Supernova 测试仪
并发扫描检测配置手册

网测科技

2021/01/22

目录

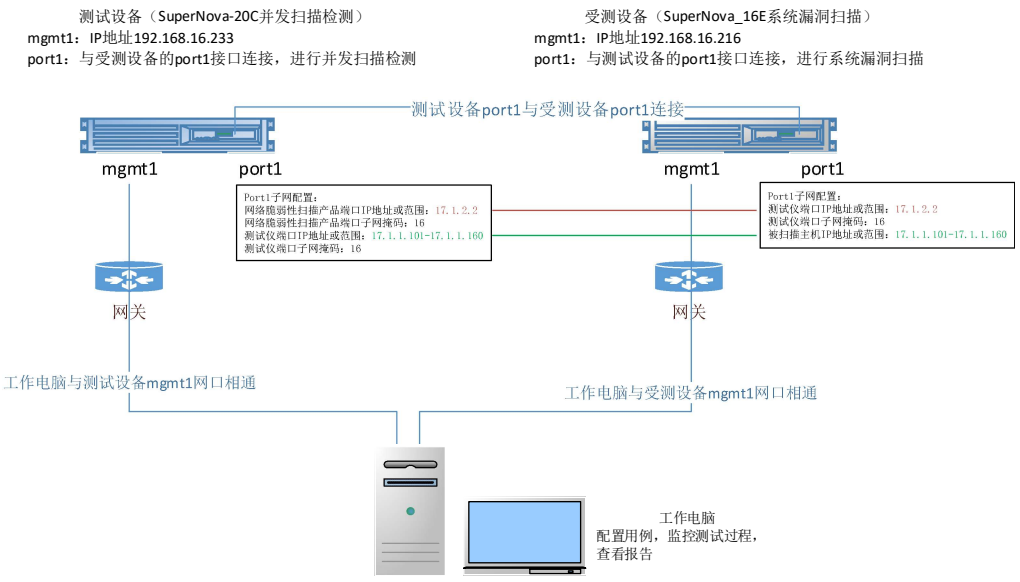
1. 文档说明

根据国家发布的《网络关键设备和网络安全专用产品目录（第一批）》（http://www.cac.gov.cn/2017-06/09/c_1121113591.htm），要求网络脆弱性扫描产品最大并行扫描 IP 数量大于等于 60 个，Supernova 系列测试仪并发扫描检测用例，支持对网络脆弱性扫描产品最大并行扫描 IP 数量进行检测认证。检测对象适用于利用扫描手段检测目标网络系统中可能被入侵者利用的脆弱性的软件或软硬件组合。

本文档主要介绍并发扫描检测的配置和测试过程。随着需求的不断改变，可能会对用例配置进行修改和升级，从而改变配置过程，所以有任何问题，请联系我们的售前或售后支持人员。

2. 网络拓扑

Supernova 系列测试仪本身支持系统漏洞扫描功能，故本文档将以一台 26E 为受测设备运行系统漏洞扫描用例扫描目标主机、一台 20C 为测试设备运行并发扫描检测用例对并发扫描 IP 数量进行统计检测为例，说明整个配置和测试过程。为了便于理解整个配置和测试过程，网络拓扑如下所示：



3. 配置过程

从第 2 章的网络拓扑中可以看出，需要在 26E（模拟受测设备）上创建一个系统漏洞扫描用例，在 20C（测试设备）上创建一个并发扫描检测用例。

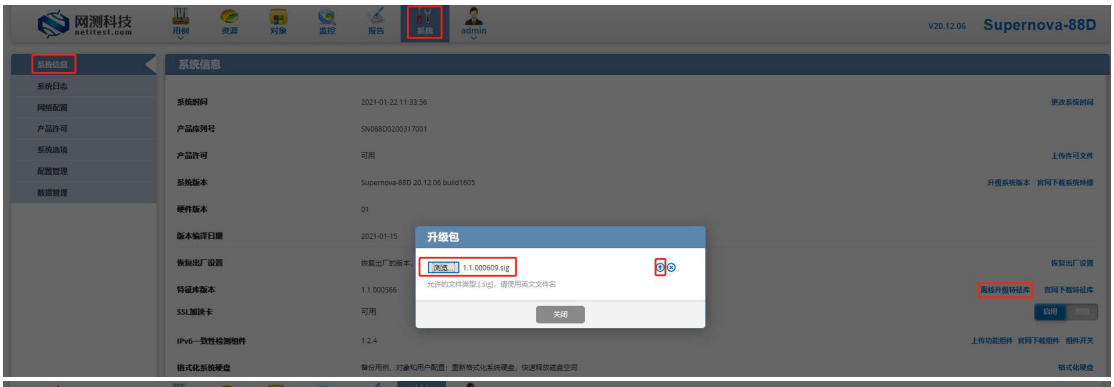
3.1 配置受测设备

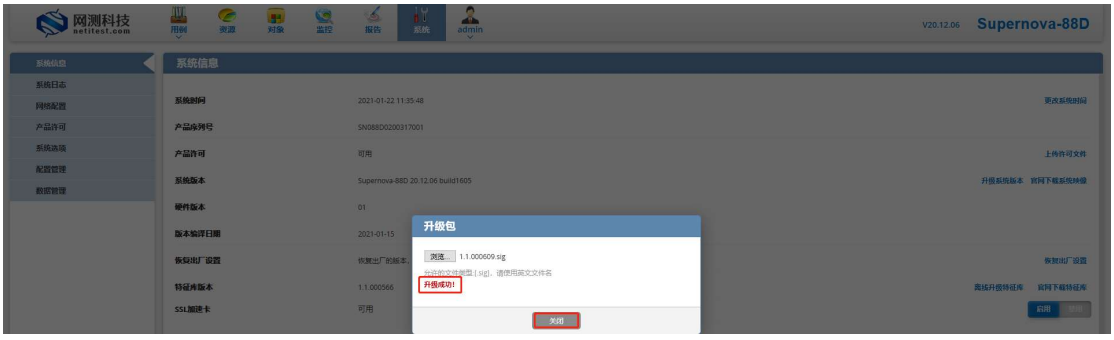
登录 26E，先确定系统是否有特征库，再创建一个系统漏洞扫描测试用例。

3.1.1 升级特征库版本

1）若需要上传或升级特征库，可以到我们官网 www.netitest.com 支持与下载页面，下载最新的特征库。

2）在系统信息页面，可以看到特征库版本，点击离线升级特征库，选择文件，之后点击上传按钮，上传特征库。升级成功后点击关闭按钮。

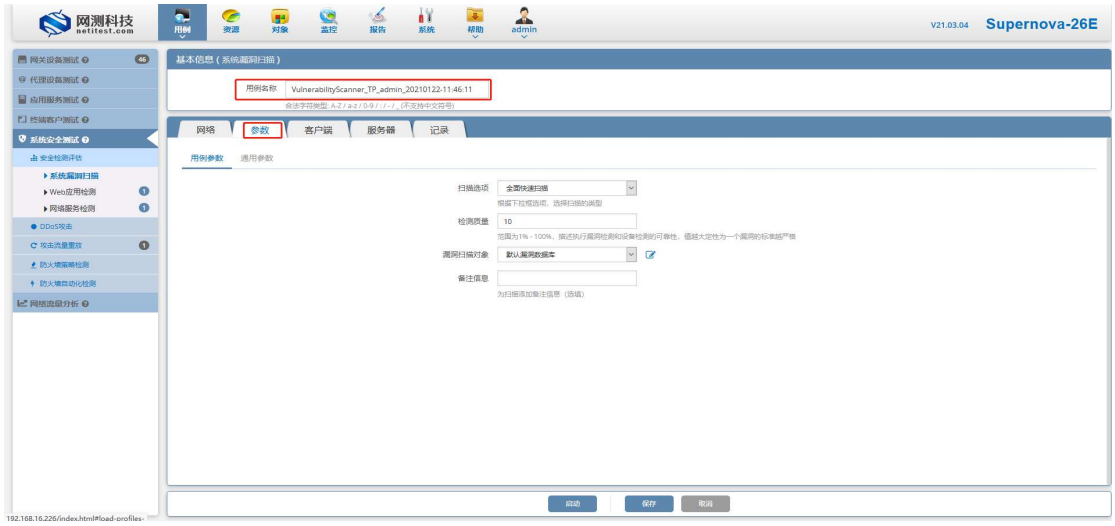




3.1.2 创建系统漏洞扫描用例

1）依次点击，用例->系统安全测试->安全检测评估->系统漏洞扫描->增加，就会弹出增加系统漏洞扫描用例的对话窗口。因为 26E 的 port1 端口与 20C 的 port1 端口是光纤直连，故选同一子网。

2）输入系统漏洞扫描用例的名称，可以根据需要设置参数等信息。



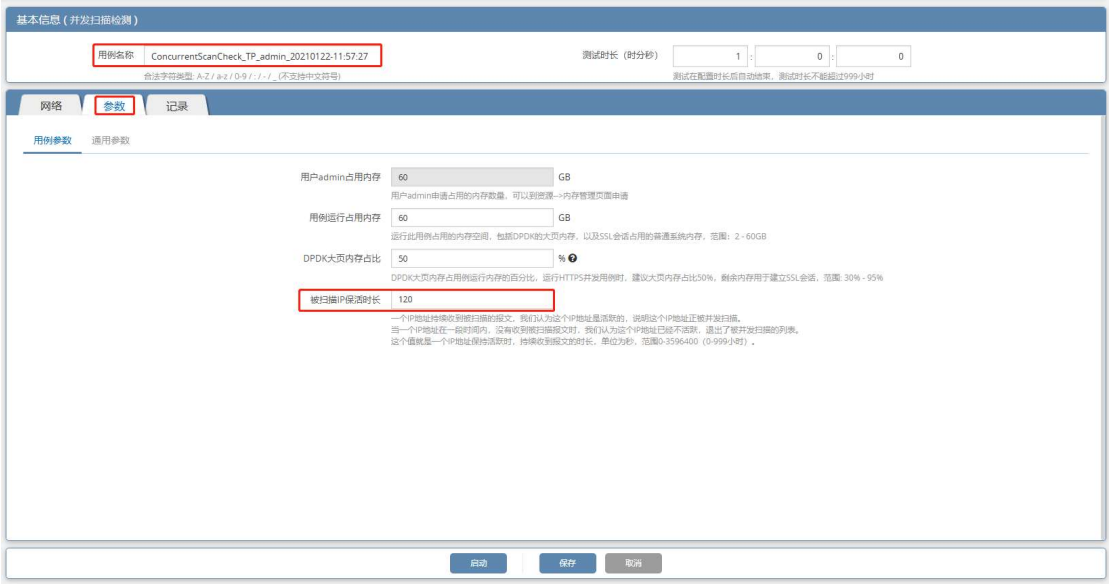
3）根据网络拓扑和 IP 设置，配置端口和 IP 地址，配置完成后，点击保存。

3.2 创建并发扫描检测用例

登录 20C 设备，创建一个并发扫描检测测试用例，修改配置参数。

1）依次点击，用例->网络流量分析->并发扫描检测->并发扫描检测->增加，就会弹出增加并发扫描检测用例的对话窗口。因为 20C 的 port1 端口与 26E 的 port1 端口是光纤直连，所以测试仪和扫描设备选同一子网。

2）输入并发扫描检测用例的名称，设置被扫描 IP 保活时长，默认配置为 120 秒。如果一个 IP 在 120 秒之内没有收到扫描报文，就说明这个 IP 是不活跃的，反之我们认为这个 IP 是活跃的，正在被并行扫描。当然，这个值可以根据需要修改。



3）根据网络拓扑和 IP 设置，配置端口和 IP 地址，配置完成后，点击保存。

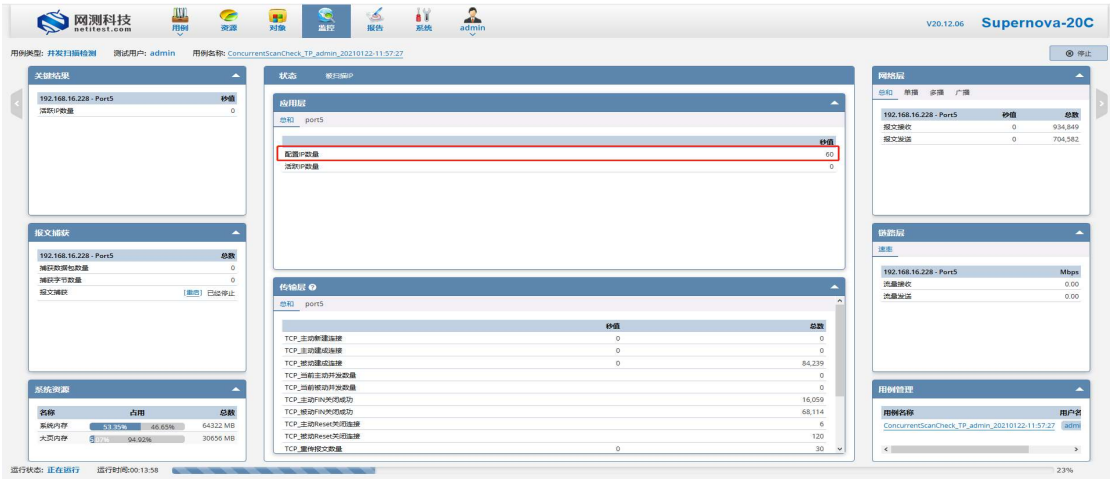
4. 运行用例

运行用例时需要先启动并发扫描检测用例，再启动系统漏洞扫描。

4.1 运行并发扫描检测用例

1）在测试设备 20C 上，点击运行在 3.2 中保存的并发扫描检测测试用例。

2）并发扫描检测测试用例启动起来后，进入到监测页面，可以看到配置的扫描 IP 数量和配置用例时设置的一样。



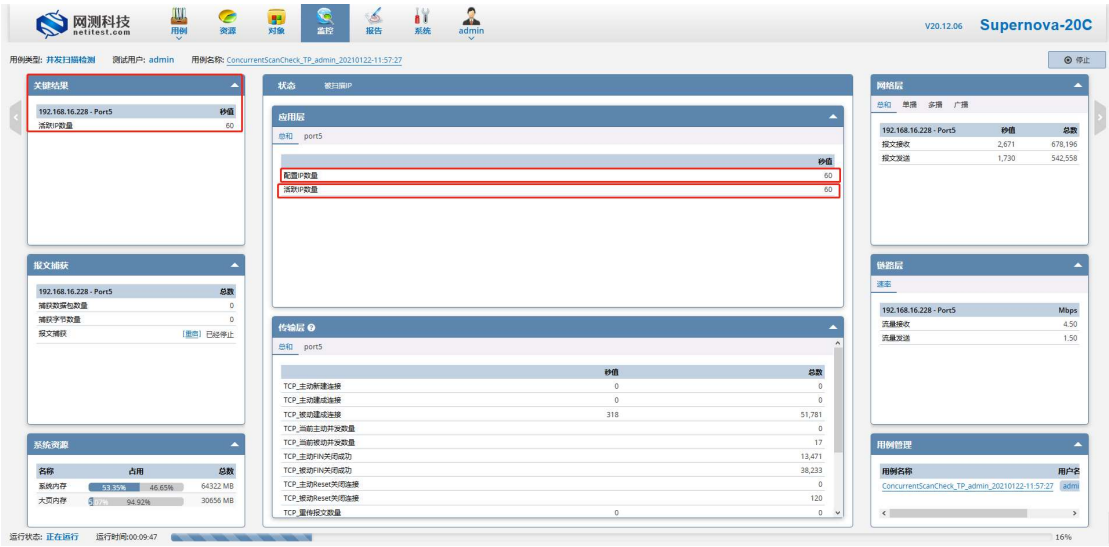
4.2 运行系统漏洞扫描用例

1）并发扫描检测测试用例启动起来进入到监测页面后，在受测设备 26E 上，点击运行在 3.1.2 中保存的系统漏洞扫描测试用例。

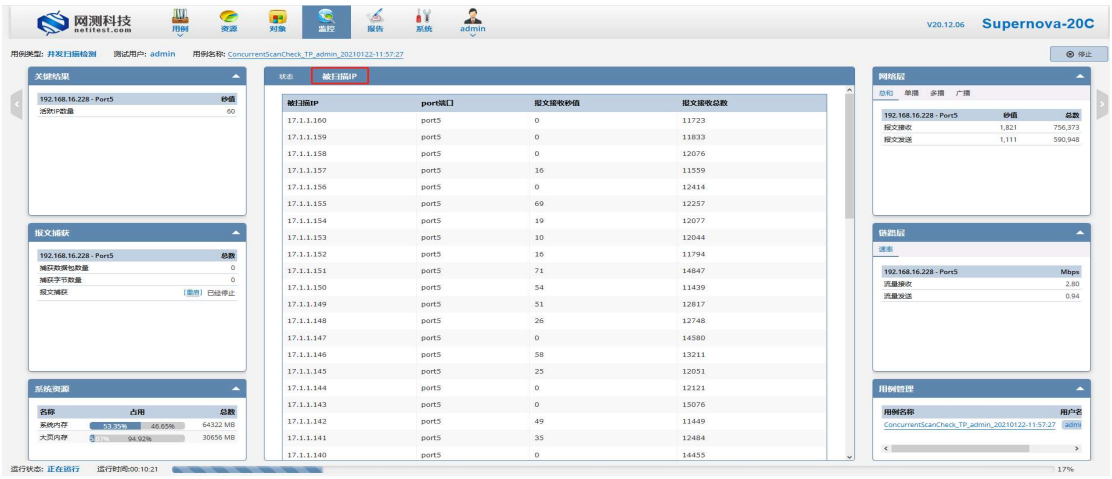
5. 监测用例

当系统漏洞扫描运行起来之后，可以在测试设备 20C 的监测页面看到并发被扫 IP 数量，即受测设备 26E 系统漏洞扫描并发扫描目标主机 IP 的数量。

1）状态→应用层数据，可以看到每秒并发被扫描 IP 数量。



2）在被扫描 IP 页签内可以看到每个 IP 报文接收秒值和报文接收总数。



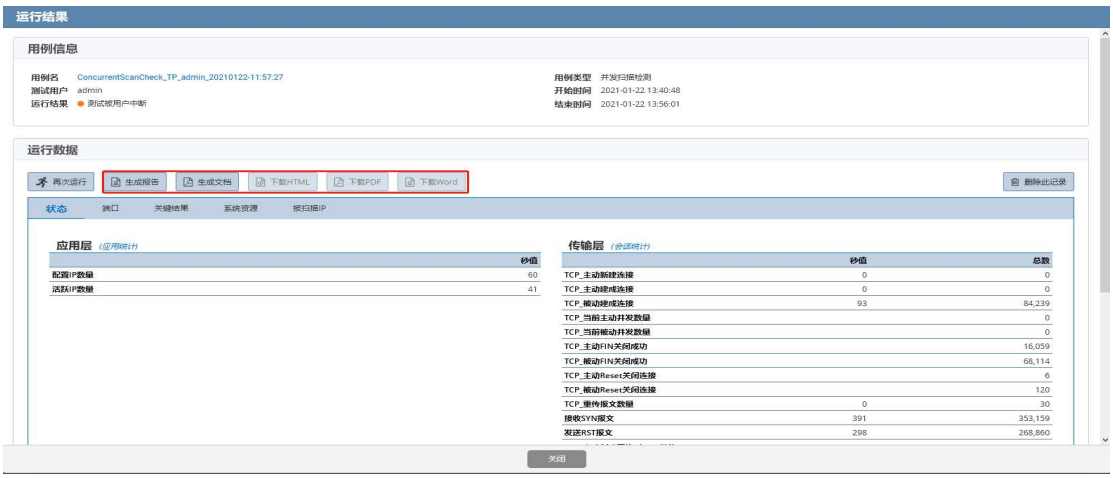
6. 历史报告

测试完成后，历史报告中也会记录测试的最大并行扫描 IP 地址的数量，也可以图形化直观显示结果。

6.1 查看历史报告

1）在测试设备上，点击报告->查看报告，找到刚刚运行的用例，点击打开测试结果按钮。

2）打开之后可以点击生成报告，生成运行数据及关键结果等数据。



3）点击关键结果，可以看到详细时间节点活跃 IP 数量图形化结果。

6.2 导出报告

在报告->查看报告页面，通过点击生成文档，可以生成 HTML/PDF/Word 格式报告并支持下载。