UNIS XSCAN-CN80 系列漏洞扫描系统

用户 FAQ

目 录

本文档介绍 UNIS 漏洞扫描系统中用户常见问题及解答。

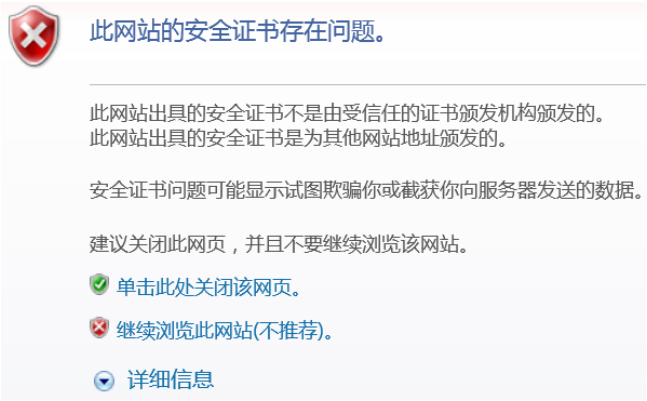
1 常用配置类 FAQ

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

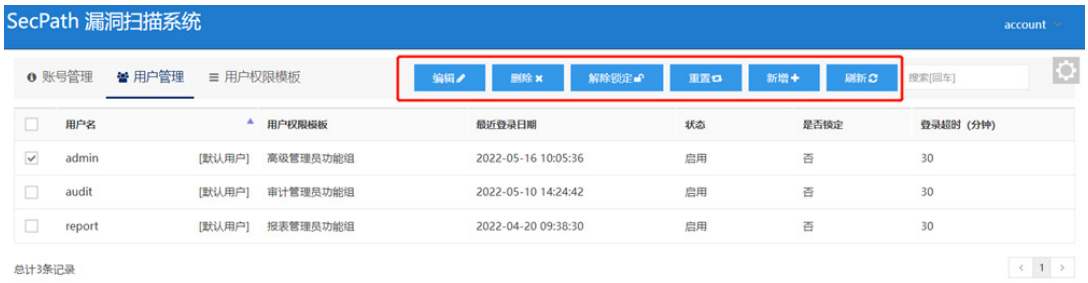


admin账户登录密码忘记，账户被锁定。

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

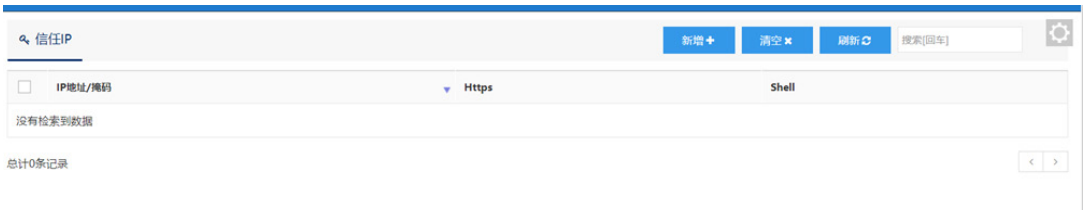


内网的地址无法管理设备，可Ping通，Web界面和SSH均不能登录。

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



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

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

2 业务功能类 FAQ

添加扫描任务有几种方式?

三种：

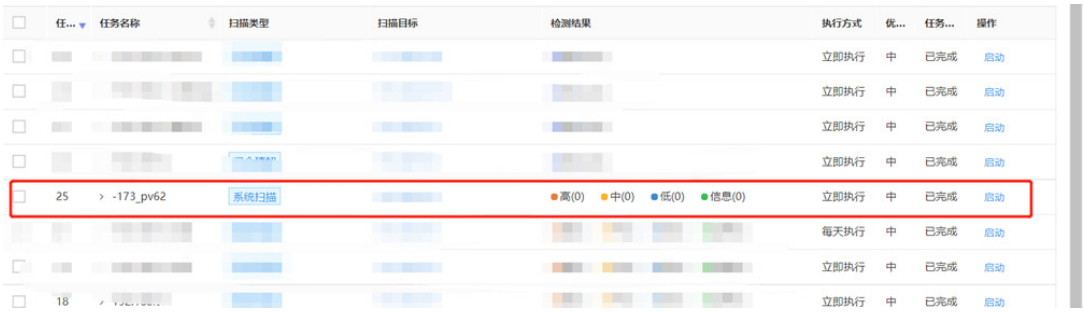
- 手动输入：可一次输入单个或多个主机。
- 使用资产列表。
- 批量导入：下载 Excel 表格，按照模板填写上传。

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



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

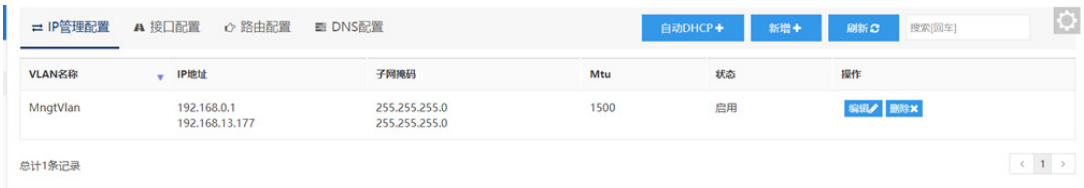


图8 路由配置

(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

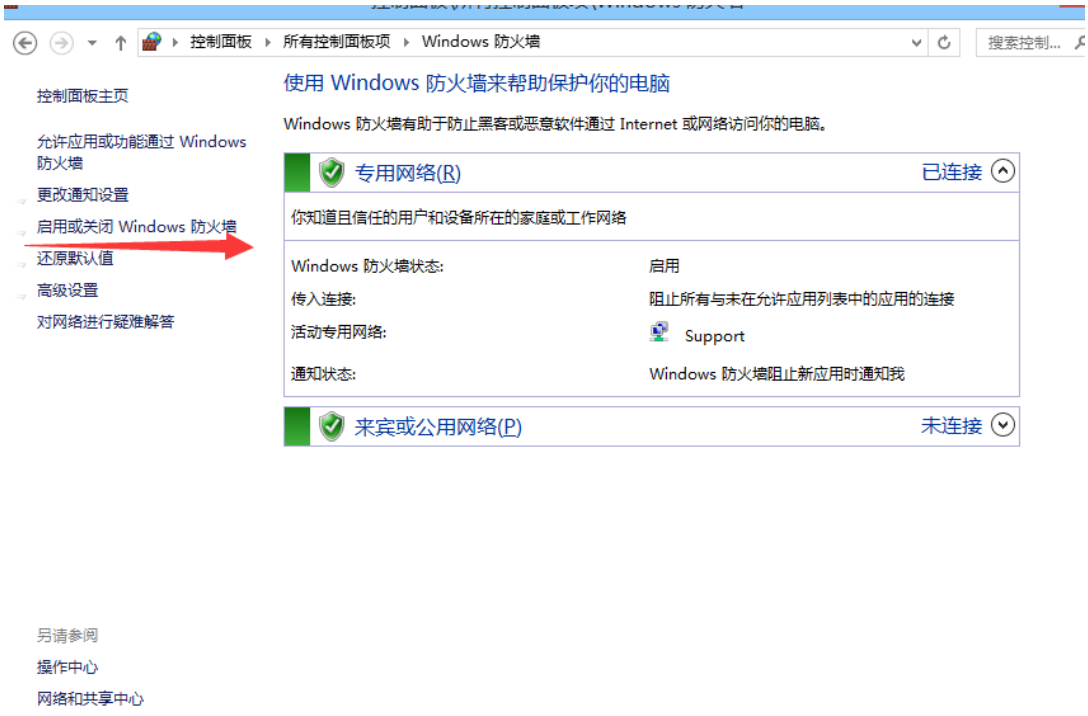
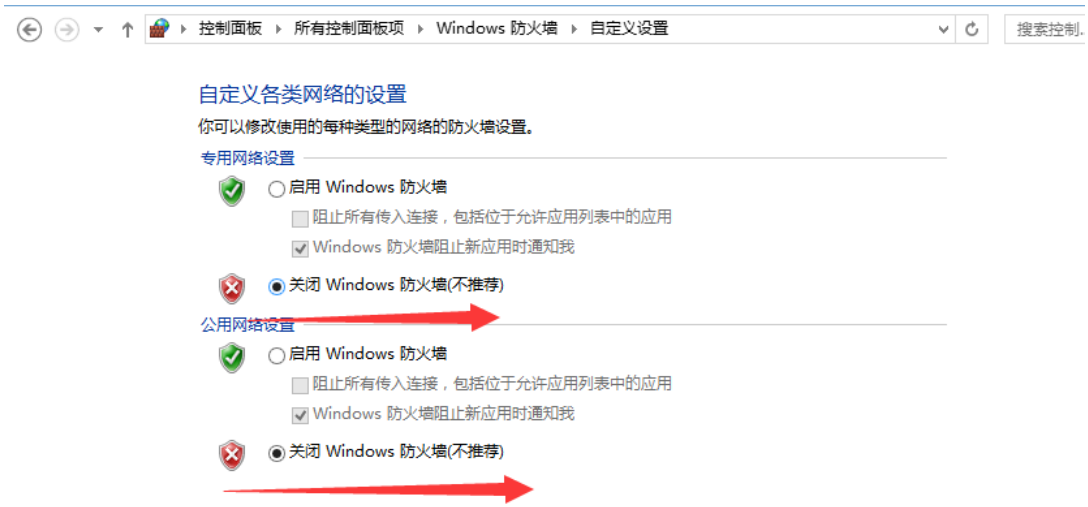
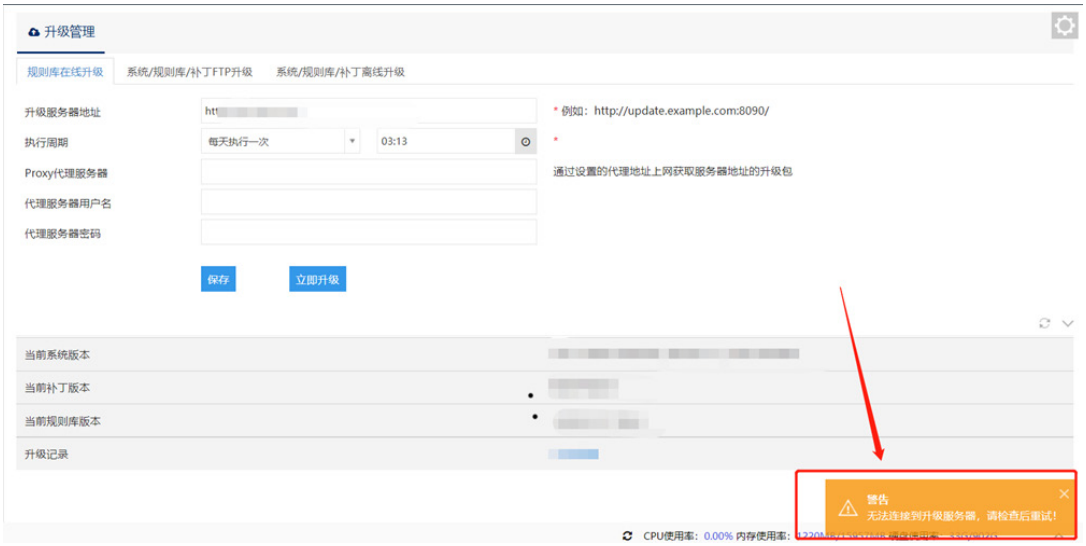


图11 关闭防火墙



规则库升级失败，提示升级失败。

图12 规则库升级失败

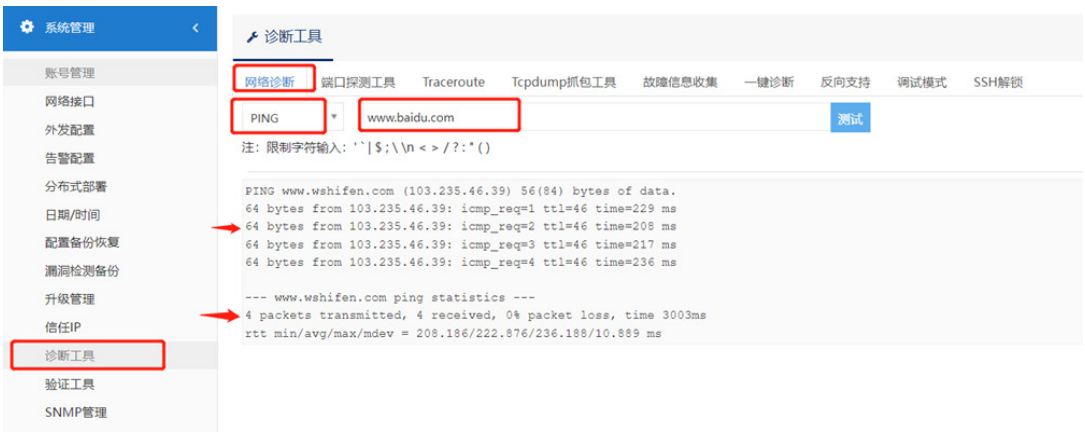


原因：网络地址不可达；升级服务器地址错误。

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



(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/。

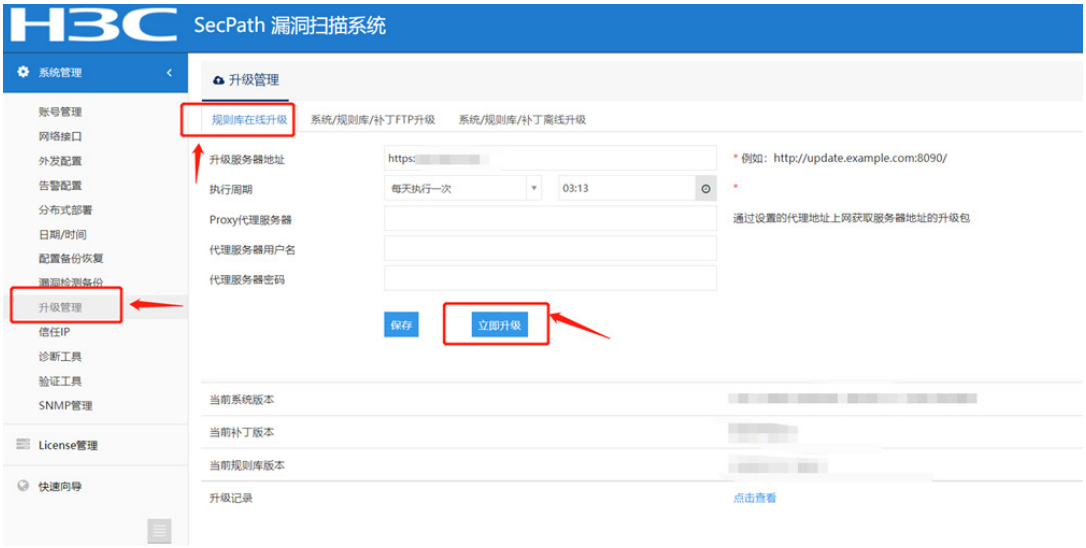
如何进行升级以及升级注意事项。

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



(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

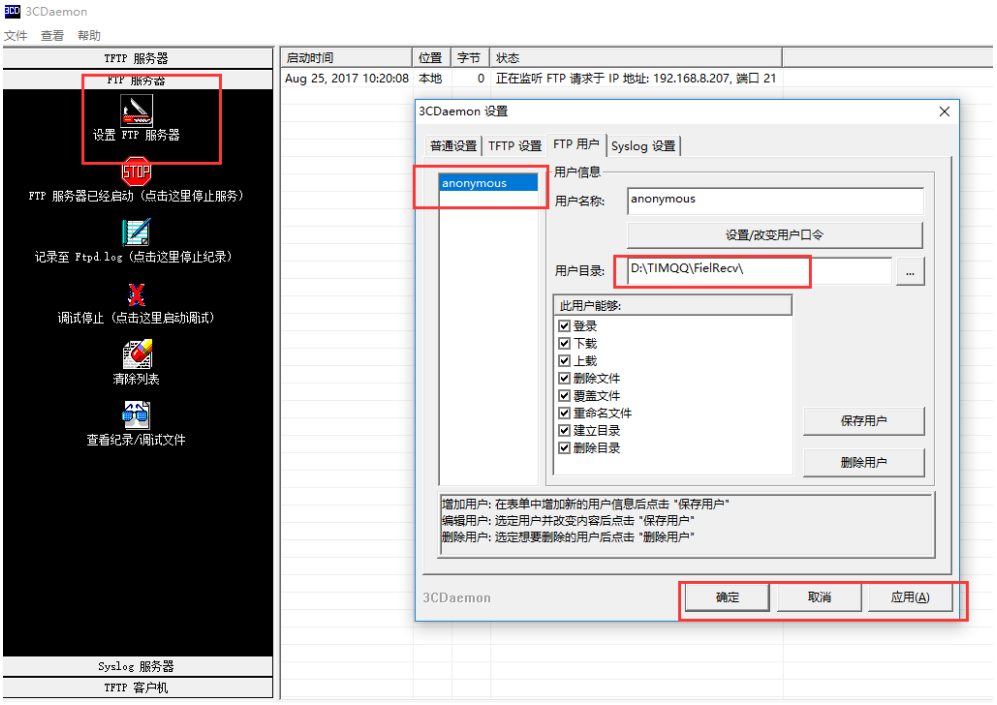


图16 手动升级

(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

(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

图19 新增资产

图20 口令猜解配置

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

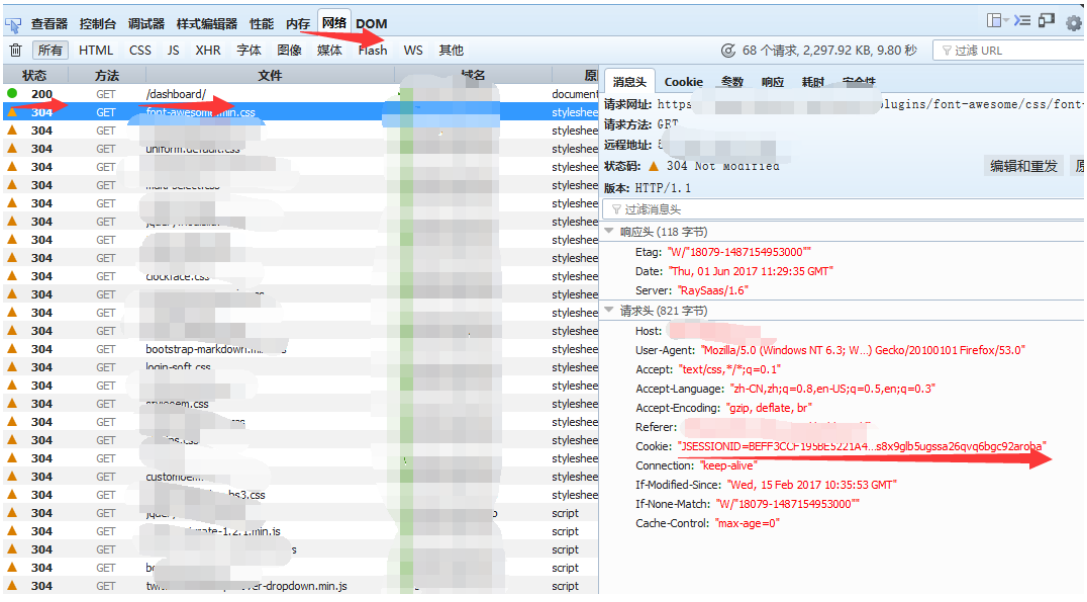
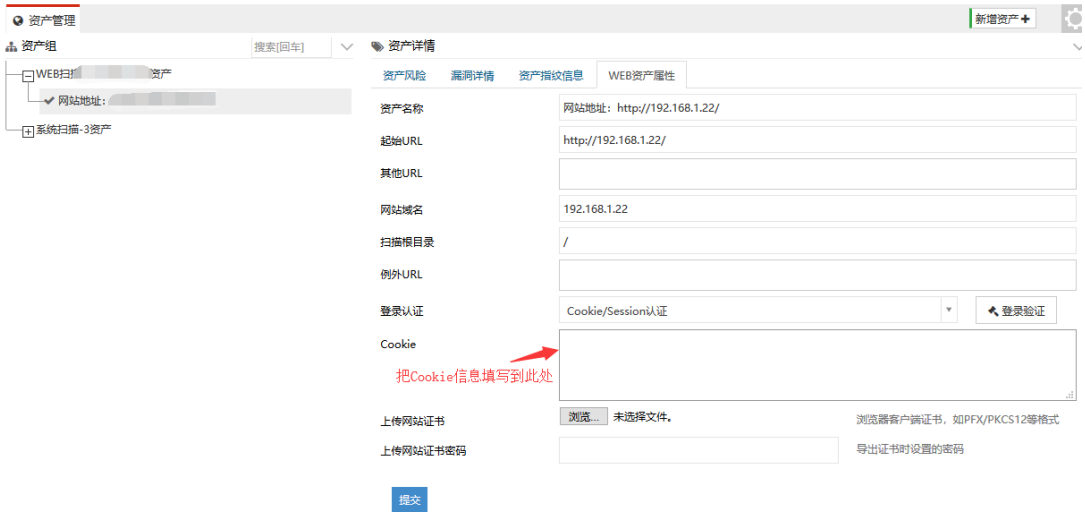


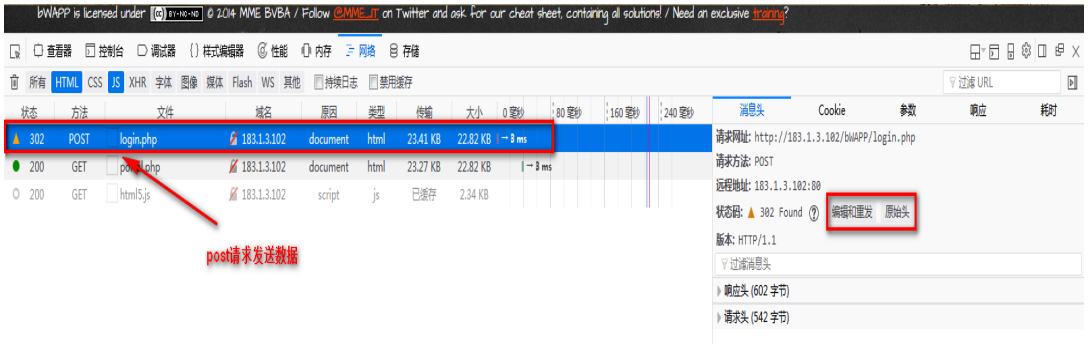
图22 Cookie 信息填写



(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

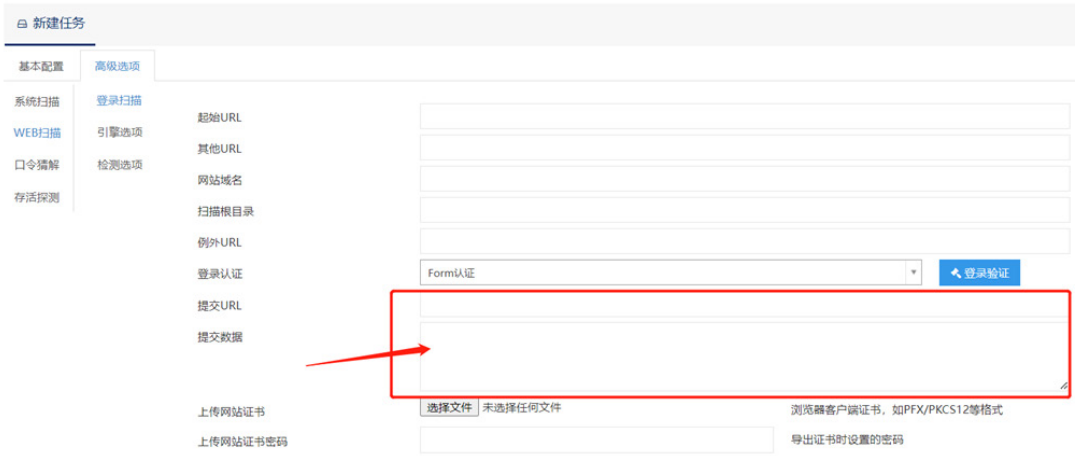


点击编辑和重发，看到 Post 请求头内容，可以用于网站认证时使用。

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

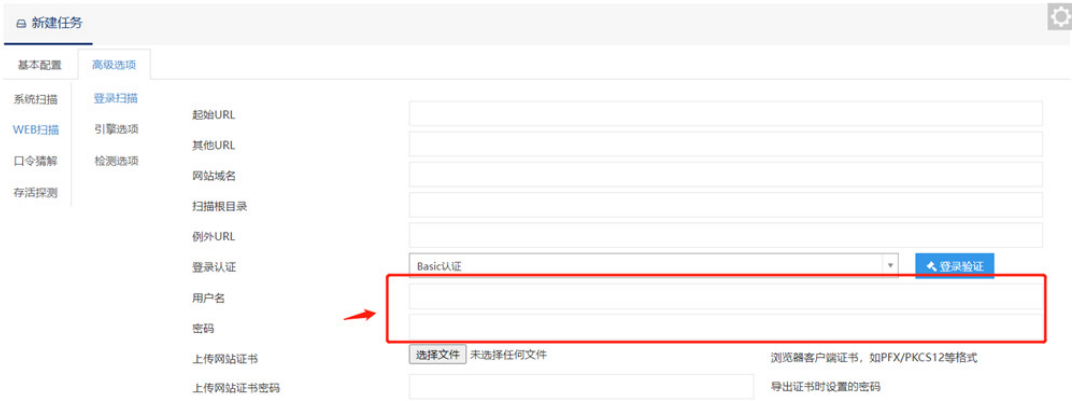
图25 Form 认证配置



(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

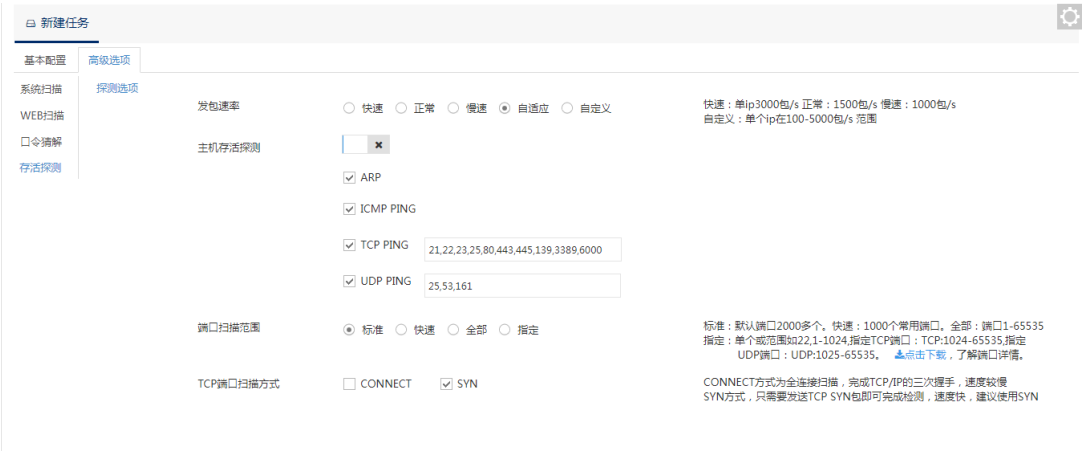


Web扫描扫不到页面。

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”。



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。

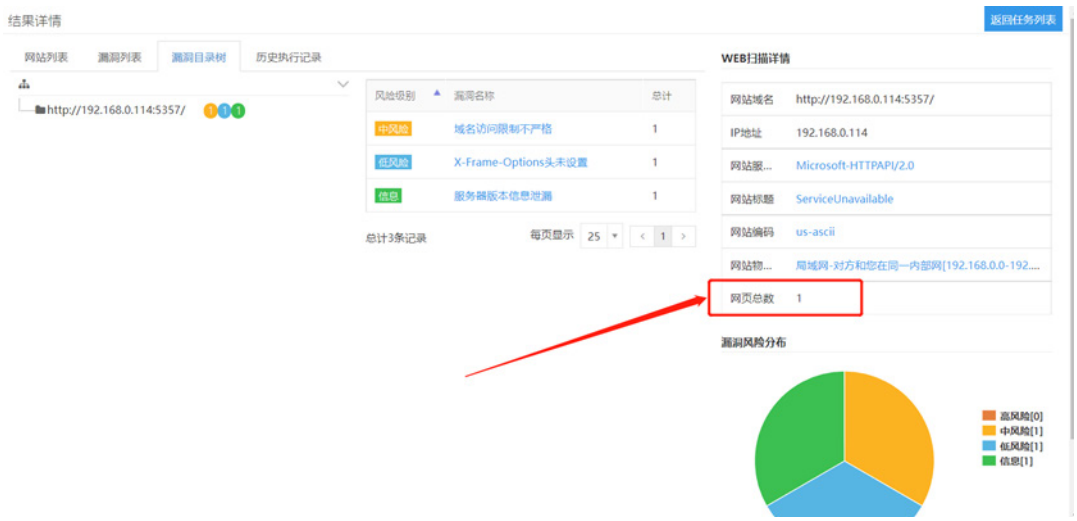
正常扫描和系统登录扫描（验证已登录成功），扫描结果没区别。

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



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

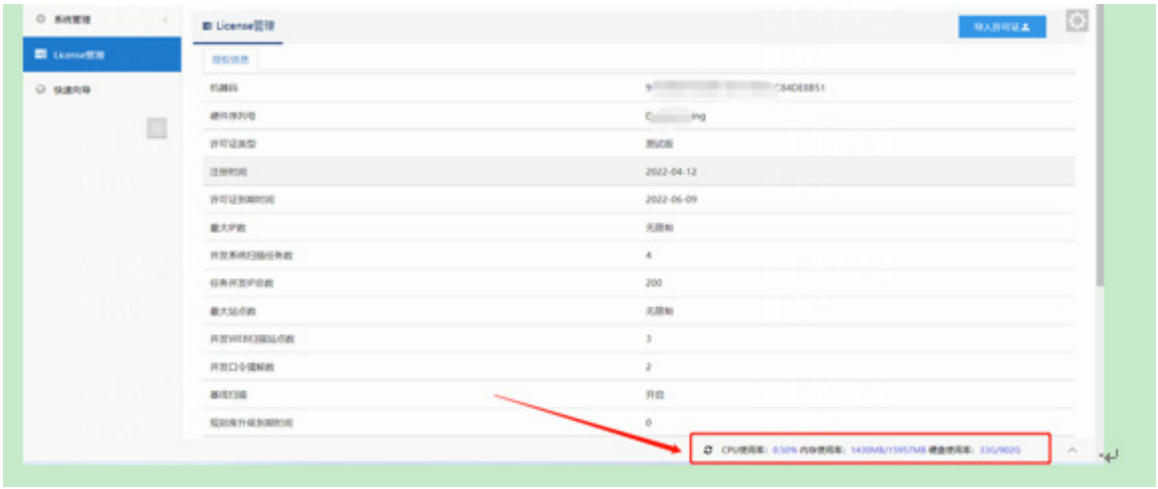


图29 Cas

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。

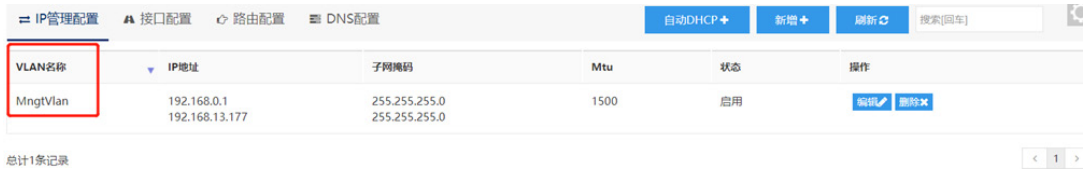
离线方式进行 ipv6 地址基线核查时，需要 ipv6 地址格式中冒号改为-，例如 2001:183:1:1::2 应配置为 2001-183-1-1--2。

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。



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

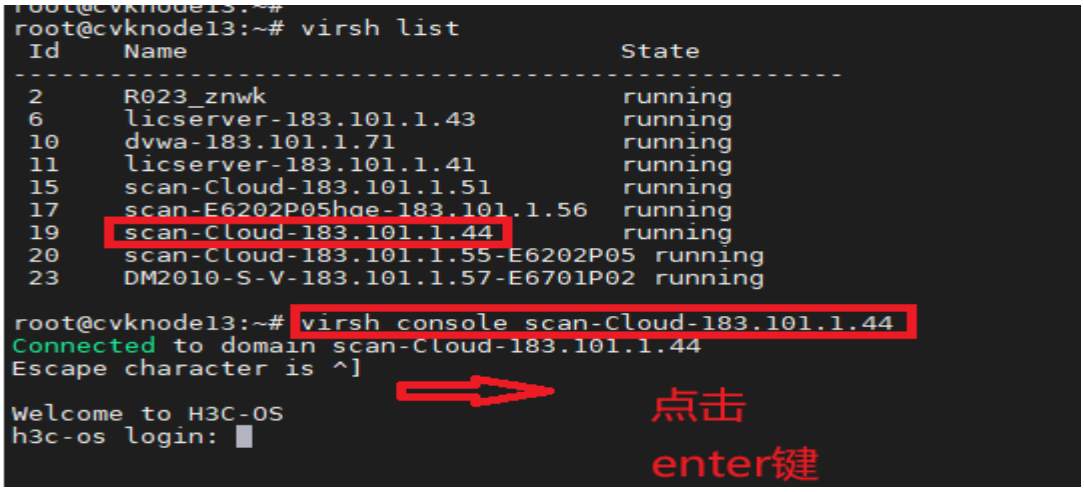
账号忘记密码如何处理？

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）

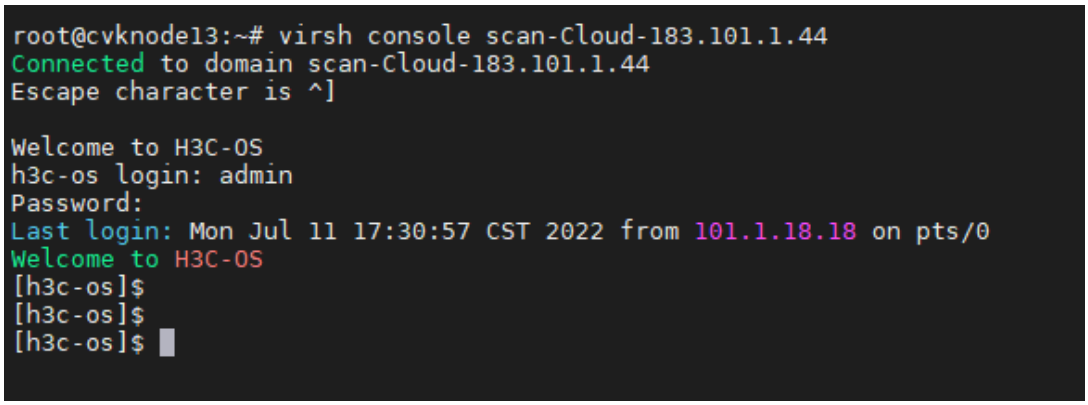
```
Welcome to H3C-OS
h3c-os login: admin
Password:
Last login: Wed Jun  1 02:07:29 CST 2022 on ttyS0
Welcome to H3C-OS
[h3c-os]$ resetpwd
Reset ok!
[h3c-os]$
```

1）硬件通过串口线进入串口

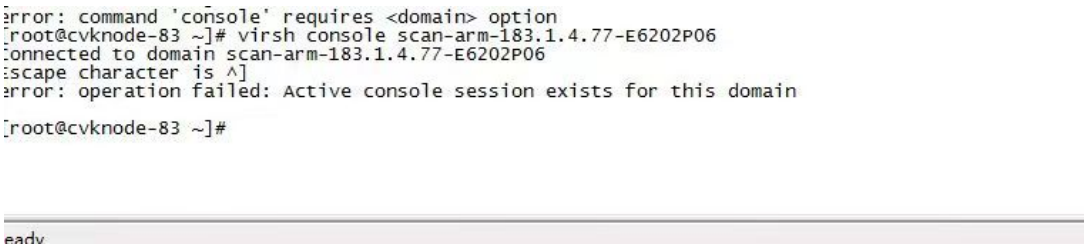
2）虚拟漏扫需要安装所在服务器 et 后台执行 virsh console （虚拟机名称）命令，进入虚拟串口，点击 enter 键登录



输入登录用户名密码 admin/admin，即可登录成功

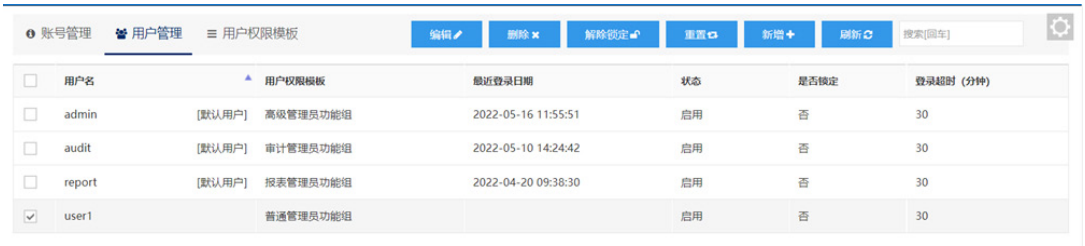


备注：出现连接报错时，如下图情况：



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



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。

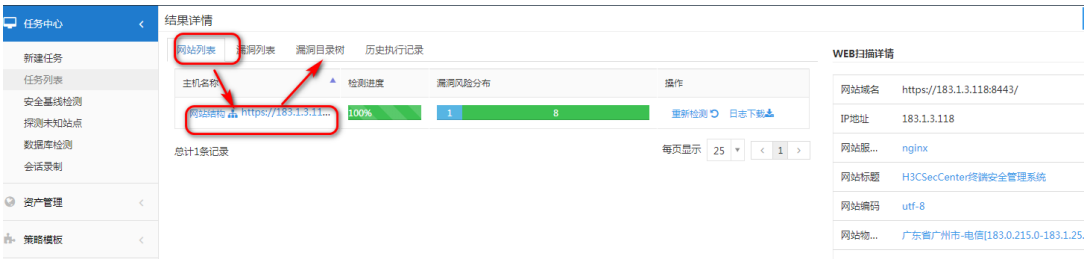
Account账号下License管理已经使用IP和剩余IP是如何统计的

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。



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。