

Supernova 测试仪 并发扫描检测配置手册

网测科技

2021/01/22



	_=.
日	豕

文档说明	3
网络拓扑	3
配置过程	4
3.1 配置受测设备	4
3.1.1 升级特征库版本	4
3.1.2 创建系统漏洞扫描用例	5
3.2 创建并发扫描检测用例	6
运行用例	7
4.1 运行并发扫描检测用例	7
4.2 运行系统漏洞扫描用例	8
监测用例	8
历史报告	9
6.1 查看历史报告	9
6.2 导出报告	10
	 文档说明



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)》 (<u>http://www.cac.gov.cn/2017-06/09/c 1121113591.htm</u>),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<u>www.netitest.com</u>支持与下载页面,下载最新的特征库。

◎ 网测科技 netitest.com			首页 产品中心	解决方案 支持与	下载 关于我们	合作伙伴(申请试	
免费资源	☞ 特征库	下载					
● 漢穴运貨廠 ● 系統議像-v20.12	编号	文件名称		更新日期	文件大小	擾作	^
• 系统摄像-v20.09	1	1.1.000609.sig.md5		2021-01-21	48		
•特征库	2	1.1.000609.sig		2021-01-21	277M	B	
 IPv6一致性检测组件 	3	1.1.000608.sig.md5		2021-01-20	48	(I)	
 网卡映像组件 	4	1.1.000608.sig		2021-01-20	277M	Ð	
	5	1.1.000607.slg.md5		2021-01-19	48	.cm	
	6	🗋 1.1.000607.sig		2021-01-19	277M	6	

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。

 	HIM SEE MR EES		v20.12.06 Supernova-88D
新始信息	系统信息		
系统日志			
网络配派	系统时间	2021-01-22.11:33:56	思改革成时间
产品许可	产品成列号	SN088D0200317001	
系统课项	产晶许可	可用	上传许可文件
配設管理	系统版本	Supernova-S8D 20.12.06 build1605	升级系统版本 前同下载系统映像
ACCE 1911	硬件版本		
	新本编译日期	2021-01-15	
		11.000609.sig 10.1.000609.sig 10.1.000609.sig 10.1.000609.sig	Sources using
	特征库版本	1.1.000566 Valiation Product Apple Ministration Contract	海线升级特征库
	SSLMD#-F	利用	2348 - 2444
	IPv6—致性检测组件	124	上传功震调件 官同下载唱件 组件开关
	格式化系统硬盘	翰份用例,対象和用户配置:重新核式化系统硬盘。快速解放磁盘空间	指式化硬盘
◎ 网测科技 netitest.com			v20.12.06 Supernova-88D
系统信息	系统信息		
系统日志			
网络配置	系统时间	2021-01-22 11:35:48	更改系统时间
产品许可	产品成列号	SN088D0200317001	
系统选项	产品许可	初用	上传許可文件
1200			
SALE MARK	系统版本	Supernova-88D 20.12.06 build1605	升级系统版本 官同下载系统映像
	系统版本 硬件版本	Supermova 480 20 12.06 bulk1605	升级系统版本 前间下载系统映输
	系統版本 硬件版本 版本编译日期	Superviews 880 20 12 05 buildt 885 01 2017 01 5	нелецья интеренне
	到他版本 閘門版本 版本编译日期 集制41 10节	Supernova 802 20 12 05 Julii 105 01 2021-01-15 988-178488 988-178488	HEERES HHTEEREN
	新始加本 続件加本 加本加行日期 後5001「必算	Superview 8012 2012 08 Juliel 1055 01 2021-01-15 1000000 ag 	HERE'S HTTESSMO
	ERGER Reflex Scharfell Reflect Sciences	Supermove 400 20 12 06 built 1000	HEARES HITTESSAG BRUTTES REARING ANTERSON



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。

 网测科技 netitest.com	 V21.03.04	Supernova-26E
A deletito A		
	ana a	 ● → ○ ● → ○ ● → ○

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。

◎ 网测科技	🚒 😹 Xák 🔐 🦉 🏑	V21.03.04	Supernova-26E
■ HALLESARANE © ● ■ HALLESARANE © ● ■ ANTREMANE © ● ■ ANTREMANE © ■ ■ COLONIA ● C REALBARE ● ▲ COLONIA ●	1000 2000 <t< th=""><th></th><th></th></t<>		
	607 RX		

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。

基本信息(系统漏洞扫描)							
用例名称	VulnerabilityScanne 合法字符类型: A-Z / a-z /	r_TP_admin_20210122-11:46:11 0-9/:/-/_(不支持中文符号)					
网络参数	客户端	服务器 记录					
保存网络设置		客户端 port3				夏 夏 夏 连择与测试设备	ž
		⊘ 禁用講口				MAC 68:91:d0:66:94:72	
		子网 😧				•	
		第1个子网	测试仪端口IP地址	17.1.2.2	0	进行漏洞扫描的端口IP	
			测试仪端口子网掩码	16	0		
			2012月1日月天		10	系统并发扫描的最大	
			被扫描主机IP地址或范围	17.1.1.101-17.1.1.160	0	主机测试数量为60,	
						所有此处填写扫描60 个目标主机地址	



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。

◎ 网测科技 netitest.com		admin	V2	0.12.06 Supernova-20C
	并发扫描检测			
	根據黨家設布的阿诺关键设备和阿诺安全专用产品的经常要求。	对网络鹅翎性目端产品,要求最大并行扫描可数量大于等于60个,进行检测认证。		
 1) 授業数户期間 0 ジ 系统安全期間 0 ① 	用例列表			
	· 编号 运行 任务列表 用户	若 疗	論語 克隆 详细	章 马出 历史记录
○并发扫描检测 >并发扫描检测	显示行数: 10 ⊻ 0-0 of 0	选择用例选项		
		2版本 ● 4 0 16 0 服金 開成(XR22開成員 ● 23月-7月 0 即用(X492 同協配室 服X3開版 14		
		Main Raini		

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。

基本信息(并发扫描检测)	
用制金額 ConcurrentScanCheck_TP_admin_20210122-11:57:27 台波寺研想型、トスノルマノロタイ: ノーノ(不安計中文研号)	調試時长(時分粉) 1 : 0 : 0 測试在影響が长后有改体形、測试が长不能超过990小df
网络参数记录	
用例参数 通用参数	
用户admin占用内存	60 GB
	用户admin申请占用的內存数量,可以到资源一>內存管理页面申请
用例运行占用内存	60 GB
	运行此用例占用的内存空间,包括DPDK的大页内存,以及SSL会话占用的普通系统内存,范围:2-60GB
DPDK大页内存占比	50 % 🛛
	DPDK大页內存占用例运行內存的百分比,运行HTTPS并发用例时,建议大页内存占比50%,剩余内存用于建立55L会活,范围: 30% - 95%
被归描印保酒时长	
	——~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~



Supernova 测试仪并发扫描检测配置手册

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。

基本信息(并							
	用例名称	ConcurrentSca 合法字符类型: A-Z	anCheck_TP_admin_20210122-11:57: / a-z / 0-9 / : / - / _ (不支持中文符号)	27	测试时长(时分秒)	1 0 創成在影響时长后自动始期,創成时长不能超过099小时	0
网络	参数	记录	k				
果存网络设置			服务端 port5				选择与受测设备连通 的测试口
			◎ 禁用跳口			MAC 68:91:d0:63:4a:cc	
			CPU核绑定			•	
				CPU検ID	2 CPU核绑定可透ID为0,1,2,3,4,5,6,7,8,9 运爆多个被机,遭使困难变了。分割, 不同族口不能使用相同的CPU核。 为了系统模定和报告插稿。 建议留何个核0,1份系统以及数据库		
			报文捕获			•	
			子网 😧			+ 添加子网 🔺	
			篇1个子网			會 称除子网 ⊘ 競用子网	
				测试仪端口IP地址或范围	17.1.1.101-17.1.1.160	测试设备设置的主机IP地址范围,	要包含受测安全扫描设备
				测试仪筒口子网接码	16	设置的目标主机的IP范围	
				测试仪满口网关		0	
			50	网络脆弱性扫描产品端口IP地址或范围	17.1.2.2	受测安全扫描设备IP	

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。

◎ 网测科技				V20.12.06	Supe	mova-20C
n 网关设备测试 🛛 🛛 🕦	并发扫描检测					
© 代理设备测试 O O	根据国家没布的网络关键设备和网络安全专用产品的检测要求,对网络脑弱性目描产品,要求最大并行目描IP数量大于等于60个,进行检测认证。					
■ 应用服务测试 ● ●						
□ 终端客户测试 Θ	用例列表					
 ⑦ 系统安全测试 Θ ① ▲ 网络混乱分析 Θ 	+ ano 8 mis					○ 2 期新
11 报文编码初始	□ 编号 <u>同日</u> 任务列表 用户 名字 区式学校出现	编辑	克羅	详细值息	导出	历史记录
○井发田間控測	1 1 admin ConcurrentScanCheck_TP_admin_20210122-11:57:27	/	ත			1
▶ 并发扫描检测 0	盥示行版: 10 ♥ 1 - 1 of 1					e 1 3

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。

netitest.com	1164 32.22	对象 报告 系统 admi	n		120.12.00	Capernova
并发扫描检测 测试用户: ad	dmin 用例名称: Concurr	rentScanCheck_TP_admin_20210122-11:57:27				
建结果	_	状态 板目前の			网络展	
2.168.16.228 - Port5	1940				急和 单指 多指 广播	
既的数量	0	NY HILE		<u>^</u>	102 169 16 229 Beers	Tell
		意和 port5			102.100.10.220-10103	0 02
					180×1900	0 70
		Eliterature and a second se		en	100,000	
		ROR SOR		60		
		2220PRCM		0		
R. hliste	<u>▲</u>				链路层	
					法在	
02.168.16.228 - Port5	总数					
获数据包数量	0				192.168.16.228 - Port5	
获字节数量	0	(5)0E 0			洗量接收	
文講院	(豊富) 已经停止	12 mas o			沈晨发送	
		min ports				
			9 0	200		
		TCP_主动物理编程	0	0		
		TCP_意动建成编程	0	0		
		TCP_被动建成油接	0	84,239		
		TCP_当前主动并发数量		0		
		TCP_当前主动并发数量 TCP_当前被动并发数量		0	EBA49979	
充實裏	-	TCP_当前主防并没数量 TCP_当前核功并没数量 TCP_主动形状光线成功		0	用粉管理	
充资源 称 占田	-	TCP_当前主助并没数量 TCP_当前报助所发数量 TCP_主动和我的发动动 TCP_主动和关闭成为		0 16,059 68,114	用制作理	,
·资源 称 占用	500 64322 MR	TCP_当前主动并没数量 TCP_当前领动并没数量 TCP_主动FNAVK的成功 TCP_振动FNAVK的成功 TCP_振动FNAVK的成功		0 16,059 68,114 6	用例名称 GonggreetScanCherk IP add	min 20210122-11-57-27
と対象 株 古田 代内存 <u>51355</u> 44	谷数 5.65% 64322 MB 20555 MB	TCP 当前主助并波波論 TCP 当前後加片波波論 TCP 当前代加片波波論 TCP 通知FAVK50成功 TCP 通知FAVK50成功 TCP 通知FAVK50成功 TCP 通知FAVK50成量線		0 16,059 68,114 6 120	田砂竹田田 田砂谷称 ConcurrentScanCheck_TP_add	F min_20210122-11:57:27



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。

◎ 网测科技	🙀 😤 💀 🖄 👬 ki 🗰 🌲 V21.03.04 -	Supernova-26E
	系统羅調扫描	
© ft⊞ig#Mit ©	扫描, 计台和管理目标主机上的感情, 通到郑门首将的立持与下都页面, 下载根形的演员年,	
■ 应用服务测试 ●		
[1] 终端客户测试 Q	漏洞风脸统计	
◎ 系统安全测试 ❷	运行校里:11.51%	
由安全检测评估		
 ▶ 系统漏洞扫描 ○ 	周月日秋: 63725 西日本 (73)	
 · Web还用加速者 · Web还用加速者 · · ·	● 酒信太雅 2955 ● 甲喃安乱 29436	
● DDos政击	• E282 7334	
C 攻击流量重放 0	458 <u>8</u> :411x	
▲ 防火液原路检测	-	
防火端目动化检测	用研究制度	
▶ 网络流型分析 ❷		
	+ 120 G Bisk T A(R) (19)	長 号入 2 刷新
	□ 编号 <u>新闻</u> 克隆 首先列表 用户 名字 编辑 克隆 详细信息	导出 历史记录
	🗆 1 📝 🗎 admin VulnerabilitySkanner_TP_admin_20210122-11:46:11 🖍 🖉 📳	R 1
	皇帝的能 10 V 1-1ef1	< 1 »

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。

并发扫描检测 测试用户: admin 用	明名称: <u>Concurren</u>	tScanCheck_TP_admin_20210122-11:57:27				
對结果	~	状态 愛白眉中			网络展	
7 169 16 779 Date 5	14.05	(manufacture)			总和 单播 多播 广播	
2100-10120-10105 21021-0	50	应用层		<u>^</u>		
		應和 port5			192.168.16.228 - Port5	1901
					报文报收	2,671 670
				紗值	报文发送	1,730 54
		配置印数量		60		
		活狀IP数量		60		
と捕获	•				链路层	
2.168.16.228 - Port5	2.0				32	
時教研何教量	0					
(2)余节数量	0				192.168.16.228 - Port5	
C 1800 (800)	THANKIF	作输展 🛛		^	流纖接收	
	0.000.07.02	CHI port5		<u>^</u>	沉地发送	
		- Perce				
			80	22		
		TCP_主动新建连接	0	0		
		TCP_主动建成编程	0	0		
		TCP.被助建成连接	318	51,781		
		TCP 当前主动并发数量		0		
- 20/30				17	ET ALAMATER	
	-	TCD #HDENX/FIGTTD		12.471	HIMELE	
t A se	(182			29 222	0.642.92	
e 100	10.95	TCD +28Darat #2010		30,235	102310101	,
你 古用				0	LoncurrentScanCheck TP ad	Imin 20210122-11:57:27
1894年 称 古用 統内存 <u>53358</u> 46.65%	64322 MB			400		



Supernova 测试仪并发扫描检测配置手册

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。

rocalisements address address concorr	entScanCheck_TP_admin_20210122	-11:57:27				۲
мж	秋春 被扫描IP				网络层	
2.168.16.228 - Port5 伊值	att all and a	nort第日	影女認識技術	時々認識ない	▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
ttp23最 60	17.1.1.100	portonica		11777	192.168.16.228 - Port5	96 S
	17.1.1.100	ports	0	11/25	报文撤收	1,821 756,3
	17.1.1.159	port5	0	11833	程文发送	1,111 590,9
	17.1.1.158	portS	0	12076		
	17.1.1.157	port5	16	11559		
	17.1.1.156	portS	0	12414		
	17.1.1.155	port5	69	12257		
	17.1.1.154	portS	19	12077		
chiác 🔺	17.1.1.153	port5	10	12044	链路层	
2.168.16.228 - Port5 总数	17.1.1.152	portS	16	11794	1216	
2.数据包数量 0	17.1.1.151	portS	71	14847	192.168.16.228 - Port5	ME
2字节数量 0	17.1.1.150	port5	54	11439	洗量接收	2
Case (ESA) Estable	17.1.1.149	port5	51	12817	派量发送	0
	17.1.1.148	portS	26	12748		
	17.1.1.147	portS	0	14580		
	17.1.1.146	port5	58	13211		
	17.1.1.145	port5	25	12051		
(空遊) _	17.1.1.144	port5	0	12121	menter	
	17.1.1.143	port5	0	15076		
彩 古田 总数					用制名称	用月

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。

🚫 M测科技	He 💓	对象		が A 系统 admin	v20.12.06 Su ‡	ernova-
吉类型						
测试日标 全部	~			用例类型 全部 >	用例编称 按用例案查找	
用例结果 全部	~			B対向(時)編 开始の(前) 子がの(前) ・ 5点地の(前)	3059	
列表						
						-
新除 自新除所有 III:	定可置於					0
新除 自 新除所有 (1) 集号 再次运行	运行通过 运行注意 ····································	用例类型	测试用户	用则名称	开始时间 结束时间 下载	ご

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。

1信息			
名 ConcurrentScanCheck,TP_edmin_20210122-11:57:27 規定 admini 結果 ●影信状形中年前	田樹美型 井波扫描绘测 开始时间 2021-01-22 13:40:48 结束时间 2021-01-22 13:56:01		
数据			
再次运行 通 生成報告 ひと 生成文档 の 下部・HTML ご 下部PDF の 下部Word			會 删除此:
VIS NUT ARDINE WATCHN PLATERS			
A23 A14 2000日本 exercises todopper	传输层(全面统计)		
	传输层 (会运统计) 砂值	砂道	en
NGU PERSON AND LOUISEF	传输层 (金調約計) 砂面 てCP.主动新建法接	砂道 0	总数 0
NG		砂道 0 0	総数 0 0
ALL Part Parties Antipart Space	 (行输展 (かぶたい)) 94面 50 TCP 主动新始体操 41 TCP 主动新始体操 TCP 法动振动保険 	砂道 0 0 93	总数 0 0 84,239
AND PALE 75800年 ANTELLE Decision	传输层(余式和行) 砂面 CP_主动场时然後 41 TCP.主动场时然後 TCP,地场中成後 TCP.地场中成後	990 0 0 93	630 0 0 84,239 0
ALL PERSON ANTIAL LINN	传输层(含調整行) 60 TCP.主动病能振播 70 TCP.基功用机振播 TCP.端的用机振播 TCP.指导的机构振播 TCP.指用运动开发数量 TCP.指导能动力发发量	80 0 0 93	8420 0 84239 0 0 0
And Ferning and Ferning and And Toring F	传输层(余点和) 砂面 下CP.主动和标志操作 41 TCP.主动和标志操作 TCP,或和标志和操作 TCP.当时和小规算和 TCP,当时和小规算和 TCP.当时和小规算和 TCP,当时最小规算和 TCP.当时最小规算和 TCP,当时最小规算和 TCP.当时最小规算和	9 01 0 93	688 0 0 84,239 0 0 0 16,059
REL PERSON ANTIRA DISUNT	作物記 (今259)	0 0 0 03	632 0 0 0 84,239 0 0 0 16,059 68,114
ALL PERSON ANTIAL LOUDER		940 0 0 93	6880 0 84,239 0 18,059 68,114 6 6
ALL PERSON ANGLIA USUBAT 政用度 (12799637) 経費PR版 高度PR版	作協同 (金30817)	0 0 0 03	Ext 0 0 84,239 0 0 16,039 68,114 6,114 5,120
AND PERSON ANTERNA DECEMPT 应用层 ((2799627) 起用层 ((2799627) 起用度 (2799627)	を結居(かぶたわけ)	9 12 0 0 93	600 0 88,239 0 16,059 68,114 6 120 3 0
ALL 2008年 AAASAN DESINF	作協同 (金田田)	0 0 03 03 03 03 03	4310 0 0 84,239 0 10,059 06,114 0 1120 120 353,159



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。

