

Supernova 测试仪 攻击流量重放配置手册

网测科技

2022/01/19

目录

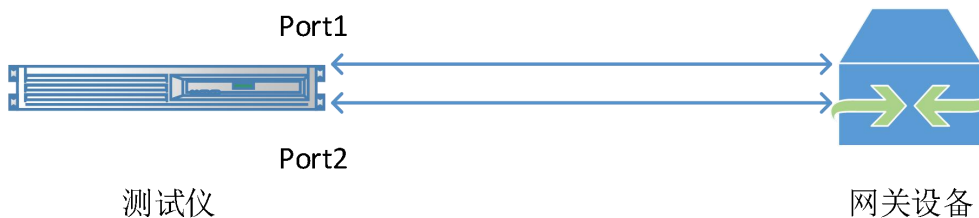
1. 文档说明.....	3
2. 测试拓扑.....	3
3. 设置 Supernova 测试仪.....	4
3.1 升级特征库版本.....	4
3.2 查看编辑攻击流量对象.....	6
3.3 创建攻击流重放用例.....	7
4. 运行用例.....	11
5. 报告生成与下载.....	12
5.1 查看历史报告.....	12
5.2 下载测试报告.....	13

1. 文档说明

本文档主要介绍攻击流重放的配置和测试过程。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. 测试拓扑

下图是一个常见测试拓扑，测试仪测试端口重放攻击报文，经过受测设备转发至对端端口，通过检查重放报文的完整性，确定受测设备的入侵检测和防御能力。



3. 设置 Supernova 测试仪

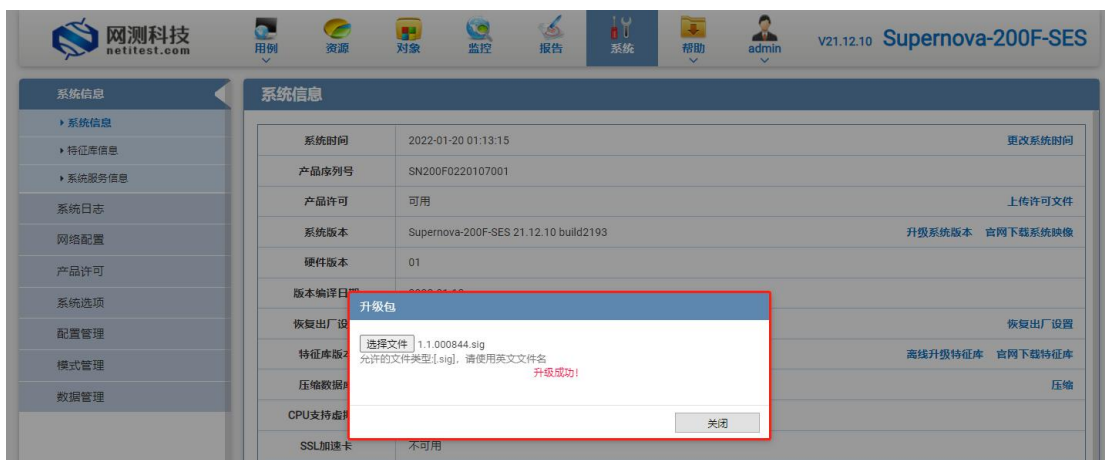
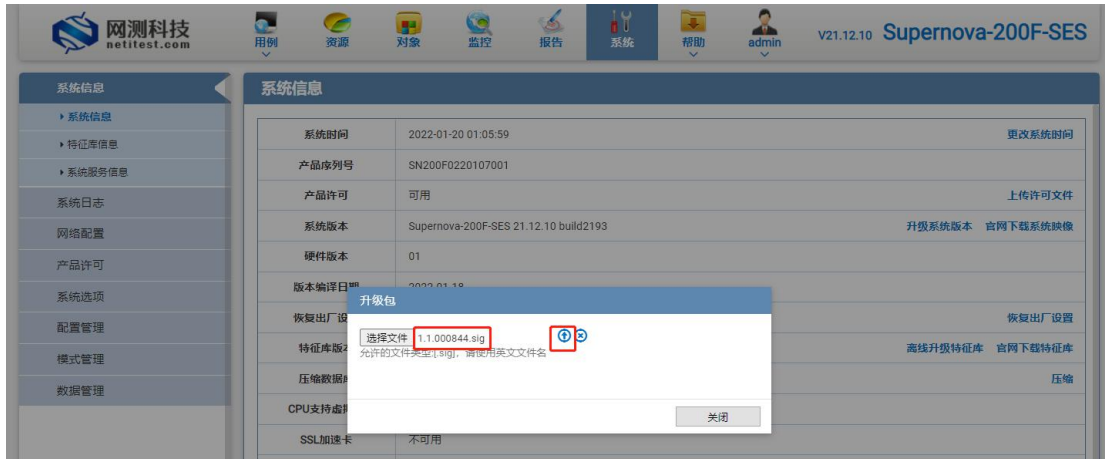
3.1 升级特征库版本

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。

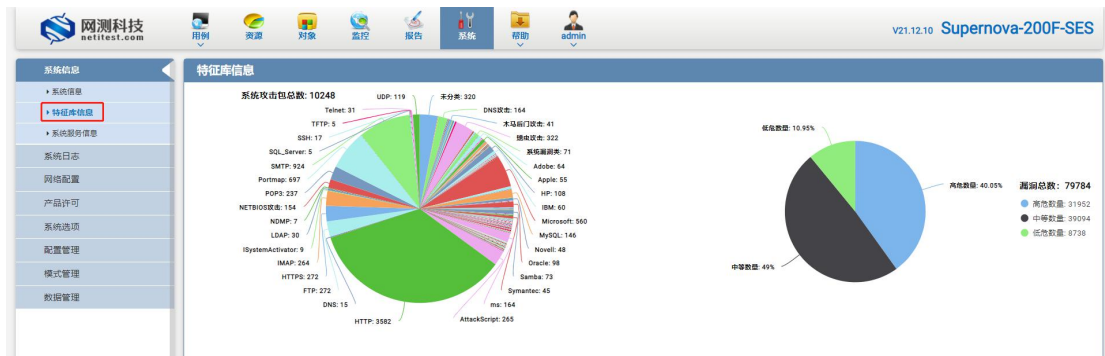


2) 在系统信息页面,可以看到特征库版本,点击“离线升级特征库”,选择文件,之后点击上传按钮,上传特征库。升级成功后系统提示升级成功,升级成功后可以点击关闭按钮,刷新页面。



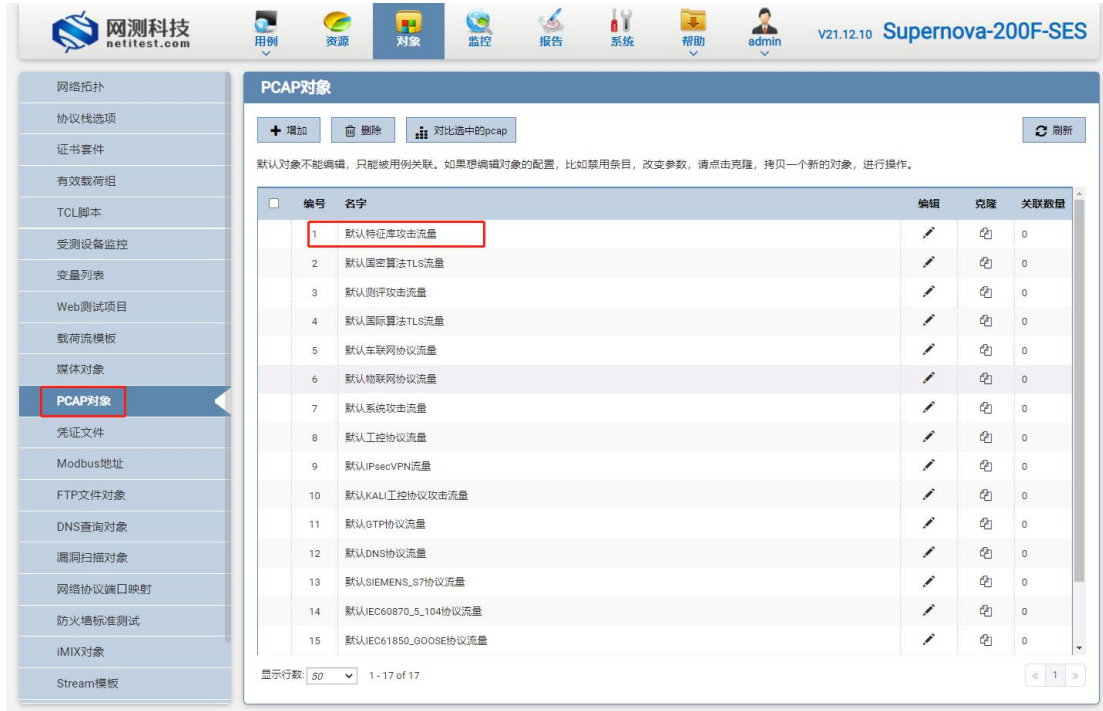




3) 点击系统信息子菜单“特征库信息”，展示最新的特征库信息。



3.2 查看编辑攻击流量对象

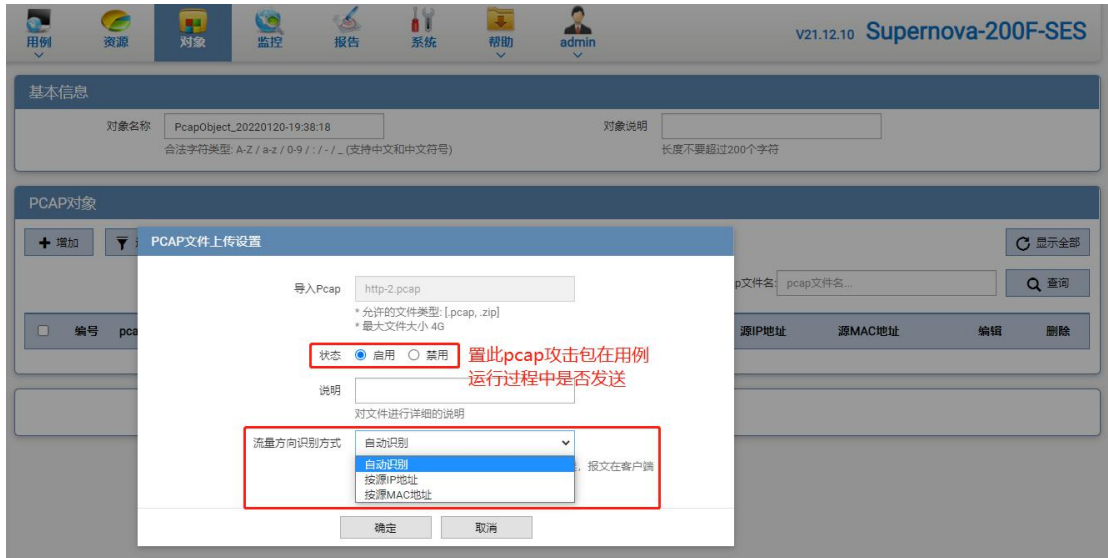
1) 升级成功后，特征库攻击包将会更新到“对象->PCAP 对象->默认特征库攻击流量”中。



2) 点击编辑  按钮可以查看具体攻击流量，不能进行编辑，若需编辑默认特征库攻击流量对象的配置，请点击克隆  按钮，生成一个新的 PCAP 对象，并对其进行编辑。



3) 如果想重放特定的攻击报文, 在“对象->PCAP 对象”页面可以点击“增加”按钮新建一个 PCAP 对象, 点击“增加”按钮, 在弹出的对话框中, 上传 [. pcap, . zip]格式的文件, 文件大小小于 4G, 点击“确定”保存。



3.3 创建攻击流重放用例

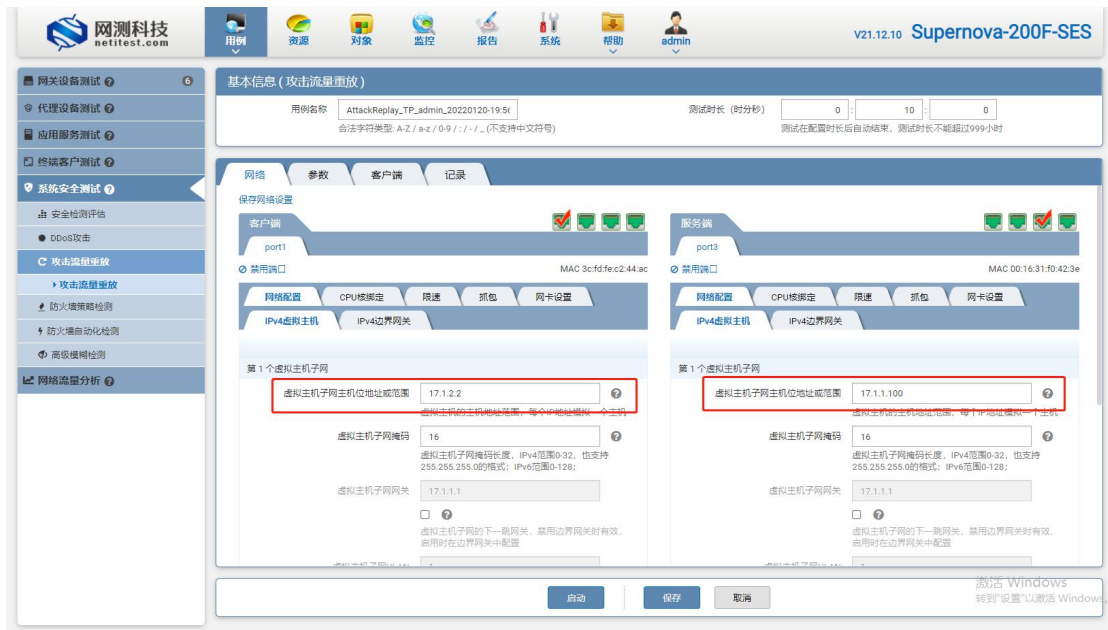
1) 依次点击“用例->系统安全测试->攻击流量重放”, 在用例页面可以看到系统特征库攻击包的类型和数量。



2) 点击“增加”按钮，新建一个测试用例，在弹出的对话框中选择受测设备工作模式。




3) 点击确定，进入用例配置界面，配置子网信息。受测设备工作模式为透明模式，两边子网可以配置同一子网。



4) 在“参数”页签，配置用例参数。重写报文 MAC 地址和 IP 地址选择“是”的时候，重放流量时会根据测试仪网口的实际 MAC 地址，修改报文中的 MAC 地址和 IP 地址。



5) 配置要重放的攻击流量。在“客户端”页签，PCAP 对象处，选择要重放的攻击流量对象，或者点击增加  按钮，新建一个 pcap 对象，上传自定义攻击流量报文。



PCAP对象
OF-SES

基本信息

对象名称

合法字符类型: A-Z/a-z/0-9/!/:/./_ (支持中文和中文符号)

对象说明

长度不要超过200个字符

PCAP对象


编号	pcap文件名	类型	说明	流量方向识别方式	报文解析	跳变设置	源IP地址	源MAC地址	编辑
<input checked="" type="checkbox"/>	1	adobe_embedded_com_firefox_CVE-2009-29...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	2	adobe_flash_cas92_int_overflow_update_1...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	3	adobe_flash_cas92_int_overflow_update_CV...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	4	adobe_flash_mp4_cpirt_1_CVE-2012-0754 pc...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	5	adobe_flash_mp4_cpirt_2_CVE-2012-0754 pc...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	6	adobe_flash_oft_font_15766_CVE-2012-1535...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	7	adobe_flash_oft_font_CVE-2012-1535 pcap	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	8	adobe_flash_pixel_bender_bof_multi_CVE-20...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	9	adobe_flashplayer_arrayindexing_CVE-2011...	攻击流量放报文	自动识别	解析	不可用			
<input checked="" type="checkbox"/>	10	adobe_flashplayer_aslaunch_1_CVE-2008-54...	攻击流量放报文	自动识别	解析	不可用			
<input type="checkbox"/>	11	adobe_flashplayer_sslaunch_2_CVE-2006-54...	攻击流量放报文	自动识别	解析	不可用			

显示行数: 1 - 50 of 200

激活 Win...
转到设置...

4. 运行用例

1) 用例配置编辑保存后自动返回主页面，找到刚刚配置的用例，点击运行

 按钮，启动测试。



系统攻击包统计

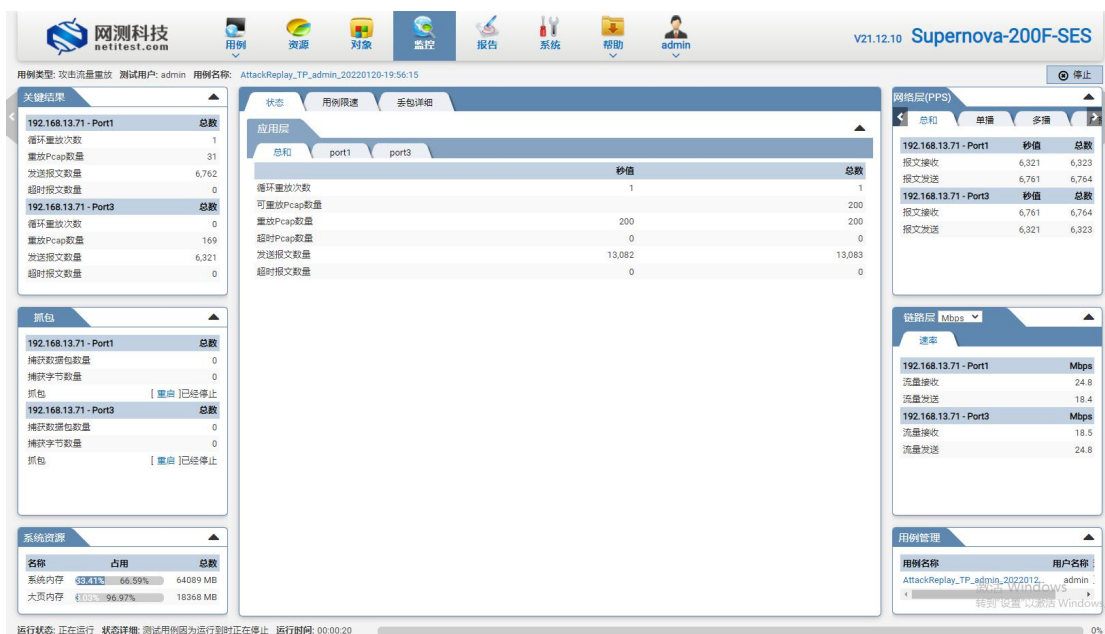
系统攻击包总数: 10248

Telnet: 31	UDP: 119	未分类: 320	DNS攻击: 164
SMTP: 924	端口攻击: 322	系统漏洞类: 71	HP: 108
Portmap: 697	POP3: 237	Microsoft: 560	MySQL: 146
NETBIOS攻击: 184	LDAP: 30	Oracle: 98	Samba: 73
IMAP: 264	HTTP: 3582	ms: 164	AttackScript: 265
FTP: 272			

用例列表

编号	运行	任务列表	用户	名字	编辑	克隆	详细信息	导出	历史记录
1			admin	AttackReplay_TP_admin_20220120-19:56:15					0

2) 用例启动后进入运行状态，监控页面的数据每秒自动刷新，可以看到实时的数据统计结果，比如重放 Pcap 数量、发送报文数量等。



关键结果

192.168.13.71 - Port1	总数
循环重放次数	1
重放Pcap数量	31
发送报文数量	6,762
超时报文数量	0

192.168.13.71 - Port3	总数
循环重放次数	0
重放Pcap数量	169
发送报文数量	6,321
超时报文数量	0

抓包

192.168.13.71 - Port1	总数
捕获数据包数量	0
捕获字节数量	0

192.168.13.71 - Port3	总数
捕获数据包数量	0
捕获字节数量	0

系统资源

名称	占用	总数
系统内存	66.59%	64089 MB
大页内存	96.97%	18368 MB

应用层

应用层	port1	port3	秒值	总数
循环重放次数	1	1	1	1
可重放Pcap数量	200	200	200	200
重放Pcap数量	200	200	200	200
超时Pcap数量	0	0	0	0
发送报文数量	13,082	13,083	13,082	13,083
超时报文数量	0	0	0	0

网络层(PPS)

192.168.13.71 - Port1	秒值	总数
报文接收	6,321	6,323
报文发送	6,761	6,764

192.168.13.71 - Port3	秒值	总数
报文接收	6,761	6,764
报文发送	6,321	6,323


链路层(Mbps)

速率	Mbps
192.168.13.71 - Port1	流量接收: 24.8
	流量发送: 18.4
192.168.13.71 - Port3	流量接收: 18.5
	流量发送: 24.8

运行状态: 正在运行 状态详情: 测试用例因为运行到定时正在停止 运行时间: 00:00:20

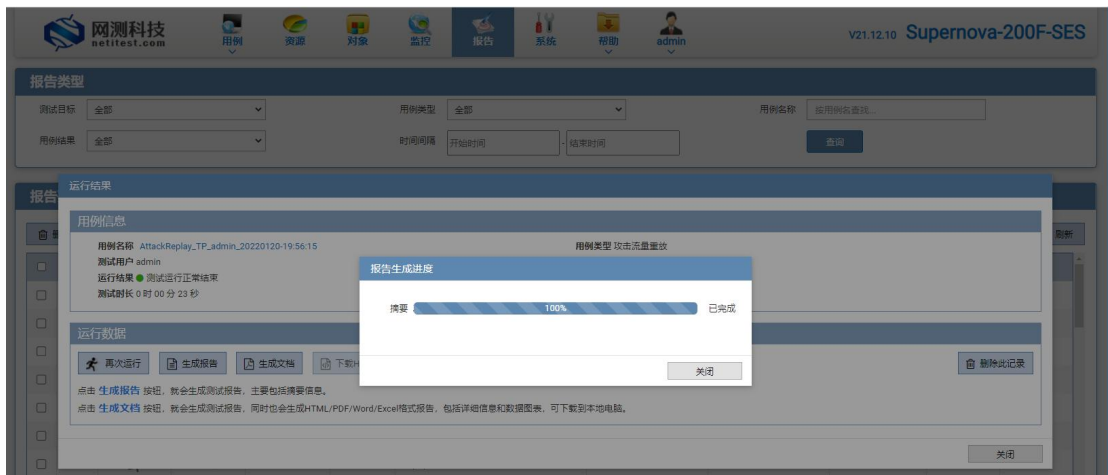
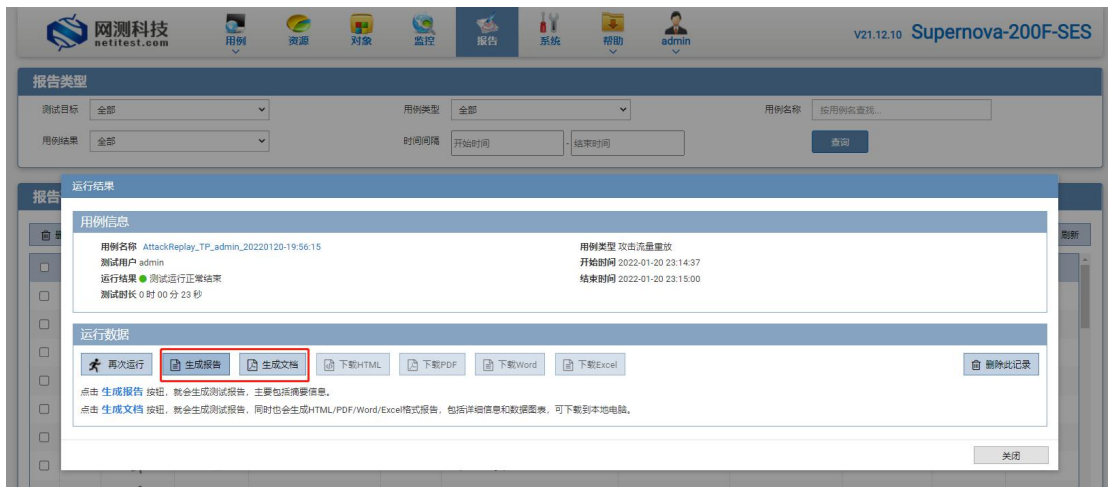
5. 报告生成与下载

5.1 查看历史报告

1) 运行结束后，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) 打开之后点击“生成报告”按钮，生成测试报告，包括摘要信息和数据图表。





5.2 下载测试报告

点击“生成文档”按钮，可以根据需要选择生成内容，之后可以生成HTML/PDF/Word 格式报告，并且支持下载。

