自动 (点击这里自动测试)       设置/改变用户口令         ILT 服力 信息       用户信息       DATOTYMOUS         IIII (点击这里自动测试)       ILT 服力 用户信息       ILT MQQ\TielRecv\	设置 FTP 服务器		普通	■设置	TFTP 设置	FTP 用户 Syslog 设置	
FIT 服务器已经自动(点击这里停止起条)       用户名称: anonymous         记录至 Ftp-4 log (点击这里停止纪录)       通信         词试停止 (点击这里启动间式)       逆量         運動       型素         通路支持       型素         道面       型参支件         運着纪录/时试文件       一         Styleg 服行器       3CD acmon         強定       取消         放出 服行器       3CD acmon	(STOP)			nonum	0.05	用户信息	
	FTP 服务器已经启动(点击这里停止服务)			monym	Jus	用户名称: anonymous	
記录至 Ftyl log (点击这里傳北段录)         ●          ●						, 设置/改变用/	<b>≏</b> □令
調用得止       (点击)这里包动测试)         運動       一 登录         可約時表       一 形成         運動       一 形成         運動       一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	记录至 Ftpd log(点击这里停止纪录)					用户目录: D:\TIMQQ\FielRecv\	
	×						
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	调试停止(点击这里启动调试)					10/10/1869/	
(保存用)     (保有用)     ((保有用)     ((R+1))     (						回下載	
	清除列表					<ul> <li>☑ 上報</li> <li>☑ 删除文件</li> </ul>	
空音紀泉/(htt文件     保存用户       空音紀泉/(htt文件     保存用户       「「空白泉」     「「空白泉」       「「空白泉」     」       「「空白泉」     」       「「空白泉」     」       「「空白泉」     」       「「空白泉」     」       「空白泉」     」       「空白泉」     」       「雪前名ス件     」       「「空白泉」     」       「「空白泉」     」       「雪前名」     「泉存用户」       「雪前日」     」       「雪前日」     」       「雪前日」     」       「雪前日」     」       「雪前日」     」       「「雪前日」     」       「「雪前日」     」       「「「「」」     」       「「「」」     」       「「」」     」       「「」」     」       「「」」     」       「「」」     」       「「」」     」       「「」」     」       「」」     」       「「」」     」       「「」」     」       「「」」     」       「」」     」       「」」     」       「」」     」       「」」     」       」     」       」     」       」     」       」     」       」 <t< td=""><td></td><td></td><td></td><td></td><td></td><td>■憲文件</td><td></td></t<>						■憲文件	
登音起張Abbut文件						☑ 重命名文件 ☑ 建立目录	保存用户
加速用户:在表单中增加新的用户信息点点击 "保存用户" 编辑用户:选定用户并改变为容后点击 "保存用户" 删除用户:选定想要删除的用户后点击 "删除用户"       3CDaemon     确定     取消     应用(Δ)	查看纪录八期试文件					☑ 劃除目录	
」 増加用户:在表単中増加新的用户信息点点由:"保存用户" 。						]	
Wife用户: 法定用户并改变内容后点击 "保存用户" 劃條用户: 法定想要删除的用户后点击 "勤除用户" 3CDaemon 确定 取消 应用(Δ)			F	曾加用户	: 在表单中期	凯新的用户信息后点击 "保存用户"	
Svalee 略分费			4	肩續用户 ₩险田白	: 选定用户并 · 选定相要	\$改变内容后点击 "保存用户" #除的用户后点击 "删除用户"	
Svalee 略符要			<u> </u>	13K3×/13/~	: ADAENSKA		
3CDaemon     确定     取消     应用(A)       Svalog 略符要			—				
Svalog 解答器			3CD	aemor	Ì	确定	取消 应用(A)
Sveloe #A-B							U
	Surl og 服务哭						
	TFTP 客户机						

#### 图19 手动升级

▲版本/特征库升	及					
特征库自动升级	版本/特征库手动升级	版本/特征库本地升级				
特征库升级	ftp://u	iser:pass@ip:port/xxx.img	升级	停止	示:升级前系统会自动保存配置,	升级过程中系统扫描引擎会重启
系统升级	ftp://u	iser:pass@ip:port/xxx.img	升级	停止	示:升级前系统会自动保存配置,	系统升级过程中系统会重启
特征库升级时间					4	
特征库升级结果				规则库已经是最新	版本	
当前特征库版本						
系统升级时间						
系统升级结果				升级成功		
当前系统版本						

#### (3) 界面本地升级

点击导入的按钮,选择本地的升级文件直接导入即可。

#### 图20 界面升级

▲ 版本/特征库升级	۶.		
特征库自动升级	版本/特征库手动升级	版本/特征库本地升级	
特征库升级	Ę	入升级包并升级特征库	操作提示:上传特征库升级包后,稍后请手动确认进行升级。提示:升级过程中系统扫描引擎会重启
系统升级		导入升级包并升级系统	操作提示: 上传系统升级包后, 稍后请手动确认进行升级。提示: 系统升级过程中系统会重启
特征库升级时间			
特征库升级结果			规则库已经是最新版本
当前特征库版本			
系统升级时间			
系统升级结果			升级成功
当前系统版本			

(4) 后台升级

打开终端管理软件,使用 ssh2 协议登录后台,初始用户名/密码: admin/admin

本地搭建 Ftp(3CDaemon 软件)环境,关闭本地主机防火墙,选择对应的升级路径和文件。 后台执行命令:

特征库升级: sigup ftp://ip/包名.img

系统升级: patchall ftp://ip/包名.img

#### 口令猜解无法添加任务问题。

原因:在无资产组信息的条件下,无法添加口令猜解任务。

解决办法:添加资产组后,勾选相应的服务类型和数据库类型提交任务。

#### 图21 资产组管理

🖵 任务中心	<	❷ 资产管理								新增资产+
③ 资产管理		▲ 资产组	搜索[回车] 🗸 🗸	🗞 资产详情						
由- 策略模板	<			资产风险	漏洞详情					
□ 报表管理		→ WEB扫描-192.108.1.22页/- → 系统扫描-3资产		开始时间沿有检索到	数据	结束时间	高	中	低	信息
✿ 系统管理		_		100 101 102 00 00	00.2m					

#### 图22 新增资产

新增资产				×		्री	/增资产 <b>十</b>
资产类型	系統扫描	٣	*提示: 请选择资产类型				
资产组名称	系统资产-		*提示:请填写资产组名称,长度在[6-40]字符之间		ф.	低	信息
扫描IP/站点			◆ IP示例: 192.168.1.100 域名示例: www.example.com 主机和示例: 192.168.1.0/24,192.168.3.1-192.168.3.254 多小IP或域名之间可使用英文()或回车分隔				
提交							

#### 图23 口令猜解配置

🖵 任务中心 🛛 🗸 🗸	□ 系统扫描 Q WEB扫描	3安全基线检测 4	> 数据库检测 ◆ □令猜解								
新建任务	基本配置 引擊选项										
任务列表 探测主知站点	资产名称	系统扫描-192.1	168.1.3资产			٣	▼ * 若资产为空,请先在资产管理处添加资产或者先执行系统或WEB扫描				
会话录制	任务名称	口令猜解-					*提示:请填写任务名称,长度在[	1-40]字符之间			
() 20 <del>- 2 PN</del> TH	执行方式	立即执行	▼ * 请选择执	行方式							
	服务类型	TELNET	组合模式	٣	TELNET组合字典	٣	端口 23	* 勾选项端口必填			
▶ 策略模板 〈		FTP	组合模式	٣	FTP组合字典	٣	端口 21				
→ 报表管理 <		SSH	组合模式	٣	SSH组合字典	٣	端口 22				
系统管理		POP3	组合模式	Ŧ	POP3组合字典	Ŧ	端口 110				
		SMB	组合模式	Ŧ	SMB组合字典	Ŧ	端口 445				
		SNMP	标准模式	٣	SNMP密码字典	٣	端口 161				
		RDP	组合模式	٣	RDP组合字典	٣	端口 3389				
		SMTP	组合模式	٣	SMTP组合字典	٣	端口 25				
		REDIS	标准模式	Ŧ	REDIS密码字典	٣	端口 6379				
	数据库类型	Oracle	组合模式	٣	Oracle组合字典	٣	端口 1521	SID			

#### 对系统扫描的个别主机信息和漏洞信息报告不准确。

原因: 主机地址可能是 NAT 或者映射之类的地址,导致服务识别与漏洞测试过程中可能出现主机信息及服务被代理或者代理主机端口转换,和多端口多服务多主机情况存在导致的信息返回紊乱。此情况是主要由网络原因导致。

该设备上还有其它设备映射过来的端口,则可能会检测到更多的特征,也会检测更多的系统。 解决方法:

避免由于网络的原因导致扫描结果不准确,可在局域网内进行系统漏洞扫描,跳过 NAT 设备、防火墙、代理类设备。同网段或者直连扫描结果准确性更高。

#### web扫描结果较少,Web站点需要登录扫描问题。

原因: Web 站点设置了主页登录,认证等方式,扫描器需要拿到对应的信息才能扫到更多的结果。 解决方法:

填写登录信息后进行扫描。

常见的登录认证方式:认证登录选型:有验证码的是 Cookie,无验证码 Form,用户名和密码写在 URL 里的是 Basic 认证。

(1) Cookie 认证信息获取

以火狐浏览器为例:登录上去后使用开发者工具,找到对应的 Cookie 信息。提交后重新扫描。

#### 图24 Cookie 认证信息获取

P	查看器	控制台 i	問试器 样式编辑器 性能 内存 网络 DOI	И		B->≡ ₽ 🌼
ŵ	所有	HTML	CSS JS XHR 字体图像媒体 Flas	h WS 其	他	④ 68 个请求, 2,297.92 KB, 9.80 秒 ♀ 过滤 URL
3	状态	方法	文件		域名 原	消息头 Cookie 参数 响应 耗时 完全性
٠	200	GET	/dashboard/		document	it that is a fact that is a fact that the second local (fact that the second local (fact the second (fact the second local (fact the seco
-	304	GET	foot-awesome anin.css	-	styleshee	High Mult nut some some css/iont-awesome/css/iont-
▲	304	GET			styleshee	隋永方法: 68.1
▲	304	GET	UNITOTITITUC registicas		styleshee	远程地址: (
▲	304	GET			styleshee	状态码: ▲ 304 Not Moalflea 编辑和重发 周
▲	304	GET	mana percentap		styleshee	版本: HTTP/1.1
▲	304	GET			styleshee	▼ 讨逢消息头
	304	GET	,		styleshee	- 明白(112) 字共)
▲	304	GET			styleshee	
	304	GET			styleshee	Etag: W/ 180 /9-148 / 154953000
▲	304	GET	CIOCKI aLE. CSS		styleshee	Date: "Thu, 01 Jun 2017 11:29:35 GMT"
	304	GET			styleshee	Server: "RaySaas/1.6"
▲	304	GET			styleshee	▼ 请求头 (821 字节)
	304	GET			. styleshee	Host:
▲	304	GET	bootstrap-markdown		styleshee	User-Agent: "Mozilla/5.0 (Windows NT 6.3; W) Gecko/20100101 Firefox/53.0"
۸.	304	GET	login-soft css		styleshee	Accept: "text/css,*/*;q=0.1"
۸.	304	GET			styleshee	Accept-Language: "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3"
۸.	304	GET	concern.css		styleshee	Accept-Encoding: "gzip, deflate, br"
	304	GET			styleshee	Referer:
	304	GET	inc. Lau		styleshee	Cookie: "ISESSIONID=REFE3CCE1958E5221A4_s8x9ab5uassa26ava6bac92araba"
۸.	304	GET		N.	styleshee	Connection: "keen-alive"
	304	GET	customoe		styleshee	If Modified Since: "Wed 15 Feb 2017 10:35:53 CMT"
۸.	304	GET	hs3.css		styleshee	If None Mothy "W/"19070 1497164052000"
	304	GET	June ,		o script	Code Codel, wy 100/3-100/13-30000
	304	GET			script	Cache-Control: max-age=0
	304	GET	s		script	
	304	GET	br		script	
	304	GET	tw		script	

#### 图25 Cookie 信息填写

❷ 资产管理				新增资产+
▲ 资产组	搜索[回车] 🗸 🗸	● 资产详情		$\sim$
一日WEB扫描 资产		资产风险 漏洞详情 资产指约	文信息 WEB资产属性	
✔ 网站地址:		资产名称	网站地址: http://192.168.1.22/	
田系统扫描-3资产		起始URL	http://192.168.1.22/	
		其他URL		
		网站域名	192.168.1.22	
		扫描根目录	/	
		例外URL		
		登录认证	Cookie/Session认证	▼ < 登录验证
		Cookie	•	
		把Cookie信息填写到此处		
		上传网站证书	浏览 未选择文件。	浏览器客户端证书,如PFX/PKCS12等格式
		上传网站证书密码		导出证书时设置的密码
		提交		

#### (2) Form 认证信息获取

用火狐登录网站, F12 开发者视图可以看到登录采用的 Post 请求, 点击编辑和重发可以看到请求头和请求体, 点击原始头可以看到请求头和响应头。

#### 图26 Post 请求发送数据

bWAPP is licensed under [@] IF-MANNE DVBA / Follow @WWE_UT on Twitter and osk for our cheat sheet, containing all solutions! / Need an exclusive interring?																	
□ □ 査請器 □ 控制台 □ 満試器 () 株式編編器 ⑥ 性能 00 内存 三 剛然 8 存储									\$ 🗆 E	γ							
前 新有 HTTML CSS IS XHR 字体 图像 媒体 Flash WS 其他 □ 持续日志 □ 莫刑集存							⊽ 过滤 URL		Þ								
状态	方法	文件	域名	原因	樊型	传输	大小	0鄣 8	01 1	.60 勤	240 肇秒	消息头	Cookie	参数	响应	耗时	
▲ 302		login.php	🔏 183.1.3.102	document	html	23.41 KB		→ 3 ms				<b>请求网址:</b> http://1	83.1.3.102/bWAPP,	/login.php			
0 200	GET	potelphp	🔏 183.1.3.102	document	html	23.27 KB	22.82 KB	→ 3 ms				请求方法: POST					
0 200	GET	html5.js	<i>🎽</i> 183.1.3.102	script	js	已缓存	2.34 KB					远程地址: 183.1.3.	102:80				
												状态码: 🔺 302 Fou	nd ⑦ 编辑和重发	t 原始头			
<b>post请求发送数据</b>							版本: HTTP/1.1	_									
												) 响应头 (602 字节)					
												)请求头 (542 字节)					

点击编辑和重发,看到 Post 请求头内容,可以用于网站认证时使用。

#### 图27 请求头内容



资产管理/资产详情,选择登录认证方法为 Form 认证,把请求头内容复制到提交数据中,提交 URL 中写入登录 URL,提交数据格式如下图中所示

#### 图28 Form 认证配置

♀ 资产管理								新增资产+
<b>山 资产组</b> 担	腔腔[回车]	~	🗞 资产详情					~
────────────────────────────────────			资产风险 漏洞	同洋情	资产指纹信题	WEB资产属性		
────────────────────────────────────			资产名称			网站地址:http://183.1.3.102/bWAPP/lo	gin.php	
────────────────────────────────────			起始URL			http://183.1.3.102/bWAPP/login.php		
✔ 网站地址:http://183.1.3.102/bWAPP/login.p	php		Mahi IDI					
—————————————————————————————————————			AUGORE					
http://183.1.3.234:8081/			网站域名			183.1.3.102		
一 王 WEB扫描-定时任务-禁用资产			扫描根目录			/		
────────────────────────────────────			例外URL					
────────────────────────────────────			登录认证			Form认证		▼ ◆登录验证
〒WEB扫描-234-1比数/ ▲	-	_	掲芯URI		Г	http://183.1.3.102/bWAPP/login.php		
────────────────────────────────────	ß	<u>ê</u>	22200011		L		1 00 ( 1 1 h	1
────────────────────────────────────	40		提交数据		l	login=bee&password=bug&security_le	evel=0&form=submit	
王WEB资产-探测未知站点转换								
WEB扫描-关闭木马检测资产						(年1日本)(年 十)(年1日)(日本)(年		
────────────────────────────────────			上传网站证书			四年又件 木四年江内又件		浏览器各户病证书,如PFX/PKCS12等格式
────────────────────────────────────			上传网站证书密码					导出证书时设置的密码
—————————————————————————————————————			10 <del>*</del>					
——IFIWEB扫描-不启用网站木马检测资产			145X					

#### (3) Basic 认证信息获取

可在提交的 URL 中获取到相应的用户名和密码,并填写到认证框内即可。

#### 图29 Basic 配置

≫ 资产详情		N						
资产风险 漏洞详情 资产指	紋信息 WEB资产属性							
资产名称	网站地址: http://192.168.1.22/							
起始URL	http://192.168.1.22/							
其他URL								
网站域名	192.168.1.22							
扫描根目录	/							
例外URL								
登录认证	Basic认证 ▼ <							
用户名	account							
密码	•••••							
上传网站证书	浏览 未选择文件。	浏览器客户端证书,如PFX/PKCS12等格式						
上传网站证书密码		导出证书时设置的密码						
提交								

#### Web扫描扫不到页面。

解决办法:检查网络是否连通,地址是否可访问,是否有防护设备,是否开了防爬虫功能。

#### Ping不通, 但是主机存活, 系统扫描扫不到主机。

解决办法:判断网络是否连通,是否有防护设备,建议强制扫描,关闭"存活探测"。

□ 系統扫描 ♥ WEB	日描 日 安全基线检测 🗅 数	■ 日本					
扫描基本配置 自主派	选择插件 探测选项 检测选计	页 引擎选项 登录信息选项					
提示被扫目标 本扫描之前提示被扫描主机,需要扫描目标支持messager服务							
开启存活探测	×	如果开启,引擎使用如下探测方法进行挑 如果不开启,则对所有主机进行漏洞监测	7题,如果不能确定存活,则不进行检测,提高检测速度 J,会延长检测时间				
端口扫描范围	• 标准	)快速 🔷 全部 🔷 指定	标准: 默认端口4000多个。快速:100个常用端口。全部: 端口0-65535 指定: 单个或范围如22,1-1024,指定TCP端口: TCP:1024-65535,指定 UDP;满口: UDP:1025-65535				
TCP端口扫描方式	CONNECT	SYN	CONNECT方式为全连接扫描,完成TCP/IP的三次握手,速度较慢 SYN方式,只需要发送TCP SYN包即可完成检测,速度快,建议使用SYN				

## Web扫描有页面数,没漏洞。

解决办法:

(1) 本身无漏洞。

- (2) 爬虫爬取下来的页面解析后无漏洞。
- (3) 发探测包解析的时候被防护设备拦截。
- (4) 发测试包的前提是根据爬到的页面发对应的测试包,所以爬不到页面也就不会发测试包,不会 去检测漏洞。
- (5) 页面数太多,但没有漏洞,原因是超过系统超时时间,自动断开,还未判断出漏洞。

#### 正常扫描和系统登录扫描(验证已登录成功),扫描结果没区别。

可能是系统本身是一个空系统,装的软件较少,开启的服务少,所以差别不大,对外提供的端口和 服务都类似。

#### Web扫描结束后,怎样可以看到单个站点的页面数。

解决办法:在任务列表里面点击对应主机,页面右边会显示该站点的网页数。

#### 图30 查看站点网页数

