UNIS XSCAN-CN80 系列漏洞扫描系统 用户 FAQ

Copyright © 2023 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。 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 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。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。
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
2 业务功能类 FAQ
添加扫描任务有几种方式?3
添加扫描地址后,任务几秒钟就结束,扫描结果无信息。
Web 靶机确实存在此漏洞,但是扫描不出来该漏洞。4
漏洞模版上显示的漏洞数量少,没有要查询的规则名称。4
主机确认存在扫描无结果,扫描结束。4
规则库升级失败,提示升级失败。7
如何进行升级以及升级注意事项。7
口令猜解无法添加任务问题。10
对系统扫描的个别主机信息和漏洞信息报告不准确。11
web 扫描结果较少, Web 站点需要登录扫描问题。11
Web 扫描扫不到页面。14
Ping 不通,但是主机存活,系统扫描扫不到主机。14
Web 扫描有页面数,没漏洞。14
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。
Web 扫描结束后,怎样可以看到单个站点的页面数。
虚拟漏扫中 CPU 使用率、内存使用率、磁盘使用率为何与 cas 上显示不同。
SysScan-SE/AK810 款型设备上插上四万兆插卡,web 界面禁用万兆光口,显示为 down 的状态,但设备 指示灯仍微亮。
SysScan-VE 款型漏扫启动后登录 web 界面,查看机器码和授权不会立即显示。
基线核查的离线任务进行 ipv6 地址检测为何失败。16
新建任务后后删除该任务,再建同名任务,资产处该同名任务信息后缀为6位数字代表含义是?16
系统管理>网络接口, IP 管理配置中 vlan 名称和默认 MngtVlan 表示为 vlan 还是网桥?17
使用系统插件中自定义策略模板进行扫描时,为何还会扫描出非自定义策略中漏洞呢?17
系统时间是否会影响授权时间?17

系统支持删除资产以及资产组吗?17
账号忘记密码如何处理?
设置信任 ip 后,无法访问 web 页面如何处理?19
系统出现 CPU、内存超高告警如何处理?19
系统出现升级卡顿,升级时间过长如何处理?19
系统网卡初始化后如何恢复?19
Account 账号下 License 管理已经使用 IP 和剩余 IP 是如何统计的19
Web 扫描任务,通过点击任务详情,再直接点击漏洞目录树展示是空的?
Cloud&Ve 型号漏扫增加是否支持多网卡,增加网卡后是否需要重新启动漏扫?
windows 密码破解出任意用户名任意密码是什么意思20
新架构(E6202P05版本以及之后版本)漏扫的资产和资产组是怎么使用的?20
使用会话录制页面操作卡顿如何处理?20
NTP 同步后,时间不正确可能什么原因导致的?20
扫描过程中出现扫描设备或其他主机与漏扫之间无法 Ping 通,扫描结束后可以 ping 通,出现此现象原因
是什么?20
临时授权的时间扩容和功能扩容以及 IP 扩容分别怎么使用?20
自定义用户可以看到 admin 账号下新建的资产吗?20
使用资产方式添加扫描目标时提示"不允许添加特殊字符",资产示例"10.0.254.1(admin)",出现此种情
况如何解决?
恢复出场设置以及初始化后,会关闭设备吗?21
编辑任务,未修改扫描目标却提示未验证通过,格式不正确是什么原因?
已经提交的扫描任务再次编辑未修改扫描目标的前提下,为什么会报扫描格式和扫描长度的错误?21
扫描后查看被扫描目标的操作系统或者版本与实际不符,怎么处理?
扫描任务列表的历史执行记录的日之下载打不开?21
在系统扫描中,检测选项里的启用口令破解与使用口令破解模块有什么区别且在口令破解功能里,分为组
合模式和标准模式,这两种模式分别是什么,在扫描速度上和对系统的影响上,有什么区别?21
授权服务器导入申请的授权提示厂商信息校验错误是什么原因?22
激活 Cloud 漏扫的授权服务器授权时,提示 "SCAN 一年订阅版不可以申请临时授权"22

本文档介绍 UNIS 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

SecPath 漏洞扫描系统 account account								account 👻	
例 (1)	号管理	● 用户管理 = 用户	权限模板	编辑 / 删除 ×	解除锁定 🖬 👔	1董 13 新增+	刷新2	搜索[回车]	¢
	用户名		用户权限模板	最近登录日期	状	à	是否锁定	登录超时 (分钟)	
~	admin	[默认用户]	高级管理员功能组	2022-05-16 10:0	5:36 启	用	否	30	
	audit	[默认用户]	审计管理员功能组	2022-05-10 14:2	4:42 启	用	ē	30	
	report	[默认用户]	报表管理员功能组	2022-04-20 09:3	8:30 启	用	否	30	
总计3条	记录								

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

a。 信任IP		新増 + 満空 x 刷新<i>C</i> 授 紫[回年]	0
□ IP地址/總码	Https	Shell	
沒有拉家到数据 总计0条记录			< >

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

扫描目标			 ・
任务名称			*提示: 请填写任务名称,长度在[1-40]字符之间
执行方式	立即执行	٣	*提示:请选择执行方式
系统漏洞横板	全部漏洞扫描	٣	*提示: 请选择漏洞插件模板
检测模式	标准扫描	٣	标准扫描: 默认选择标准端口的端口范围,采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描
			议想过册:议组的对过细目的运行主的好声。第日进步转动 完全扫描:我儿选择全部国内的端门范围,用主体的将为斯斯,端口扫描,服务判断,漏洞测试的步骤对扫描目标进行完整的安全扫描 深度扫描:利用配置好的用户名密码列表对主机进行登录后的安全扫描
调试模式	× .		若开启,则记录目标评细插件执行日志。
执行优先级别	ф	٠	*提示:当任务达到并发上限时,'排队等待中'级别高的任务将优先执行
分布式引擎	默认	٠	*默认:系统将根据引擎的负载情况,智能选择工作引擎 local:系统将会选择本地引擎
吉警模板	无	٠	*提示:告警发送配置,请到(系统管理>任务告警)下设置
	提交		

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 SSH 方式登录密码可不一致,请注意保存密码,以免遗忘)。示意如下。

[root]\$ changepass

Input the new password:

Input the new password again: [root]\$

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。

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。E6202P05 以及之后版本默认开启, 页面无此配置项。

图5 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 イ 若道	5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 苯 若道	韬开启: 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 考試	提开启:某些已例外的漏洞将加入到扫描结果当中。
③ 资产管理	呆存漏洞检测详情 X 若道	指开启:漏洞的详细打印信息将加入到扫描结果当中。
	自适应网络 X 根拠	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 × 包括	——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
合 <i>无体等</i> 理	停止探测无响应主机 🗙 如5	思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	目默认字典对系统或服务的口令进行猜解
	测试Oracle账号 🗙	
	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6 扫描任务异常

任… 🔻	任务名称	扫描类型	扫描目标	检测结果	执行方式	fit	任务	操作
-		transmitting of the second sec			立即执行	中	已完成	启动
	1000				立即执行	中	已完成	启动
10	1000	The second s		and the second se	立即执行	中	已完成	启动
					立即执行	中	已完成	启动
25	> -173_pv62	系统扫描		●高(0) ●中(0) ●低(0) ●信息(0)	立即执行	中	已完成	启动
					每天执行	中	已完成	启动
10		-		And the second second	立即执行	中	已完成	启动
18	> 100000			The second second second	立即执行	中	已完成	启动

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7 业务地址配置

≓ IP管理配置	▲ 接口配置 ◇ 路由配置	■ DNS配置		自动DHCP + 新增	+ 刷新C 投索[回车]	12
VLAN名称	▼ IP地址	子网挽码	Mtu	状态	操作	
MngtVlan	192.168.0.1 192.168.13.177	255.255.255.0 255.255.255.0	1500	启用	编组》	
总计1条记录						< 1 →

图8 路由配置

= 1	P管理配置 A 接口翻	で 路由配置	■ DNS配置		新增+ 刷新 C	授茶[回车]
	目的地址		▼ 子网掩码/子网前缀长度	下一跳	M	letric
	0.0.0.0		0.0.0	192.168.13.1	0	
总计1分	和记录					< 1 →

(2) 关闭主机防火墙。

Linux 防火墙

开启: service iptables start 关闭: service iptables stop

图9 Windows 防火墙





图10 启用或关闭 Windows 防火墙

	עראס איזעראיידר בין איז איזראיידר (יידי	
🛞 🌛 🔻 🕈 🗬 🕨 控制面板 🕨	所有控制面板项 ▶ Windows 防火墙	∨ Ů 搜索控制… ۶
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 Windows 防火墙有助于防止黑客或恶意软件通过 I	电脑 nternet 或网络访问你的电脑。
防火墙	● 受用网络(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
	🛛 🔮 来宾或公用网络(P)	未连接 🕑

另请参阅
操作中心
网络和共享中心

图11 关闭防火墙

🔄 🎅 ▼ ↑ 🍻 > 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.
自定义各类网络的设置			
你可以修改使用的每种类型的网络的防火墙设置。			
5日网络设置 			
Image: Imag			
□ 阳止所有传入连接,包括位于分许应用列表中的应用			
☑ Windows 防火墙阻止新应用时通知我			
● 天均 Windows 的大幅(小程序)			
公用网络设置			
🕢 🔿 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12 规则库升级失败

▲ 升级管理					¢
规则库在线升级 系统/	规则库/补丁FTP升级 系统/制	观则库/补丁离线升级			
升级服务器地址	htt			*例如: http://update.example.com:8090/	
执行周期	每天执行一次	* 03:13	٥	•	
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					
当前系统版本	_				2 v
当前补丁版本					
当前规则库版本			•		
升级记录					
					× 登告 无法连接到升级服务器,请检查后重试!
					The second second second many second second second

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13 诊断工具

~	26 (c) 66 TH	
*	於九昌理	▶ 诊断工具
	账号管理	网络诊断 端口探测工具 Traceroute Tcpdump抓包工具 故障信息收集 一键诊断 反向支持 调试模式 SSH解锁
	网络接口	
	外发配置	PING * www.baidu.com
	告警配置	注: 限制字符输入: '` \$;\\n < > /?:"()
	分布式部署	PING www.wshifen.com (103.235.46.39) 56(84) bytes of data.
	日期/时间	64 bytes from 103.235.46.39: icmp_req=1 ttl=46 time=229 ms
	配置备份恢复	64 bytes from 103.235.46.39: icmp_req=3 ttl=46 time=217 ms
	漏洞检测备份	64 bytes from 103.235.46.39: icmp_req=4 ttl=46 time=236 ms
	升级管理	www.wshifen.com ping statistics
	信任IP	4 packets transmitted, 4 received, 0% packet loss, time 3003ms rtt min/avg/max/mdev = 208.186/222.876/236.188/10.889 ms
	诊断工具	
	验证工具	
	SNMP管理	

(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/。

如何进行升级以及升级注意事项。

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>升级管理。

图14 自动升级规则库

HBC	SecPath 漏洞扫描	苗系统			
系統管理	< ① 升级管理				
账号管理 网络接口	规则库在线升级 系统/	规则库/补丁FTP升级 系统/规则库/补	丁腐线升级		
外发配置	升级服务器地址	https://			* 例如: http://update.example.com:8090/
告警配置	执行周期	每天执行一次	03:13	0	
分布式部署	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
日期/时间	(4) 理解 友 慧 田 白 友				
配置备份恢复	代理版另簡用广告				
漏洞检测条份	代理服务器密码				
升级管理		保存 文册升级			
信任IP		24.947 F 94			
诊断上具 验证工具					
^{短星上兵} SNMP管理	当前系统版本				
License管理	当前补丁版本				
	当前规则库版本				
快速向导	升级记录				点击查看

(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15 搭建 Ftp(3CDaemon 软件)环境

aemon									
看帮助 TFTP 略条哭	一一启动时间	位置	字节	状态					
FTP BESSM	Aug 25, 2017 10:20:08	本地	0	正在监听	FTP 请求于 IP 地	#ŀ: 192.168.	8.207. 端口 2	21	
		3CD	aemon i	受置					
		普	通设置	TFTP 设置	FTP 用户 日户信息	og 设置			
服务器已经启动(点击这里停止服务)			anonym	ous	用户名称: a	anonymous			
							设置/改	变用户口令	
至 Ftpd.log(点击这里停止纪录)					用户目录:	D:\TIMQQ\F	elRecv∖		
<u> </u>					此用户能够:				
调试停止(点击这里启动调试)					☑登录				
					⊻ ト载 ☑上载				
清除列表					☑ 删除文件				
6					● 複 = ×1+			4	25日户
查看纪录/调试文件					 ✓ 建立目录 ✓ 删除日录 				×(13713)
								fl	删除用户
		F	增加田白	• 在書前中#	きかぶか田内信官!	后占主 " 促友	田白。		
			编辑用户	· 选定用户;	#改变内容后点击	"保存用户" "哪路用户"			
		1	1617 KON / TO /	: 120AE/3KSK8					
		301	Daemor	1			确定	取消	应用(A)
Syslog 服务器									
TFTP 客户机									

图16 手动升级

▲ 升级管理		
规则库在线升级 系统/规则	库/补丁FTP升级 系统/规则库/补丁离线升级	
规则库升级 (切换至SFTP)	ftp://u	开极 停止 提示:升级前系统会自动保存配置
系统/补丁升级 (切换至SFTP)	ftp://user:pass@	升级 停止 提示:升级前系统会自动保存配置,系统升级过程中会重启系统
当前系统版本		*****
当前补丁版本		暂未升级补丁
当前规则库版本		
升级记录		点击查看

(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17 界面升级

▲ 升级管理		
规则库在线升级	系统/规则库/补丁FTP升级 系统/规则库/补丁离线升级	
规则库升级	导入规则库升级包 提示:	上传规则库升级包后,需手动确认进行升级。
系统/补丁升级	导入系统补丁升级包 提示:	上传系统/补丁升级包后,需手动确认进行升级。系统升级过程中会重启系统
当前系统版本		a starting party in the
当前补丁版本		暂未升级补丁
当前规则库版本		and the second sec
升级记录		言言言言

(4) 后台升级

打开终端管理软件,如 putty,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

(5) 注意事项

升级前需要停止。正在执行的任务,升级过程中需要重启设备,升级过程所需要时间根据产品型号和性能不同,大概在 40 分钟到 1.5 小时左右,升级过程请耐心等待,不要在升级过程进行断电重 启等异常操作,否则可能出现系统无法启动等问题。

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18 资产组管理

🖵 任务中心	<	● 资产管理	新借+ 批型等入土 :	Q ¥≋e
 资产管理 			◆颜态产: 10 主机态产: 8 ₩EB资产: 2	
资产管理				
资产组管理		全部字段 * 搜索	操作系统 * mact地址 * > 1	10 III
止 策略模板		▲资产 ♀	✓ ●资产属性	编辑 🗡
■ 报表管理		 ★ □ ● 资产2 ★ □ ● 资产1 		
◎ 系统管理	2	田□ ● 默认资产组		

图19 新增资产

新增资产			×
资产目标		* 请填写资产目标,多个资产以逗号分隔。 主机资产填写示例: 192.168.1.1, www.baidu.com web资产填写示例: http://www.baidu.com/	
_頁 标签	添加一个标签	提示: 输入标签后按回车确定	
	提交		
● 默认资产组			

图20 口令猜解配置

🖵 任务中心	~	⊖ 新建任务				¢.
新建任务 任务列表		基本配置 高级选项				
探测未知站点 安全基线检测		新建任务类型 扫描目标方式	 ● 系統扫描 ● We ● 手动输入 ● 使 	b扫描 用资产	 ✓ 口令猜解 ○ 從最等入 	*提示:如句逸仅做基础探测,则不进行漏洞扫描,仅探测资产存活状态和端口开放情况
数据库检测 会话录制		扫描目标				* 扫描目标填写规范: IP44示例:192.168.1.100.IPv6示例: x000cc000cc000cc000cc000cc000cc000cc00
资产管理						域名示例: www.example.com URL示例: http://192.168.1.100/https://www.example.com/ http://icooccooccooccooccooccooccooc/
- 策略模板			此栏为必填项		4	排卵P或IP段: 1192.168.1.1/24.192.168.1.1-255.192.168.1.1 多个之间以英文逗号()或换行分隔
□ 报表管理		任务名称				*提示: 请填写任务名称,长度在[1-40]字符之间
◎ 系统管理		执行方式	立即执行	٣	*提示:请选择执行方式	
	_	口令猜解服务	TELNET, FTP, SSH, POP	P3, SMB	SNMP, RDP, SMTP +	*提示:选择口令猜解默认需要猜解服务类型。如需选择字典,请前往->高级选项->口令登
		执行优先级别		٠	*提示:当任务达到并发上跟时,"排队等待中"级别?	鸟的任务将优先执行
		分布式引擎	RtiA	٠	*默认: 系統将根据引擎的负载情况, 智能选择工作	弓]肇 local: 系统将会选择本地引擎
		告警模板	无	٣	●提示:告警发送配置,请到[系统管理>任务告警]"	下设置
			_			CPU停田本・1 50% 肉類停田本・124RMR/15957MR 適合使田本・33G/902G 人

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21 Cookie 认证信息获取

R	查看器	控制台	调试器 样式编辑器 性能 内存 网络 DOM		⊡->≡ ₽ 🌼
ŵ	所有	HTML	CSS JS XHR 字体 图像 媒体 Flash	WS 其他	④ 68 个请求, 2,297.92 KB, 9.80 秒
	状态	方法	文件	试名 原	海中头 Cookie 参数 脑灰 耗财 完全性
٠	200	GET	/dashboard/	document	
-	304		font-awesome	styleshee	hy Mun nttps //ugins/iont-awesome/css/iont
	304	GET		styleshee	请求方法: GET
۸	304	GET	UNITORING COLORISA	styleshee	远程地址: 〔
۸	304	GET		styleshee	状态码: ▲ 304 Not Moalliea 编辑和重发 原
۸	304	GET	mane percetteep	styleshee	版本: HTTP/1.1
۸	304	GET		styleshee	△ 妊娠湯首オ
۸	304	GET		styleshee	
۸	304	GET		styleshee	▼ 响应头 (118 子中)
۸	304	GET		styleshee	Etag: "W/"18079-1487154953000""
۸	304	GET	CIUCKIACE, CSS	styleshee	Date: "Thu, 01 Jun 2017 11:29:35 GMT"
۸	304	GET	· •	styleshee	Server: "RaySaas/1.6"
۸	304	GET		styleshee	▼ 请求头 (821 字节)
۸	304	GET		. styleshee	Host:
۸	304	GET	bootstrap-markdowriting a	styleshee	User-Agent: "Mozilla/5.0 (Windows NT 6.3; W) Gecko/20100101 Firefox/53.0"
۸	304	GET	Innin-soft rss	styleshee	Accept: "text/css,*/*;q=0.1"
۸	304	GET		styleshee	Accept-Language: "zh-CN,zh;g=0.8,en-US;g=0.5,en;g=0.3"
۸	304	GET	emenoem, CSS	styleshee	Accept-Encoding: "gzip, deflate, br"
۸	304	GET		styleshee	Referer:
۸	304	GET	ine.cou	styleshee	Cookie: "ISESSIONID=REFE3CC+1958E5221A4_s8x9alb5uassa26ava6bac92araba"
۸	304	GET		v styleshee	Connection: "keen-alive"
۸	304	GET	customue	styleshee	If Modified Since: "Wed 15 Feb 2017 10:35:53 GMT"
۸	304	GET	he3.css	styleshee	If North Methy 2017 10 2017 10:00:00 101
	304	GET	June ,	o script	Code Coded "www.com.of"
۸	304	GET	·····te-1.2.1.min.is	script	Cache-Control: max-age=0
۸	304	GET	2	script	
۸	304	GET	br	script	
	304	GET	tw	script	

图22 Cookie 信息填写

❷ 资产管理				新增资产+				
盐 资产组	捜索[回车] >	● 资产详情		~				
		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/					
─────────────────────────────────────		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		Б.				
		上传网站证书	浏览 未远择文件。	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23 Post 请求发送数据

	bWA	PP is licen	sed under ((a) ev-NO-ND	@ 2014 MME BVBA /	Folow <u>@M</u>	<u>MELIT</u> on	Twitter and	ask for o	ur cheat sheet, ci	ontaining all solutio	ons! / Need ar	1 exclusive <u>training</u> ?					
R														Х			
Û	所有 🖡	ITML CSS	JS XHR 字体图像:	媒体 Flash WS 其他	□ 持续日志	. ○ 禁用	渡存								♡ 过滤 URL	Į	7
3	挞	方法	文件	嫏	原因	翅	(輸	大小	0 毫秒 80 毫	眇 160 勤	240 翹	消息头	Cookie	参数	响应	耗时	
4			login.php	🔏 183.1.3.102	document	html	23.41 KB		l → 8 ms			请求网址: http://1	83.1.3.102/bWAPP/	login.php			
•	200	GET	pontohp	🔏 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	已緩存	2.34 KB				远程地址:183.1.3.	102:80				
												状态码: ▲ 302 Fou	nd ⑦ 编辑和重发	原始头			
				nonk主隶								版本: HTTP/1.1	_	_			
				pusilll小仪应效加								♡ 过滤消息头					
) 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24 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25 Form 认证配置

□ 新建任务	5			
基本配置	高级选项			
系統扫描 WEB扫描 口令猜解 存活探测	登录扫描 引擎选项 检测选项	起始URL 其他URL 网站域名 扫描根目录 例外URL 登录认证 提交URL 提交数据	FormULIE	 ・ ・ ・
		上传网站证书 上传网站证书密码	选择文件 未选择任何文件	浏览酬客户续证书,如PFX/PKCS12等格式 导出证书时设置的密码

(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26 Basic 配置

白 新建任务	5			0
基本配置	高级选项			
系統扫描	登录扫描			
WEB扫描	引輩选项	起始URL		
口令猜解 存活探测	检测选项	具他URL 网站域名 扫描根目录 例外URL 登录认证 用户名	BasicU.E	 ▼ ◆ 登录验证
		密码 上传网站证书 上传网站证书密码	选择文件	浏览器客户端证书,如PFX/PKCS12等格式 导出证书时设置的宏码

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"。

□ 新建任	务			0
基本配置	高级选项			
系统扫描	探测选项			
WEB扫描		友包速率	○ 快速 ○ 正常 ○ 慢速 ④ 自适应 ○ 自定义	快速:単ip300004/s 止常:1500包/s 慢速:1000包/s 自定义:单个ip在100-5000包/s 范围
口令猜解		主机存活探测	×	
存活探测			✓ ARP	
			✓ ICMP PING	
			V TCP PING 21,22,23,25,80,443,445,139,3389,6000	
			UDP PING 25,53,161	
		端口扫描范围	 ● 标准 ○ 快速 ○ 全部 ○ 指定 	标准: 新认确口2000多个,快速:1000个常用)通口,全部: 请口1-65535 描注: 单个或范围如22,1-1024指定TCPI图口: TCP:1024-65535,指定 UDPI第口: UDP:1025-65535, 查信由下载,了解调口详情,
		TCP講口扫描方式	CONNECT V 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27 查看站点网页数

吉果详情						返回任务列表
网站列表 淵源	副列表 漏洞目录树	历史执行记录				WEB扫描详情
ф 		~	风险级别	漏洞名称	总计	网站域名 http://192.168.0.114:5357/
http://192.16	8.0.114:5357/	•	中风险	域名访问限制不严格	1	IP地址 192.168.0.114
			低风险	X-Frame-Options头未设置	1	网站跟 Microsoft-HTTPAPI/2.0
			信息	服务器版本信息泄漏	1	网站标题 ServiceUnavailable
			总计3条记录	每页显示 2	5 ▼ < 1 >	网站编码 us-ascii
						网站物 局域网-对方和您在同一内部网[192.168.0.0-192
					-	网页总数 1
						漏洞风险分布
						■ 25.948(0) ■ 49.848(1) ■ 45.846(1) ■ 45.846(1) ■ 45.846(1)

虚拟漏扫中CPU使用率、内存使用率、磁盘使用率为何与cas上显示不同。

漏扫中 CPU 使用率、内存使用率、磁盘使用率的计算方式为: top -bn1 | grep load |awk '{printf "CPU Load: %.2f\n",\$(NF-2)}' free -m | awk 'NR==2{printf "Memory Usage: %s/%sMB (%.2f%%)\n",\$3,\$2,\$3*100/\$2}' df -h | awk '\$NF=="/"{printf "Disk Usage: %d/%dGB (%s)\n",\$3,\$2,\$5}' 注:漏扫的磁盘占用为日志分区占用,不包含根分区。

图28 虚拟漏扫

kensettit	10042	
1819	6.865	9 (840(885)
	451.5710	C ing
	N-TERS	MAGE
	12.69454	2022-04-12
	H-TUERENTA)	2022-06-09
	最大P数	光微和
	并发系统扫描任务数	4
	任务师发产业绩	200
	最大站市政	ALEN .
	ASSIMILATION	1
	开发口令情解散	2
	8038	ла
	KERON (H-KERONIK)	0

图29 Cas

云资源 / 主机;	食豪/主切胞:smantcard/主切:cvknode/ 虚拟机:scanVE3-183.101.1.62									
● 启动	🕐 安全关闭 🕴 关闭电源 🔗 修改的	虚拟机 🖸 技術台 👔 境路 📝 迁移 🔯 快照管理 🗙 勤齢 ・・・・ 更多操作 ▼								
⊟ 概要	會 性能监控 全 进程服务监控	ရ 省份管理 🖂 控制台 🕥 迁移历史 🔹 任务								
基本属性		硬件信息								
显示名称	scanVE3-183.101.1.62 🔗	CPU配置: 4x1 内存: 8.0GB 容量: 80.00GB								
描述		CPU CPU利用率: 内存利用率: 总线类型:高速								
主机	cvknode [183.1.1.13]	2.30% 80.46% 存储路径: /vms/images/scanVE3-18								
状态	₩2)运行									
操作系统	Linux 👌	MAC地址: 0c:da:41:1d:5e:3f 察量: 2.07GB 留量: 0.00MB								
版本	Debian GUN/Linux 7(64位)	PV4地址: 183.101.1.62 D2 总线类型: IDE 意线类型: FDC 方体略 G た体験 G								
存储	80.00GB	vuonin in triageno ://insumages/Sectramista (†18,890 :								
CAStools	(1) 未运行									

SysScan-SE/AK810款型设备上插上四万兆插卡,web界面禁用万兆光口,显示为down的状态,但设备指示灯仍微亮。

X710&XL710网卡芯片问题,物理实际为 down,可根据漏扫界面端口状态判断端口状态。

SysScan-VE款型漏扫启动后登录web界面,查看机器码和授权不会立即显示。

SysScan-VE 款型漏扫启动后登录 web 界面,查看机器码和授权不会立即显示,由于 agent 服务启动需要一段时间,请耐心等待 5 分钟左右。

基线核查的离线任务进行ipv6地址检测为何失败。

离线方式进行 ipv6 地址基线核查时, 需要 ipv6 地址格式中冒号改为-, 例如 2001:183:1:1::2 应配置为 2001-183-1-1--2。

新建任务后后删除该任务,再建同名任务,资产处该同名任务信息后缀为6位数字代表含义 是?

后缀表示为该任务建立时间。

系统管理>网络接口, IP管理配置中vlan名称和默认MngtVlan表示为vlan还是网桥?

漏扫中表示为网桥的含义。

≓ IP管理配置	▲ 接口配置 ☆ 路由配置 ■	E DNS配置	É	自动DHCP+ 新增+	刷新 ○ 搜索[回车]	
VLAN名称	▼ IP地址	子网鵙码	Mtu	状态	操作	
MngtVlan	192.168.0.1 192.168.13.177	255.255.255.0 255.255.255.0	1500	启用	编辑✔ 删除★	
总计1条记录						< 1 >

使用系统插件中自定义策略模板进行扫描时,为何还会扫描出非自定义策略中漏洞呢?

使用自定义策略模板扫描时,会自动执行相关联漏洞,导致不在策略模板中漏扫也可以扫描出来,属于正常检测范围。

系统时间是否会影响授权时间?

导入授权前请先查看系统时间,确保时间正确,否则会影响授权使用

系统支持删除资产以及资产组吗?

E6202P04版本以及之后版本支持对资产组的删除,E6202P04之前版本不支持

账号忘记密码如何处理?

1、Account 账号忘记密码需要通过登录漏扫串口,执行 resetpwd 命令,将 web 界面 account 账户 的密码恢复为默认密码。注意:此命令需要在串口下操作!SSH 登录时不可执行此命令。(此 命令在 E6202P05 版本以及之后版本支持)

Welcome to H3C-OS h3c-os login: admin nsc-os login: admin Password: Last login: Wed Jun 1 02:07:29 CST 2022 on ttyS0 Welcome to H3C-OS [h3c-os]\$ resetpwd Reset ok! [h3c-os]\$ ■

1)硬件通过串口线进入串口

2) 虚拟漏扫需要安装所在服务器 et 后台执行 virsh console (虚拟机名称)命令,进入虚拟串口, 点击 enter 键登录



输入登录用户名密码 admin/admin,即可登录成功

root@cvknodel3:~# virsh console scan-Cloud-183.101.1.44 Connected to domain scan-Cloud-183.101.1.44 Escape character is ^] Welcome to H3C-OS h3c-os login: admin Password: Last login: Mon Jul 11 17:30:57 CST 2022 from 101.1.18.18 on pts/0 Welcome to H3C-OS [h3c-os]\$ [h3c-os]\$ [h3c-os]\$

备注: 出现连接报错时, 如下图情况:

error: command 'console' requires <domain> option [root@cvknode-83 ~]# virsh console scan-arm-183.1.4.77-E6202P06 connected to domain scan-arm-183.1.4.77-E6202P06 [scape character is ^] error: operation failed: Active console session exists for this domain

[root@cvknode-83 ~]#

eadv

是因为串口登录限制,有别的活跃连接在登录漏扫的串口,执行 virsh console 虚拟机名称 –force 强制连接,进入串口。

2、其余管理员忘记密码可以登录 account 账号进行密码重置,重置后密码与管理员用户名一致

测 0	号管理	用户管理 ≡ 用户根	又限模板	编辑!	删除 ×	解除锁定■	正置の	新增+	刷新2	搜索[回车]	0
	用户名		用户权限模板		最近登录日期		状态	是否	锁定	登录超时 (分钟)	
	admin	[默认用户]	高級管理员功能组		2022-05-16 11:	55:51	启用	否		30	
	audit	[默认用户]	审计管理员功能组		2022-05-10 14:	24:42	启用	否		30	
	report	[默认用户]	报表管理员功能组		2022-04-20 09:	38:30	启用	否		30	
~	user1		普通管理员功能组				启用	否		30	

设置信任ip后,无法访问web页面如何处理?

连接串口或控制台,使用 admin 管理员登录, adminlan –S 可查看当前配置的信任 ip; adminlan -A 0.0.0.0/0 可用于增加信任 ip; adminlan -D 0.0.0.0/0 可用于删除当前信任 ip;adminlan –F 可用于清 空当前配置。

系统出现CPU、内存超高告警如何处理?

请根据系统当前系统负载判断,是否已经达到阈值,可以登录 account 管理员,在告警配置中调整 告警阈值

升级软件版本至 E6202P02 及之后版本,升级特征库至最新发布版本,升级稳定运行后再观察如上述办法无法满足,请联系研发处理

系统出现升级卡顿,升级时间过长如何处理?

升级时间在 30 分钟到 1.5 小时不等,根据产品负载和型号不同而不同,请耐心等待,设备重启 后,页面无法访问并展示进度,可查看串口打印,当串口再次出现 login 页面后,刷新浏览器,当 浏览器出现登录页面,升级完成。

如存在页面升级卡顿在某一进度时间过长(超过上述时间),如网络延迟大导致升级包上传更新卡在某一进度,可联系研发使用后台进行升级。

系统网卡初始化后如何恢复?

Initnetwork 后系统会自动关机,需要手动启动 ip 地址被初始化为 192.168.0.1,请使用该地址访问 web 页面,并重新配置管理地址。

Account账号下License管理已经使用IP和剩余IP是如何统计的

根据扫描到的资产的实际情况判断,资产在线且存在扫描结果会自动+1 资产,删除资产-1 (删除资 产在 E6202P04 以及以后版本支持)

如下发的是一个网段或多个 IP 的扫描任务,系统会先按照下发的 IP 数量(所有 ip)进行授权统计,但不体现在 account 账号 license 统计,等扫描结束会在 account 账号根据实际在线情况进行 license 统计。

Web扫描任务,通过点击任务详情,再直接点击漏洞目录树展示是空的?

目前设计如此,查看漏洞目录树需要通过如下方式查看:点击 web 任务详情的网站列表下的网站结构,跳转到漏洞目录树。

Ģ	任务中心	结果	详情							
	新建任务		站列表 漏洞列表	漏洞目录树	历史执行记录				WEB扫描详情	i
	任务列表	з	主机名称	1.	检测进度	漏洞风险分布		攝作	网站域名	https://183.1.3.118:8443/
	安全基线检测 探测未知站点		网站结构 🚠 https://1	编结构 击 https://183.1.3.11 100% 1	1	8	重新检测 🕽 日志下數之	IP地址	183.1.3.118	
	数据库检测	息	计1条记录					毎页显示 25 ▼ < 1 >	网站服	nginx
	会话录制								网站标题	H3CSecCenter终端安全管理系统
0	资产管理								网站编码	utf-8
ė.	策略模板								网站物	广东省广州市-电信[183.0.215.0-183.1.25.

Cloud&Ve型号漏扫增加是否支持多网卡,增加网卡后是否需要重新启动漏扫?

支持多网卡, 增加网卡后需要重启才能生效。

windows密码破解出任意用户名任意密码是什么意思

密码破解具有协议版本局限性如口令猜解 RDP 协议仅支持: windows 7、windows 8、windows server 2008;其余操作系统不支持,进行破解结果不准确,存在出现任意用户名、任意密码的可能性,请根据实际情况判断。

新架构(E6202P05版本以及之后版本)漏扫的资产和资产组是怎么使用的?

架构变更后资产和资产组做了分离,应该先增加资产组,并配置资产组范围,再新增该范围的资产时,将自动划入资产组内,扫描结果也会归入该资产组的资产目录下。未新建资产和资产组进行扫描时将会把扫描结果归入默认分组下,新增资产组未新增资产也会将资产扫描结果归入默认分组下。

使用会话录制页面操作卡顿如何处理?

会话录制中录制的 URL 数量过多的话,在解析 URL 的过程会造成页面卡段,建议一次录制较少数量 URL,分批多次录制。

NTP同步后,时间不正确可能什么原因导致的?

排查 NTP 服务器时区和时间是否正确,修改 NTP 服务器时间时区与北京时间一致。

扫描过程中出现扫描设备或其他主机与漏扫之间无法Ping通,扫描结束后可以ping通,出现 此现象原因是什么?

一般由于被扫描设备与漏扫之间有防护设备,漏扫在扫描过程被防护设备拉黑导致,扫描结束可恢复。

临时授权的时间扩容和功能扩容以及IP扩容分别怎么使用?

临时授权功能使用到期后,需要使用基础功能授权函进行时间扩容,即系统功能授权函,功能扩容 使用相应功能进行扩容,如 web 扫描功能等,IP 数量扩容使用 IP 授权函进行扩容。 正式授权不涉及基础功能时间扩容,涉及特征库扩容、IP 扩容和功能扩容。

自定义用户可以看到admin账号下新建的资产吗?

不可以,资产分离,只能看到自己账户下新建的资产。

使用资产方式添加扫描目标时提示"不允许添加特殊字符",资产示例"10.0.254.1(admin)", 出现此种情况如何解决?

清空浏览器缓存重新下发,或者更换谷歌 90 版本以上的浏览器。

恢复出场设置以及初始化后, 会关闭设备吗?

会的, 需要手动启动。

编辑任务,未修改扫描目标却提示未验证通过,格式不正确是什么原因?

确认任务来源,如果通过导入资产或者引用资产/资产组生成的扫描任务,扫描目标的格式要求与手动输入框不一致,且前两种方式没有长度限制,此时编辑任务,会对扫描目标进行校验,如果不满 足手动输入框校验条件就会报错。

已经提交的扫描任务再次编辑未修改扫描目标的前提下,为什么会报扫描格式和扫描长度的 错误?

此种情况下扫描目标是通过导入或者引用资产等其余方式新增的,这些方式对扫描目标是没有限制 的,而再次编辑会校验扫描目标的输入框,需要满足格式和长度要求,导致报错。此时需要重新建 立扫描任务,来修改扫描参数。

扫描后查看被扫描目标的操作系统或者版本与实际不符,怎么处理?

需要进行登录验证扫描,如 windows 可以使用 SMB 协议登录, linux 可以使用 SSH 协议登录扫描。 非登录扫描是通过暴露的 banner 信息获取版本信息, banner 信息隐藏,或者有防火墙等导致返回的 banner 信息不明显等情况,都会导致识别不准确.登录扫描是底层命令执行 linux 本身共有的命令(通 用的 linux 命令),获取系统的版本,登录扫描收集的信息会更多,收集的信息越多,识别的越准确。

扫描任务列表的历史执行记录的日之下载打不开?

该日志为研发定位问题使用,密码不对外。

在系统扫描中,检测选项里的启用口令破解与使用口令破解模块有什么区别且在口令破解功 能里,分为组合模式和标准模式,这两种模式分别是什么,在扫描速度上和对系统的影响上, 有什么区别?

1、启用口令破解是默认开启的,使用的是规则库中的插件进行口令破解,没有口令字典那么全,如果需要专门扫描弱口令,建议使用口令猜解;
 2、组合模式对应的就是组合字典,"用户名:密码"格式,猜解的时候就是按照组合字典猜解,标准模式同理,是指用户字典和密码字典需要分开选择,可以选择默认用户民,自定义的密码字典;或者自定义的用户名字典,默认密码字典;或者全部选自定义;
 3、两种模式区别不大,主要看什么时候匹配到用户名和密码。两种字典数量同样多的情况下,标准模式相对来说较慢,一个用户名匹配密码字典中的密码后下一个用户名再进行匹配。

授权服务器导入申请的授权提示厂商信息校验错误是什么原因?

授权码使用错误导致,请校验授权的厂商信息是否是 UNIS。

激活Cloud漏扫的授权服务器授权时,提示"SCAN一年订阅版不可以申请临时授权"

授权码使用错误导致,一年版授权不能申请临时授权,请使用永久订阅函申请临时授权。