

CyberFlood 简明操作手册

任红波

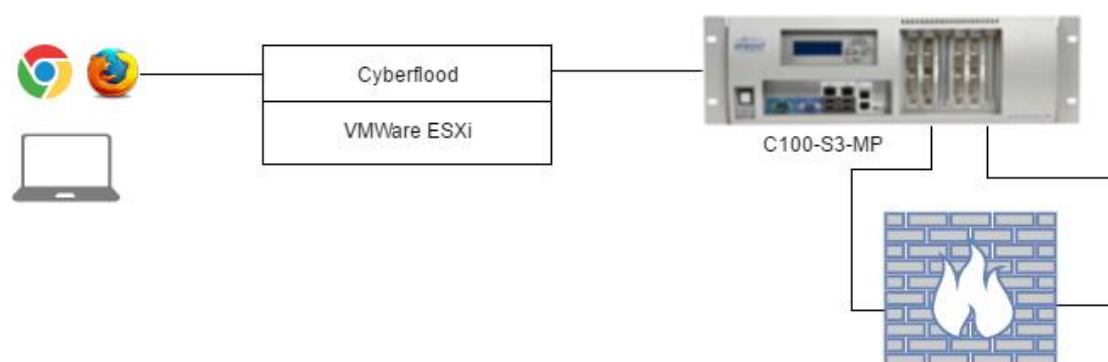
Hongbo.ren@spirent.com

2018.3

1. 准备篇

CyberFlood 组网

CyberFlood 是部署并运行在虚拟机中的软件，控制 C100-S3-MP 等硬件。使用最新版的谷歌、火狐或者 Safari 浏览器访问，不支持 IE 浏览器。



登录系统

使用 <https://CyberFlood> 控制器 IP 登录系统。因为使用了自签名证书，如果提示不受支持，点击继续前往。



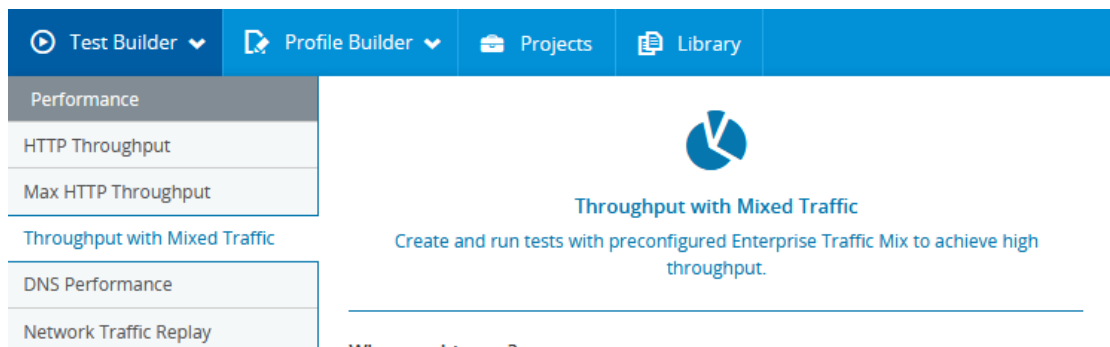
登录用户名和密码

请咨询系统管理员。

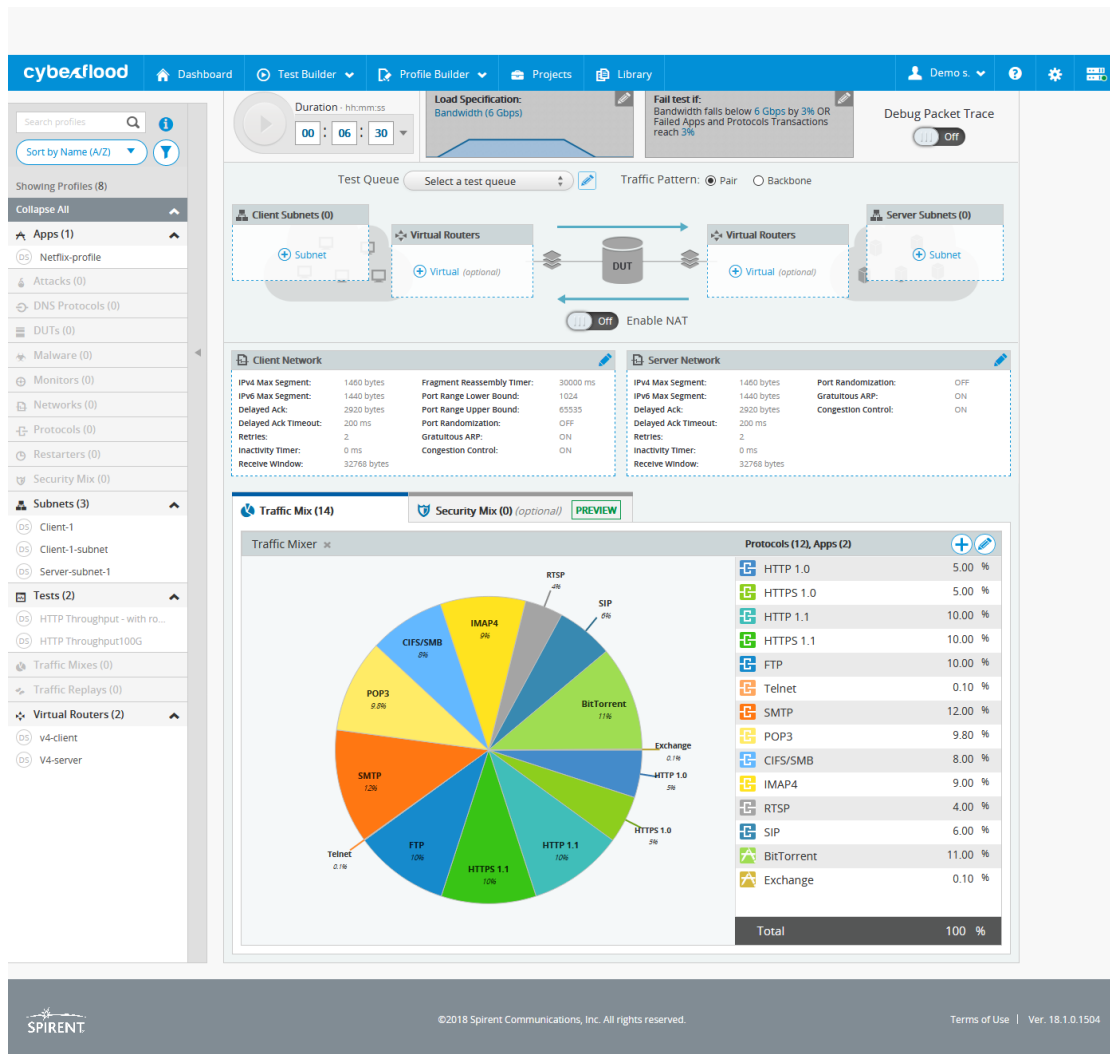
2. 配置混合流量测试（eMix）

配置混合流量测试


在 Test Builder 里面选择 Throughput With Mixed Traffic 模板，点击 [Build a New Test](#) 开始一个新的测试。




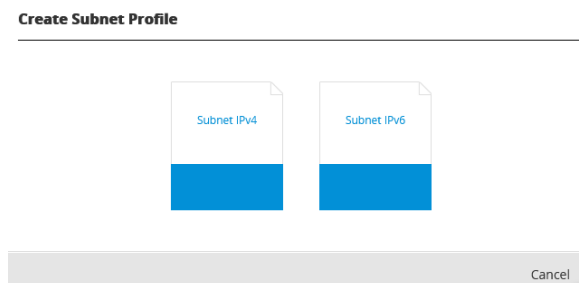
默认的配置如下。



在 Test Queue 里面通过下拉框选择 Brave 队列。

在 Client Subnets 配置子网。有 2 种方法，一种是点击  Subnet 配置一个新的子网，另一种是从左边拖拽一个 subnet 到 Client Subnets 中。

如果是点击  Subnet 配置了子网，进入如下画面配置：



选择 Subnet IPv4，并配置网络信息和 vlan 等。

Create Subnet Profile

Custom IPs Global IPs

The First Address * 10.1.0.2 / 24

Count * 253

Force Server IP Count Off ⓘ

* Server Subnet Profiles only. Not supported in Client Subnet Profiles.

Default Gateway Off

▶ Advanced Settings

Static Routing + Add Static Routing

VLAN + Add VLAN

Cancel · Save Profile and Update Player

保存配置

Create Subnet Profile

Save IPv4 Subnet Profile

Profile Name
IPv4 Subnet Loop 1

Description (Optional) 140

Cancel · Save

Cancel · Save Profile and Update Player

分配测试仪端口，如果没有出现端口画面，点击 (---)。把 1/1 端口分配给客户端。

Client Subnets (1) +

1 IPv4 Sub... (---)

Select Ports

Client Network

IPv4 Max Segment:
IPv6 Max Segment:
Delayed Ack:
Delayed Ack Timeout:
Retries:
Inactivity Timer:
Receive Window:

Select Port(s) for Subnet Profile ⓘ

SPT-CF20 (169.254.0.1)
SPT-CF20-01

40G

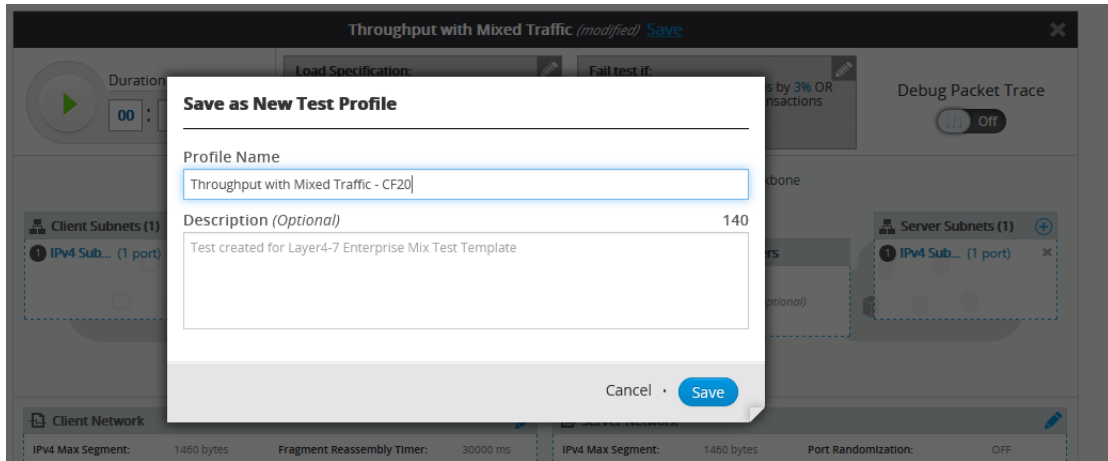
1/1
4

1/2
5

Cancel · OK

同样的，建立服务器侧子网 IPv4 Subnet Loop 2，并分配端口。注意两个子网地址不要重复。

保存配置

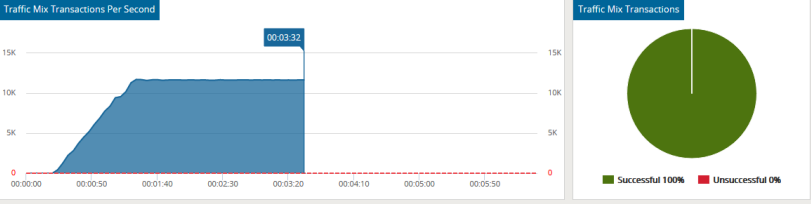
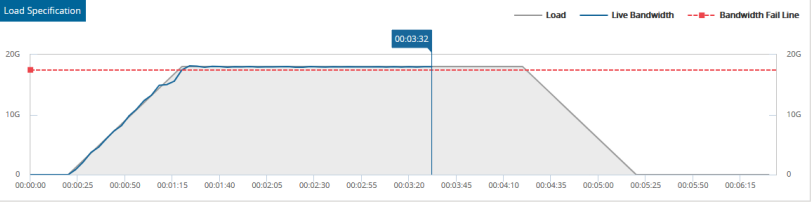


运行并查看结果

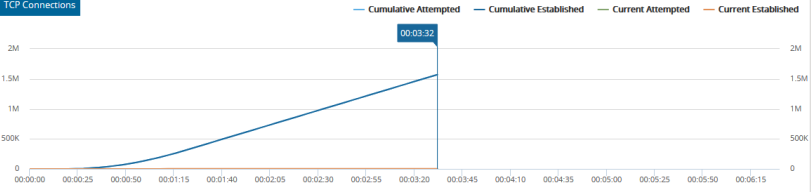
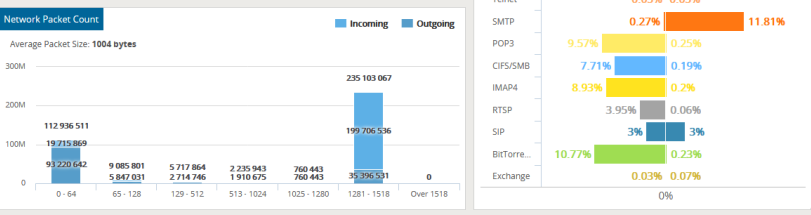
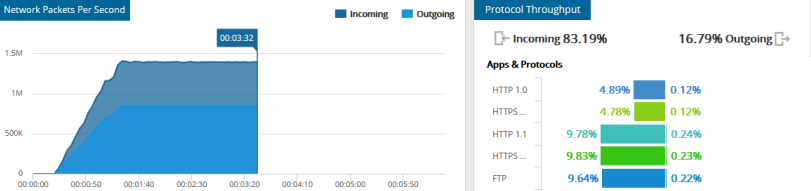
点击绿色的三角开始运行。运行状态如下：

Duration: hh:mm:ss **54%** ~ 00:02:58 [View Report](#) [Download](#)

Test Criteria Charts



Live Charts



Traffic Mix Data

Protocol	Incoming BW	Outgoing BW	Actual/Goal	Successful Transactions	Unsuccessful Transactions	Attempted Transactions
HTTP 1.0	880.85 Mbps	22.03 Mbps	5.02% / 5%	171 664	0	171 664
HTTPS 1.0	861.26 Mbps	21.85 Mbps	4.91% / 5%	87 000	0	87 004
HTTP 1.1	1.76 Gbps	42.72 Mbps	10.02% / 10%	341 968	0	341 968
HTTPS 1.1	1.77 Gbps	42.16 Mbps	10.06% / 10%	172 283	0	172 285
FTP	1.73 Gbps	39 Mbps	9.85% / 10%	68 720	0	68 720
Telnet	8.96 Mbps	8.92 Mbps	0.1% / 0.1%	24 760	0	24 760
SMTP	47.99 Mbps	2.13 Gbps	12.08% / 12%	82 378	0	82 384
POP3	1.72 Gbps	44.36 Mbps	9.81% / 9.8%	323 966	0	323 972
CIFS/SMB	1.39 Gbps	34.78 Mbps	7.0% / 8%	45 596	0	45 597
IMAP4	1.61 Gbps	35.85 Mbps	9.12% / 9%	69 084	0	69 085
RTSP	710.99 Mbps	11.38 Mbps	4.01% / 4%	137 014	0	137 674
SIP	540.76 Mbps	539.34 Mbps	6% / 6%	289 331	0	289 509
BitTorrent	1.94 Gbps	41.45 Mbps	11% / 11%	51 994	0	52 394
Exchange	6.16 Mbps	11.84 Mbps	0.1% / 0.1%	36 224	0	36 486

Port to Subnet Mapping

Port	Subnets
1/1	10.1.0.2 - 10.1.0.254
1/2	10.1.1.2 - 10.1.1.254

测试报告

测试结束后点击 View Report 生成测试报告。

A Actual bandwidth never fell below the specified goal of 3% of 18 Gbps over the total duration** of the test. Apps and Protocols Transactions never fell below the specified goal of 3% of Total Apps and Protocols Transactions over the total duration** of the test.

* This score is calculated by taking the specified criteria goal defined in the test and measuring if they met or failed the minimum requirement set and averaging the amount of time data fell below the goal. A = 95% and above, B = 85%, C = 75%, D = 65%, E = 55% and below.
** Duration is the total test time, excluding everything up to the Ramp-up and after the Ramp-down.

Summary

Created By	Test Name	Number Of Traffic Mix
dem@quest.com	Throughput with Mixed Traffic - CF20	14

Queue Name	Started at	Finished at	Vol. for Server Bandwidth	Measurement
Blank	2019-0-10 11:00:25	2019-0-10 11:17:15	18 Gbps	Bandwidth

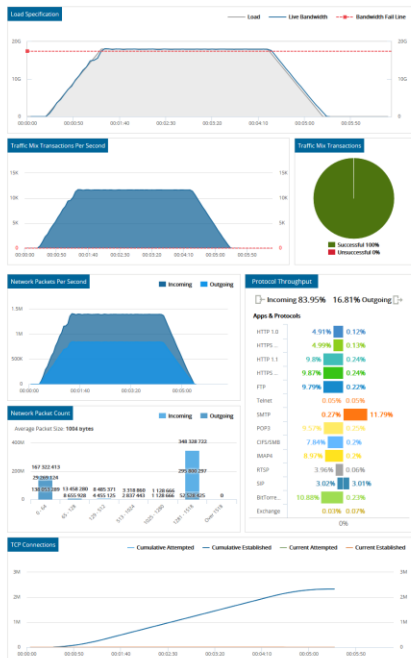
Client Sent	Server Received	Server Sent	Client Received	Average Throughput
90.72 GB	90.72 GB	453.42 GB	453.42 GB	17.95 Gbps

Enclosed	Passed	Failed
2,822,092 Connections	100% (2,822,092 Connections)	0% (0 Connections)

Network Profile Configuration

Client Network	Server Network
IPv4 Max Segment: 1460 B	IPv4 Max Segment: 1460 B
IPv6 Max Segment: 1460 B	IPv6 Max Segment: 1460 B
Receive Window: 32768 B	Receive Window: 32768 B
Retries: 2	Retries: 2
Delayed Ack Timeout: 200 ms	Delayed Ack Timeout: 200 ms
Delayed Ack: 2920 B	Delayed Ack: 2920 B
Port Range: 1024 - 65535	

Charts



Traffic Mix Data

Protocol	Incoming MB	Outgoing MB	Actual/Goal	Successful Transactions	Unsuccessful Transactions	Attempted Transactions
HTTP 1.0	884.63 Mbps	22.12 Mbps	5.04%/3%	254,503	0	254,503
HTTP 1.1	886.55 Mbps	22.79 Mbps	5.12%/3%	128,512	0	128,512
FTP	1.76 Gbps	42.8 Mbps	10.07%/3%	507,872	0	507,872
POP3	1.72 Gbps	44.39 Mbps	9.82%/3%	480,800	0	480,800
SMTP	47.88 Mbps	2.12 Gbps	12.05%/3%	122,264	0	122,264
Exchange	6.58 Mbps	11.87 Mbps	0.14%/3%	54,060	0	54,060

Port Interfaces

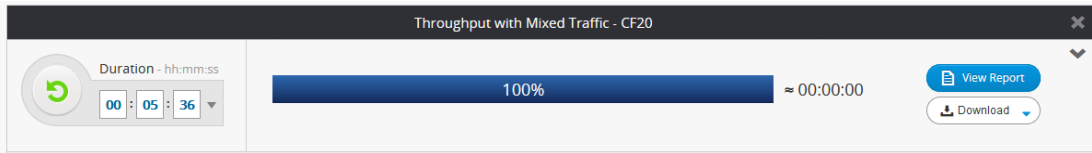
Port Interface	Protocol	Incoming MB	Outgoing MB	Actual/Goal	Successful Transactions	Unsuccessful Transactions	Attempted Transactions
v11	HTTP 1.0	884.63 Mbps	22.12 Mbps	5.04%/3%	254,503	0	254,503
	HTTP 1.1	886.55 Mbps	22.79 Mbps	5.12%/3%	128,512	0	128,512
	FTP	1.76 Gbps	42.8 Mbps	10.07%/3%	507,872	0	507,872
	POP3	1.72 Gbps	44.39 Mbps	9.82%/3%	480,800	0	480,800
	SMTP	47.88 Mbps	2.12 Gbps	12.05%/3%	122,264	0	122,264
	Exchange	6.58 Mbps	11.87 Mbps	0.14%/3%	54,060	0	54,060

Port to Subnet Mapping

Port	Subnets
v11	10.1.1.2 - 10.1.1.254
v12	10.1.1.2 - 10.1.1.254

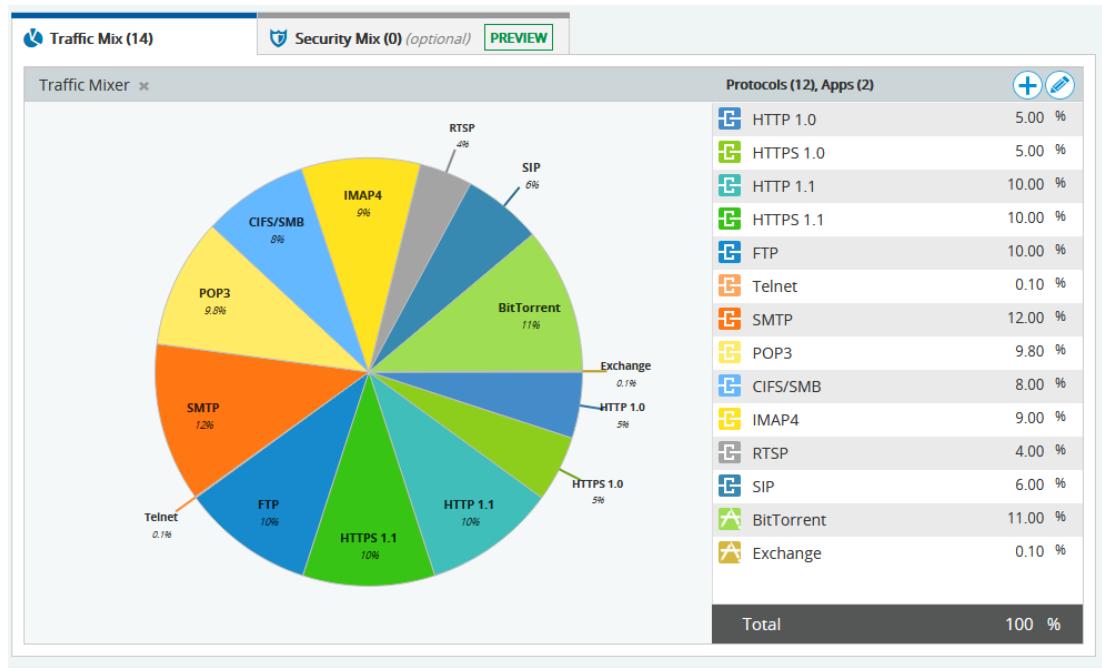
测试重新运行和编辑

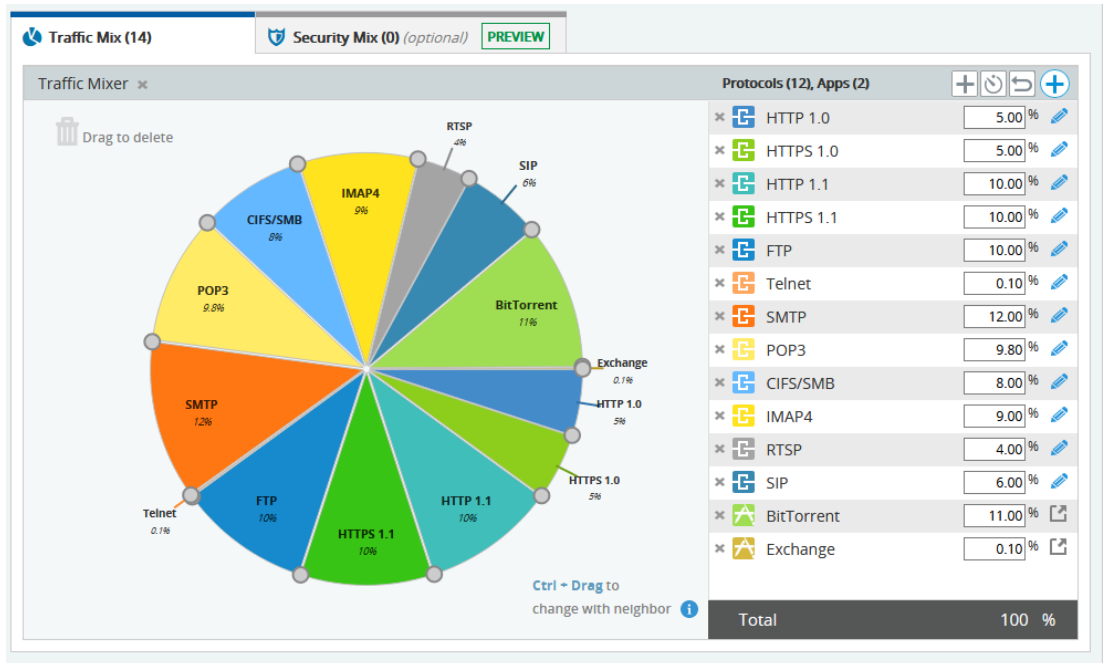
测试结束后，点击绿色的循环按钮可以重跑一遍测试。点击右上角的 X 返回并编辑测试配置。



增加应用场景

点击右上角的铅笔图标编辑业务配置。





增加新应用。

HTTPS 1.0

里面的 X 删除应用，铅笔编辑或者

查看配置。

退出

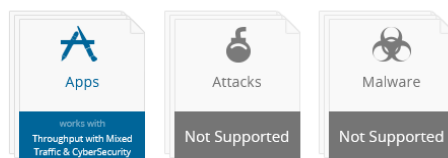
撤销

增加应用

以增加微信业务为例：

点击 进入应用选择，点击 APPS。

Create Mix Scenario Profile



Cancel

进入 App Scenarios

Create Mix Scenario Profile

App Scenarios: 9744 App Scenarios

Predefined App Profiles: 78 App Profiles

Cancel

Create Mix Scenario Profile

Import Scenario Show Filters Search App Scenarios

Business Systems 367: Adobe, Sharepoint, MYSQL ...

Communication 1132: Skype, IMAP, Jabber ...

Games And Entertainment 180: FarmVille, Battlefield, Mafia Wars ...

Miscellaneous 2767: Fandango, eBay, Kayak ...

Network Protocols 100: Diameter, Telnet, Molbus ...

P2P 987: BitTorrent, Gnutella, eDonkey ...

Productivity 379: Box, Drupal, Google Finance ...

Social Networking 1349: Facebook, Twitter, Instagram ...

Streaming Media 2457: Netflix, Youtube, Pandora ...

Cancel

搜索 wechat,

Create Mix Scenario Profile

Import Scenario Show Filters wechat

38 Found Filtering by: No Filters are applied

<input type="checkbox"/>	Add Selected	Scenario Name	Encryption	Client Name	Client Version	Last Updated	NAT Supported	
<input type="checkbox"/>	Add to Profile	WeChat: Login, send file and logout (01) This scenario contains user-initiated operations of WeChat on an iPad. The user logs on to WeChat, selects a friend,	N/A	WeChat	4.5.0.11	06/27/2013		
<input type="checkbox"/>	Add to Profile	WeChat: Login, send file and logout (02) This scenario contains user-initiated operations of WeChat on an iPhone. The user logs on to WeChat, selects a friend,	N/A	WeChat	4.5.0.11	06/27/2013		
<input type="checkbox"/>	Add to Profile	WeChat: Login, chat, voice chat, video call and I... This scenario contains user-initiated operations of WeChat on an iPhone 5. The user logs on to WeChat, selects a	N/A	WeChat	6.0.1	02/24/2015		
<input type="checkbox"/>	Added	WeChat: Login, chat, voice chat, video call and I... This scenario contains user-initiated operations of WeChat on an iPhone 4. The user logs on to WeChat, selects a	N/A	WeChat	6.0.1	02/24/2015		
<input type="checkbox"/>	Add to Profile	WeChat: Login, chat, voice chat, video call and I... This scenario contains user-initiated operations of WeChat on an iPhone 4. The user logs on to WeChat, selects a	N/A	WeChat	6.1	04/09/2015		

1 added

Cancel Save Profile

选中需要的场景并点击 Add to Profile, 保存为 Wechat App Profile。

Save App Profile

Scenarios (1)

01 WeChat: Login, chat, voice chat, video call and logout (02)

Profile Name

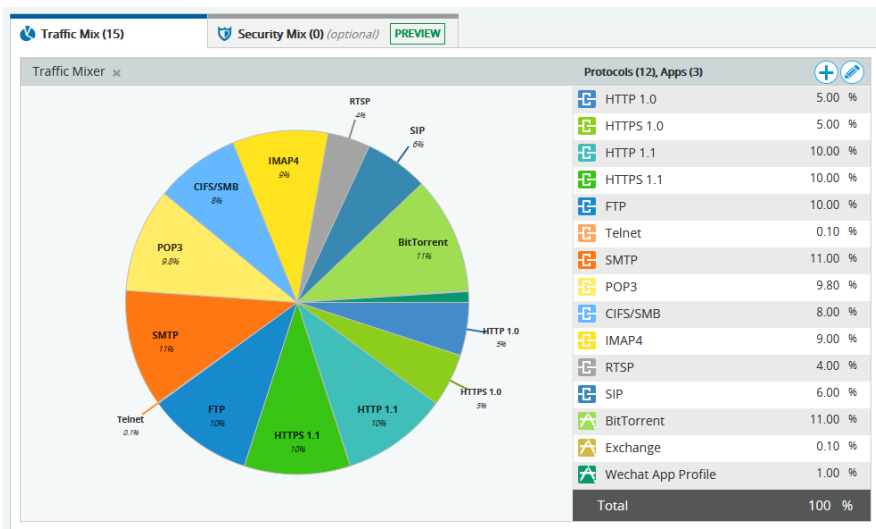
Wechat App Profile

Description (Optional) 140

New App Profile

Cancel · Save

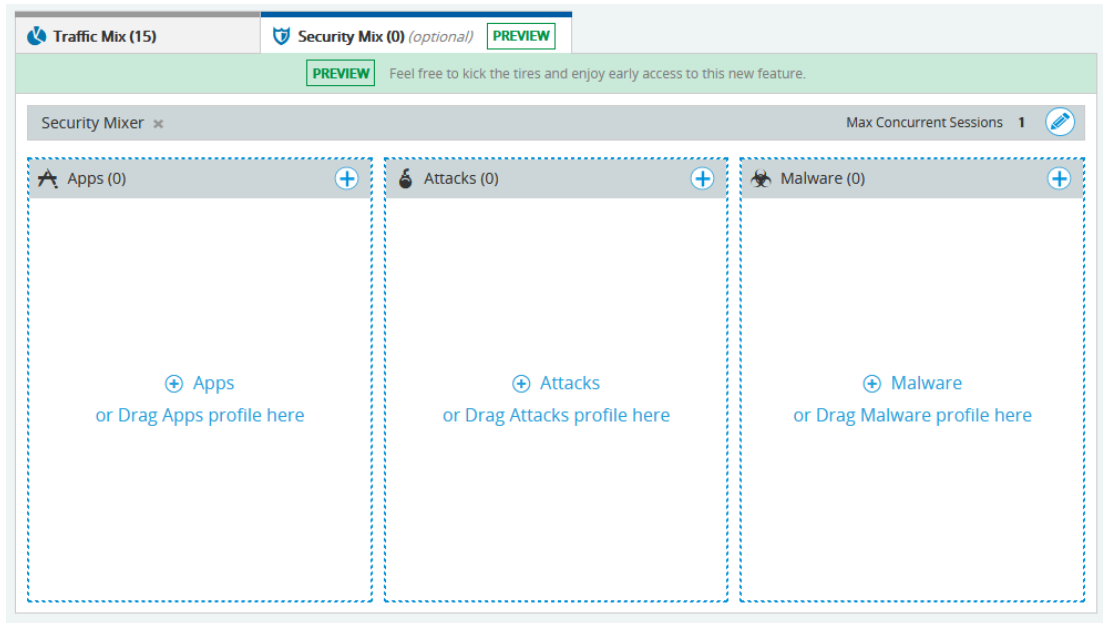
可以看到应用中多了微信场景。



增加网络攻击和恶意软件

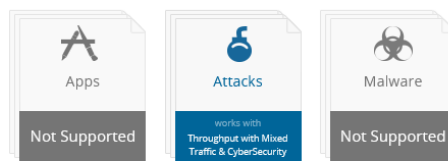
除了混合多种应用之外，也可以混合攻击病毒等内容。

进入 Security Mix



点击+ Attacks 增加攻击内容。

Create Mix Scenario Profile



Cancel

选择 Attack Scenarios

Create Mix Scenario Profile



Cancel

Create Mix Scenario Profile

Import Scenario

3073 Found

<input type="checkbox"/> Add Selected	Scenario Name	CVE ID	Severity	Last Updated	
<input type="checkbox"/> Add to Profile	Microsoft Internet Explorer Cross Frame Scripting Restriction ... There is a vulnerability in the way Internet Explorer, a web browser developed and maintained by Microsoft Corporation, handles interaction	2004-2383	High	02/07/2018	▼
<input type="checkbox"/> Add to Profile	Oracle Web Cache Unspecified Client Request Handling The Oracle Web Cache contains several vulnerabilities. These vulnerabilities enable attackers to falsify log data, to perform Cross-Site Scripting attacks	2004-0385	Moderate	02/07/2018	▼
<input type="checkbox"/> Add to Profile	Microsoft showHelp Vulnerability There is a vulnerability in the way Microsoft's HTML help system validates .chm files. The URI parameter to this system through the showHelp method	2003-1041	High	02/07/2018	▼
<input type="checkbox"/> Add to Profile	Microsoft Exchange OWA XSS and Spoofing Vulnerability There is vulnerability in Microsoft Outlook Web Access, a component of Microsoft Exchange, in the validation of user input. This vulnerability could	2004-0203	Moderate	02/07/2018	▼
<input type="checkbox"/> Add to Profile	Microsoft Windows Graphics Rendering Engine Buffer Overflow A vulnerability exists in the Microsoft Windows Graphics Rendering Engine. The vulnerability exists in the routines that handle the parsing of the	2004-0209	High	02/07/2018	▼

Cancel

搜索 Flash，找到 51 种，选择并保存。

Create Mix Scenario Profile

Import Scenario

51 Found

<input type="checkbox"/> Add Selected	Scenario Name	CVE ID	Severity	Last Updated	
<input type="checkbox"/> Added	Adobe Flash Player Memory Corruption A code execution vulnerability exists in Adobe Flash Player 10 and the authplay.dll file that ships with Adobe Reader and Acrobat X products. The	2011-0609	High	02/07/2018	▼
<input type="checkbox"/> Added	Adobe Flash Player MP4 File Memory Corruption A memory corruption vulnerability exists in Adobe Flash Player. The vulnerability is due to insufficient validation of a user-supplied length value	2012-0753	High	02/07/2018	▼
<input type="checkbox"/> Added	Adobe Flash Player Shader Memory Corruption A code execution vulnerability exists in Adobe Flash Player. The vulnerability is due to a memory corruption error while processing crafted Shader	2014-0515	High	02/07/2018	▼
<input type="checkbox"/> Added	Adobe Flash MP3 ID3 Tag Integer Overflow An integer overflow vulnerability has been reported in Adobe Flash. The vulnerability is due to an issue with parsing ID3 tag data. A remote attacker	2015-5560	High	02/07/2018	▼
<input type="checkbox"/> Added	Adobe Flash Player FileReference Type Confusion A type confusion vulnerability has been reported in Adobe Flash. This vulnerability is due to improper validation of properties in FileReference	2016-1105	High	02/07/2018	▼

51 added

Cancel

Save Attacks Profile

Scenarios (51)

- 01 Adobe Flash Player Memory Corruption
- 02 Adobe Flash Player MP4 File Memory Corruption
- 03 Adobe Flash Player Shader Memory Corruption
- 04 Adobe Flash MP3 ID3 Tag Integer Overflow
- 05 Adobe Flash Player FileReference Type Confusion
- 06 Adobe Flash Player Rectangle Use After Free
- 07 Adobe Flash Player FLV Processing Buffer Overflow

Profile Name

Attacks: Flash

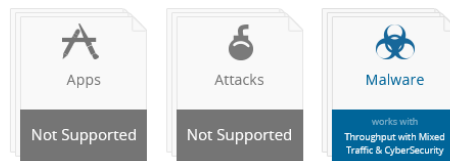
Description (Optional) 140

New Attacks Profile

Cancel · Save

同样的，增加恶意软件。

Create Mix Scenario Profile



Cancel

Create Mix Scenario Profile

Import Scenario

773 Found

Add Selected

Add to Profile

Added

Added

2 added

Cancel · Save Profile

Save Malware Profile

Scenarios (2)

- 01 Trojan-Downloader.Win32.Banload.ykl
- 02 Trojan.Lineage.Gen.Pac.3

Profile Name

Malware: Profile 1

Description (Optional) 140

New Malware Profile

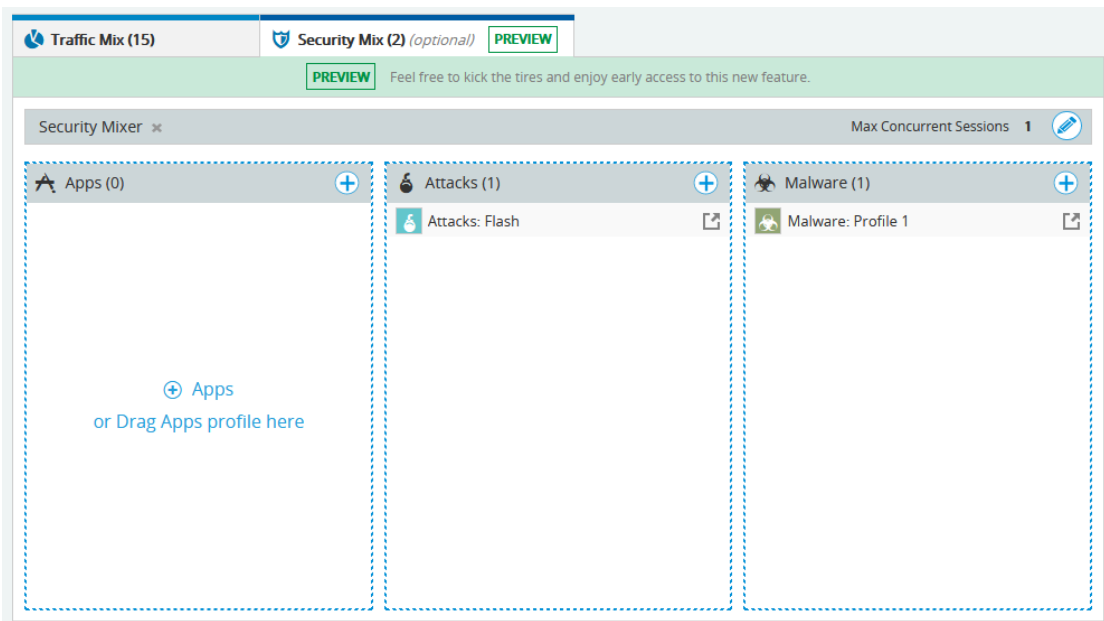
Cancel · Save

Last Updated	Advanced Malware
09/27/2016	
09/27/2016	
09/27/2016	
09/27/2016	
01/07/2009	09/27/2016

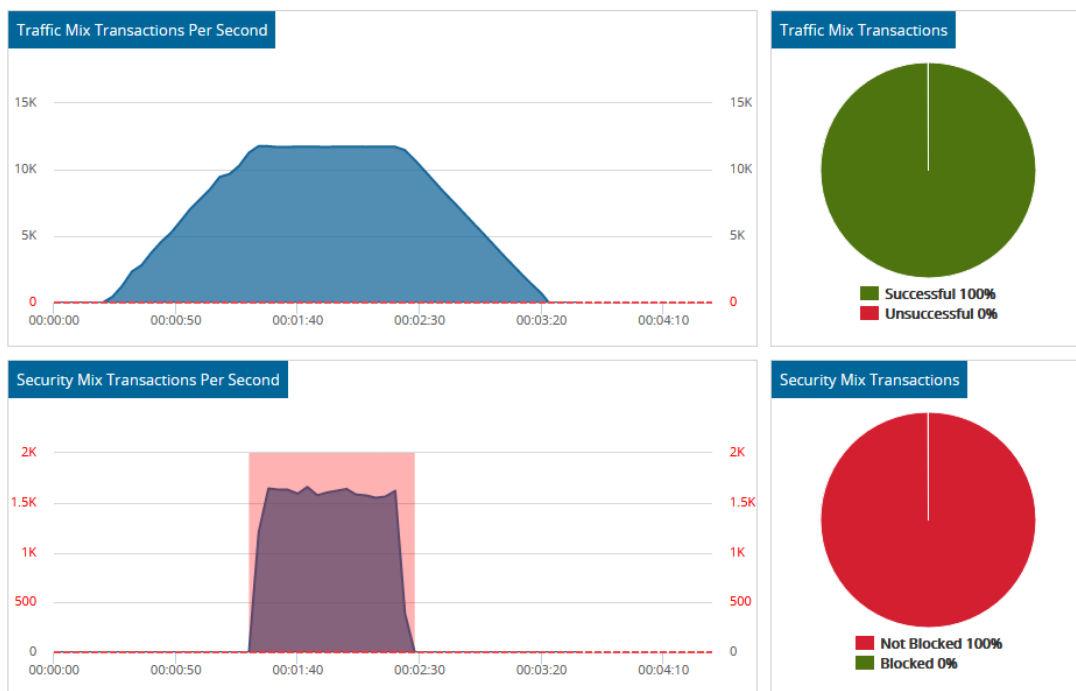
Trojan.Lineage.Gen.Pac.3 is a Trojan application that installs malicious files and libraries on the system and requests malicious

Trojan-Downloader.Win32.Banload.aajs

效果如图。默认最大并发是 1。



运行测试并观察结果。



Security Mix Data

Attacks Data

Protocol	Incoming BW	Outgoing BW	Not Blocked Transactions	Blocked Transactions	Attempted Transactions
Attacks: Flash	338.2 Mbps	12.84 Mbps	69 105	0	69 105

Malware Data

Protocol	Incoming BW	Outgoing BW	Not Blocked Transactions	Blocked Transactions	Attempted Transactions
Malware: Profile 1	620.22 Mbps	13.8 Mbps	27 236	0	27 236

3. HTTP 新建测试

选择 HTTP Connection Per Second 模板，建立测试。

The screenshot shows the Test Builder interface. On the left is a navigation menu with categories: Performance, Capacity, and Security. Under Performance, 'HTTP Connections Per Second' is highlighted. The main content area features a green wrench icon and the title 'HTTP Connections Per Second'. Below the title is a description: 'Create tests to achieve industry's leading TCP state generation to confirm connections per second.' A section titled 'Why run this test?' contains two items: 'Measure new connections' (with a server rack icon) and 'Test with stateful traffic' (with a laptop icon). A blue 'Build a New Test' button is located at the bottom right of the main content area.

配置测试队列，子网，压力模型。

HTTP Connections Per Second 1

Duration - hh:mm:ss: **00 : 04 : 00**

Load Specification: Connections Per Second (824 K)

Fail test if: Connections Per Second falls below 824 K by 1% OR Failed Transactions reach 3%

Debug Packet Trace: **Off**

Client Only | Client/Server | Brave (2 ports)

Client Subnets (1): IPv4 Sub... (1 port)

Virtual Routers: Virtual (optional)

DUT

Server Subnets (1): IPv4 Sub... (1 port)

Pair | Backbone

Client Network		Server Network	
IP4 Max Segment:	1460 bytes	Fragment Reassembly Timer:	30000 ms
IP6 Max Segment:	1440 bytes	Port Range Lower Bound:	1024
Delayed Ack:	OFF	Port Range Upper Bound:	65535
Retries:	5	Port Randomization:	OFF
Inactivity Timer:	70000 ms	Gratuitous ARP:	ON
Receive Window:	32768 bytes	Congestion Control:	ON
		IP4 Max Segment:	1460 bytes
		IP6 Max Segment:	1440 bytes
		Delayed Ack:	2920 bytes
		Delayed Ack Timeout:	200 ms
		Retries:	2
		Inactivity Timer:	0 ms
		Receive Window:	32768 bytes
		Port Randomization:	OFF
		Gratuitous ARP:	ON
		Congestion Control:	ON

检查或调整 HTTP 层参数。

HTTP

HTTP Version: 1.1

Client

Method: GET

User-Agent Header: Mozilla/4.0 (compatible MSIE 5.01; Windows NT)

Connection Type: Separate Connections

Max Requests Per Connection: 999

Max Connections Per Server: 999

Server

Server Port (TCP): 80

Response Body Type: Fixed/ASCII

File Size: 1 Bytes

Server Type: Jetty/4.2.9rc2 (SunOS/5.8 sparc java/1.4.1_04)

ToS (HEX): 00

Connection Termination: RST

Supplemental Settings

Security (SSL/TLS): OFF

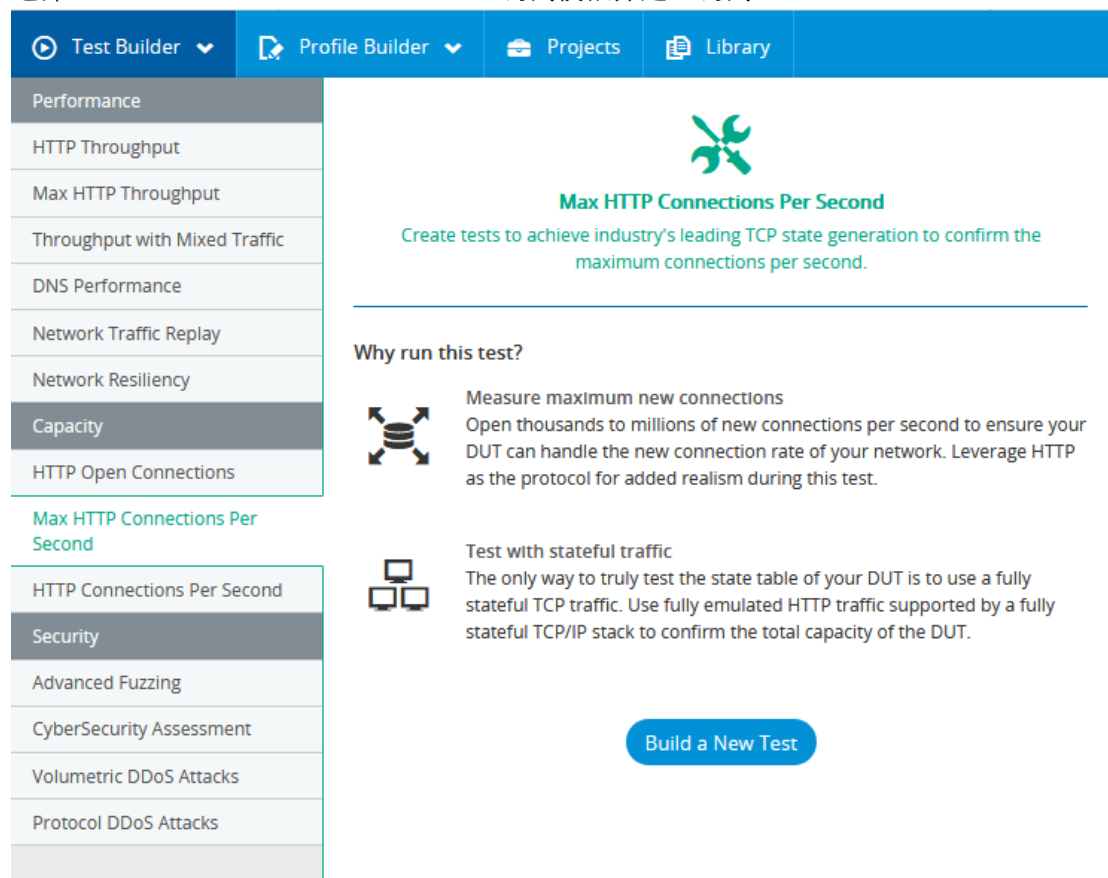
Proxy: NO

Authentication: OFF

执行测试。

4. 最大 HTTP 新建测试

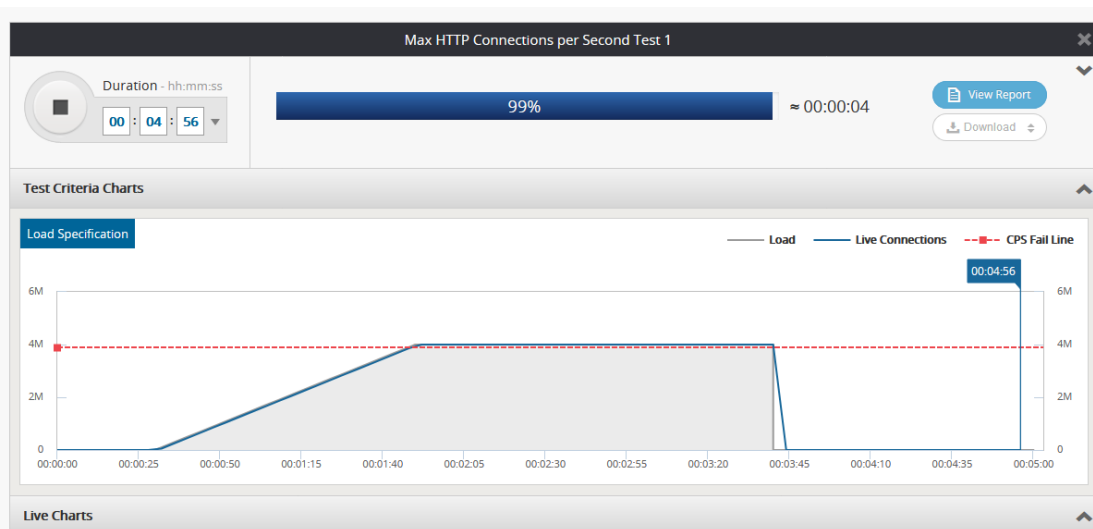
选择 Max HTTP Connection Per Second 测试模板并建立测试。



The screenshot shows the Test Builder interface. On the left is a navigation menu with categories: Performance, Capacity, Security. Under Performance, 'Max HTTP Connections Per Second' is highlighted. Under Capacity, 'HTTP Open Connections' is highlighted. Under Security, 'Advanced Fuzzing', 'CyberSecurity Assessment', 'Volumetric DDoS Attacks', and 'Protocol DDoS Attacks' are listed. The main area displays the 'Max HTTP Connections Per Second' test template. It features a green wrench icon and the text: 'Max HTTP Connections Per Second. Create tests to achieve industry's leading TCP state generation to confirm the maximum connections per second.' Below this, under 'Why run this test?', there are two points: 1. 'Measure maximum new connections' with a server rack icon, explaining that it tests thousands to millions of new connections per second to ensure DUT capacity. 2. 'Test with stateful traffic' with a server rack icon, explaining that it tests the state table of the DUT using fully emulated HTTP traffic. A blue button 'Build a New Test' is at the bottom right.

配置测试队列，子网，端口等内容。

默认性能为一个核心 100 万新建，根据实际设备的情况调整。
运行测试并观察结果。



5. 网络攻击：Bash 破壳漏洞

Bash 破壳漏洞（Shell Shock）攻击是影响广泛的系统漏洞，CVSS 评分为 10 分，危害性为最高。

Bash 是 Linux 用户广泛使用的一款用于控制命令提示符工具，导致该漏洞影响范围甚广。同时，当 HTTP 服务开放 CGI 服务或其他地方引用 bash 时可直接导致远程命令执行漏洞。主要影响系统为 Redhat、Centos、Ubuntu、Debian、Suse 等主流 Linux 操作系统。


漏洞危害主要表现在：影响基于 bash 开放的服务、程序。当网站利用 CGI 执行 bash 后可导致攻击者远程执行系统命令，从而可以利用系统命令反弹 shell 之后进行内网渗透、挂马、篡改主页、脱库等行为。

CyberFlood 中 Bash shell shock 的描述

A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment variables. A remote attacker can exploit this vulnerability by interacting with an application that uses Bash environment variables. If an attacker can control the value of an environment variable, then command execution can be achieved in the context of the application using the environment variable.

攻击元数据 ¹	
属性	值
Severity	Critical
"CVE ID"	2014-6271

攻击描述



GNU Bash Environment Variable Handling Command...

[View Ca...](#)

Description

A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment variables. A remote attacker can exploit this vulnerability by interacting with an application that uses Bash environment variables. If an attacker can control the value of an environment variable, then command execution can be achieved in the context of the application using the environment variable.

Severity

Updated

CVE ID

Secunia

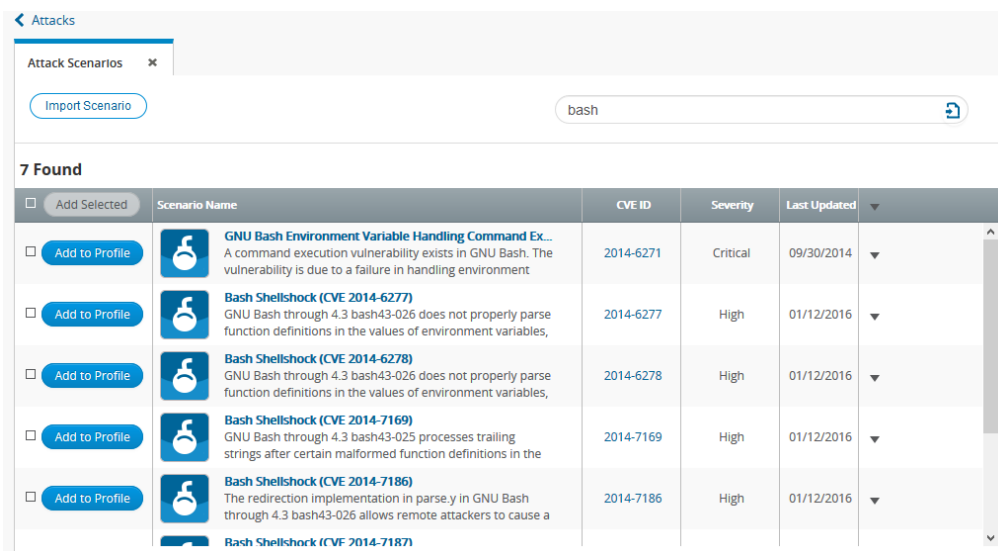
Bugtraq

NAT Support

Created By

用 CyberFlood 仿真 CVE 2014-6271 攻击

1. 搜索 bash 相关的攻击，找到多个相关漏洞



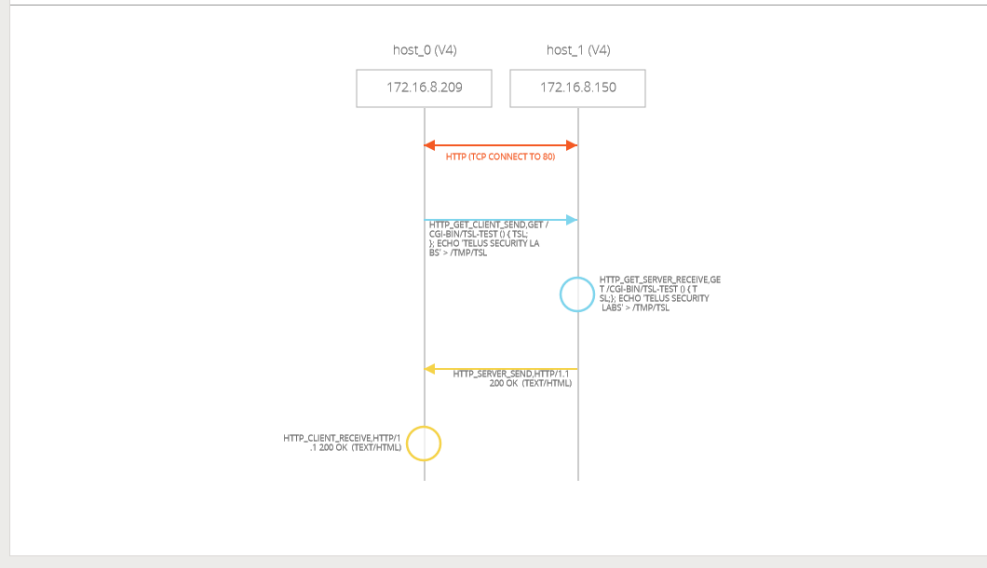
The screenshot shows the 'Attacks' section of the CyberFlood interface. A search bar contains the text 'bash'. Below the search bar, it indicates '7 Found' results. The results are displayed in a table with columns for 'Scenario Name', 'CVE ID', 'Severity', and 'Last Updated'. Each row includes an 'Add to Profile' button.

Scenario Name	CVE ID	Severity	Last Updated
GNU Bash Environment Variable Handling Command Ex... A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment	2014-6271	Critical	09/30/2014
Bash Shellshock (CVE 2014-6277) GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables,	2014-6277	High	01/12/2016
Bash Shellshock (CVE 2014-6278) GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables,	2014-6278	High	01/12/2016
Bash Shellshock (CVE 2014-7169) GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the	2014-7169	High	01/12/2016
Bash Shellshock (CVE 2014-7186) The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a	2014-7186	High	01/12/2016
Bash Shellshock (CVE 2014-7187)			

2. 查看攻击对应的报文流程

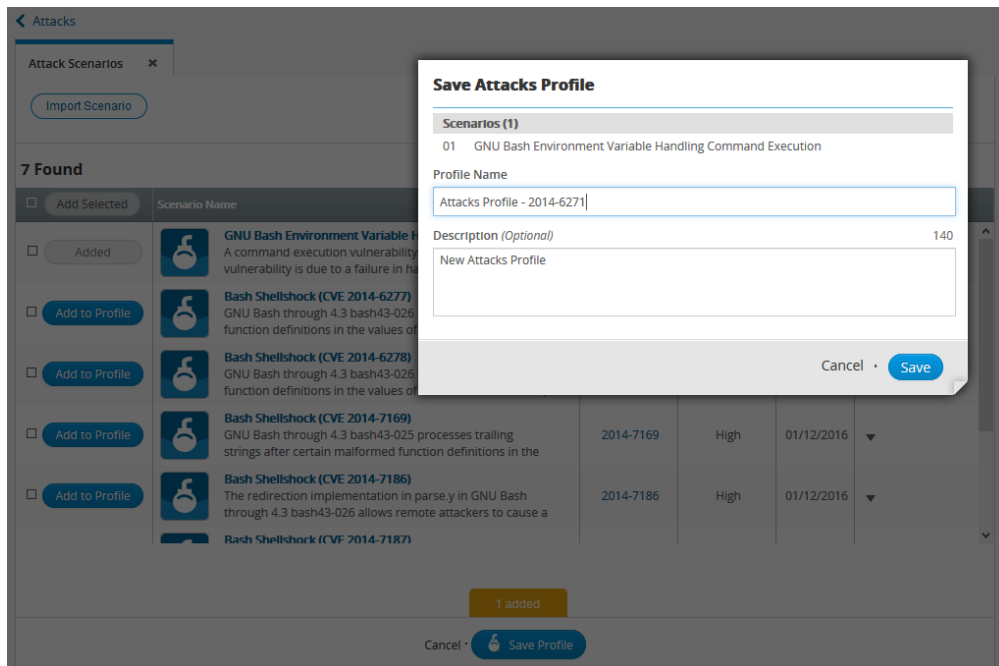
Summary

ID: 04.2014.09.20140924-07
 Description: A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment variables. A remote attacker can exploit this vulnerability by interacting with an application that uses Bash environment variables. If an attacker can control the value of an environment variable, then command execution can be achieved in the context of the application using the environment variable.
 Category: Attacks
 Hosts: 2
 Steps: 5



3. 配置 Cyber Security Assessment，发送攻击

1.) 建议一个攻击 profile。



2.) 配置 Cyber Security Assessment。把 *Attack Profile 2014-6271* 从左边拽到右边 detect 模式下。

配置 subnet 和网关。

- Client IP 地址范围 4.3.2.10 - 4.3.2.209，网关 4.3.2.1。
- Server IP 地址范围 192.168.10.10 - 192.168.10.209，网关 192.168.10.1。

IPv4 Subnet Profile Editor

The First Address /

Count

Force Server IP Count Off

* Server Subnet Profiles only. Not supported in Client Subnet Profiles.

Default Gateway On

IP

▶ Advanced Settings

Static Routing + Add Static Routing

VLAN + Add VLAN

Save as Separate Profile Cancel Update Player

3.) 选择队列和端口。打开抓包选项

CyberSecurity Assessment - CVE 2014-6271

Start Delay Sec

Prevent Scenario (0)

Detect Scenario (1) Attacks Profile - 2014-6271

Background Traffic OFF

Enable PCAP

Test Criteria

Test Mode Single Direction Both Directions

Test Queue

Client Subnets (1)

Server Subnets (1)

Enable NAT Off

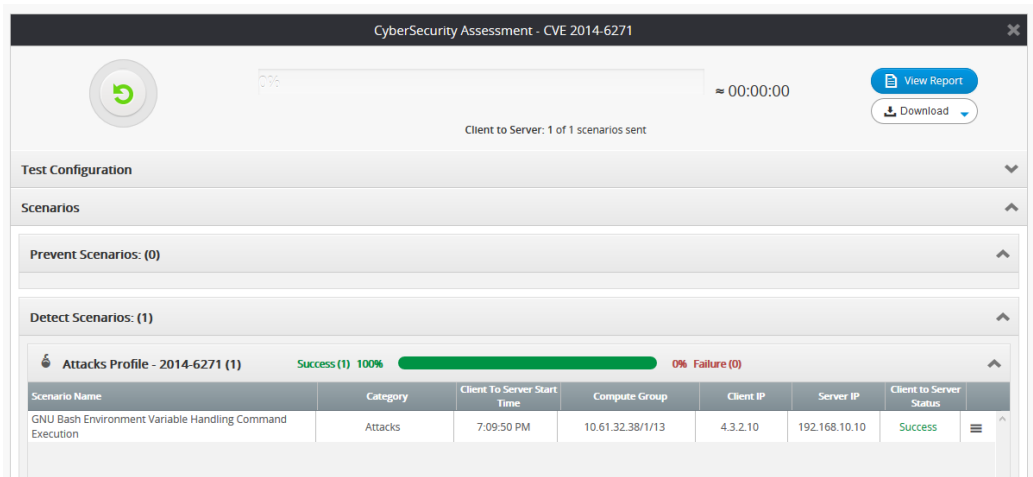
Scenario profiles

Prevent Scenarios 0 total / 0 selected Hide not selected

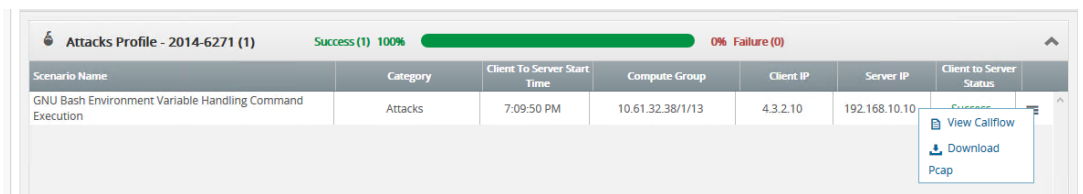
Detect Scenarios 1 total / 1 selected Hide not selected

Attacks Profile - 2014-6271 1 total / 1 selected

4.) 运行测试，查看结果。



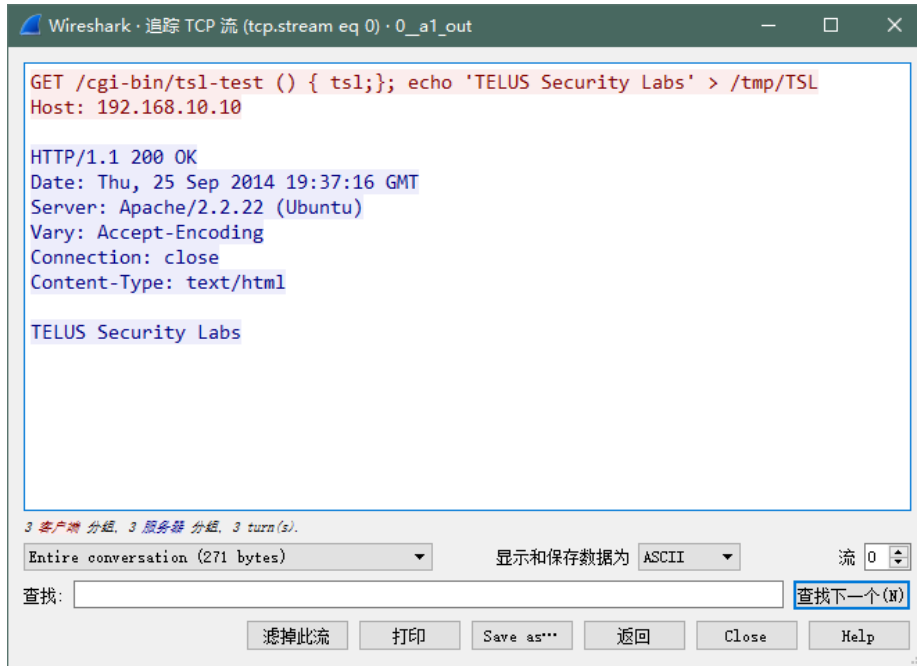
5.) 下载运行时报文。



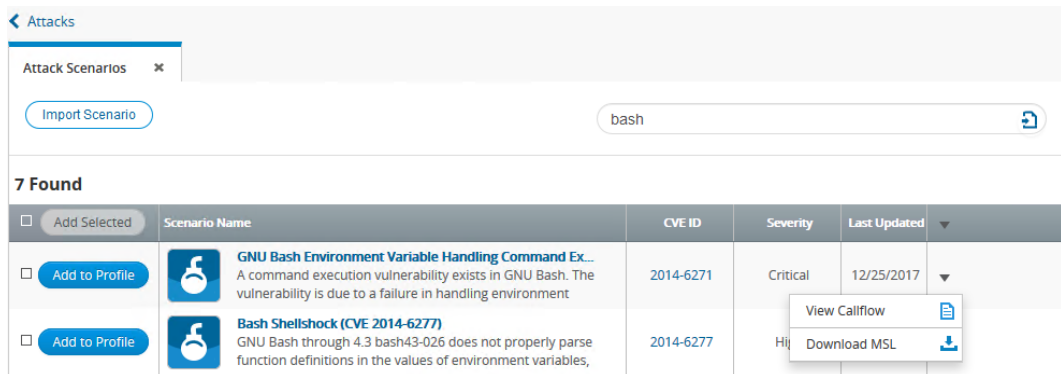
6.) 分析报文

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	4.3.2.10	192.168.10.10	TCP	58	1024 → 80 [SYN] Seq=0 Win=2048 Len=0 WS=512
2	0.011997	192.168.10.10	4.3.2.10	TCP	60	80 → 1024 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 WS=512
3	0.023010	4.3.2.10	192.168.10.10	TCP	54	1024 → 80 [ACK] Seq=1 Ack=1 Win=1048576 Len=0
4	0.023010	4.3.2.10	192.168.10.10	HTTP	150	GET /cgi-bin/ssl-test () { ts1; }; echo 'TELUS Security Labs' > /tmp/SSL
5	0.035000	192.168.10.10	4.3.2.10	TCP	60	80 → 1024 [ACK] Seq=1 Ack=97 Win=1048576 Len=0
6	0.035000	192.168.10.10	4.3.2.10	TCP	229	80 → 1024 [PSH, ACK] Seq=1 Ack=97 Win=1048576 Len=175 [TCP segment of a reassembled PDU]
7	0.047013	4.3.2.10	192.168.10.10	TCP	54	1024 → 80 [ACK] Seq=97 Ack=176 Win=1048576 Len=0
8	0.047013	4.3.2.10	192.168.10.10	TCP	54	1024 → 80 [RST, ACK] Seq=97 Ack=176 Win=1048576 Len=0
9	0.047013	192.168.10.10	4.3.2.10	TCP	60	80 → 1024 [RST, ACK] Seq=176 Ack=97 Win=1048576 Len=0

跟踪一条业务流。注意观察请求的 URL 内容。



7.) 下载并分析报文 ms1 文件，查看规则。



通过文本编辑器打开 ms1，查看攻击原理。

```

steps {
  HTTP = tcp(src: &host_0, dst: &host_1, dst_port: 80)

  # GET /cgi-bin/tsl-test () { tsl;}; echo 'TELUS Security Labs' > /tmp/TSL
  HTTP_GET_Client_Send = HTTP.client_send {
    # http|Hypertext Transfer Protocol
    struct [
      "GET /cgi-bin/tsl-test () { tsl;}; echo \"TELUS Security Labs\" > /tmp/TSL\r\n"
      "Host: #{@HTTP.dst_ip}\r\n"
      "\r\n"
    ]
  }

  # GET /cgi-bin/tsl-test () { tsl;}; echo 'TELUS Security Labs' > /tmp/TSL
  HTTP_GET_Server_Receive = HTTP_GET_Client_Send.server_receive

  # HTTP/1.1 200 OK (text/html)
  HTTP_Server_Send = HTTP.server_send {
    # http|Hypertext Transfer Protocol
    struct [
      "HTTP/1.1 200 OK\r\n"
      "Date: Thu, 25 Sep 2014 19:37:16 GMT\r\n"
      "Server: Apache/2.2.22 (Ubuntu)\r\n"
      "Vary: Accept-Encoding\r\n"
      "Connection: close\r\n"
      "Content-Type: text/html\r\n"
      "\r\n"
      content_1 = "TELUS Security Labs\r\n"
    ]
  }
}

```

2. 观察 snort 防火墙的告警

PfSense 可以安装 snort 防火墙。通过 Services -> Snort -> Alerts 查看 Snort 的安全日志。可以看到 snort 的告警为 *UNESCAPED SPACE IN HTTP URI* 和 *INVALID CONENTE-LENGTH OR CHUNK SIZE*。

可以看出 snort 并没有检测出这个攻击。属于漏报攻击。对于靶场，这是一个很好的素材，需要认真分析规则库的内容，判断是规则没有更新还是规则的内容无法识别该攻击。

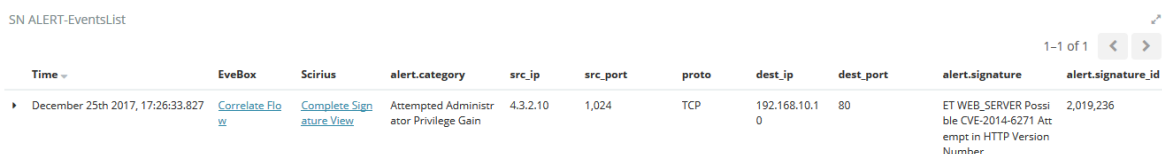
The screenshot shows the PfSense web interface for Snort Alerts. The 'Alert Log View Settings' section is configured for the 'WAN' interface, with 'Auto-refresh view' disabled and 'Alert lines to display' set to 250. Below this, the 'Alert Log View Filter' is empty. The 'Last 250 Alert Log Entries' table shows the following data:

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-12-25 01:26:19	3	TCP	Unknown Traffic	4.3.2.10	1024	192.168.10.10	80	120:8	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE
2017-12-25 01:26:19	3	TCP	Unknown Traffic	192.168.10.10	80	4.3.2.10	1024	119:32	(http_inspect) SIMPLE REQUEST
2017-12-25 01:26:19	3	TCP	Unknown Traffic	4.3.2.10	1024	192.168.10.10	80	119:33	(http_inspect) UNESCAPED SPACE IN HTTP URI

3. 观察 suricata 的告警

我们使用了 SELKS 内置的 suricata，版本是 4.0.0。

1.) 通过 SELKS 的 Kibana 看到一条安全日志，显示源 IP 是 4.3.2.10，目的 IP 是 192.168.10.10，目的端口是 80。告警的签名是 *ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number*



Time	EveBox	Scirius	alert.category	src_ip	src_port	proto	dest_ip	dest_port	alert.signature	alert.signature_id
December 25th 2017, 17:26:33.827	Correlate Flow	Complete Signature View	Attempted Administrator Privilege Gain	4.3.2.10	1,024	TCP	192.168.10.10	80	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number	2,019,236

2.) 点击 *Complete Signature View* 查看具体触发了那条规则。



ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number

References

- [Uri: blogs.akamai.com/2014/09/environment-bashing.html](http://blogs.akamai.com/2014/09/environment-bashing.html)

Statistics Information History

Definition

```
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number"; flow:established,to_server; content:"|20 28 29 20 7b|"; fast_pattern:only; pcre:"/^[^s]+s+[^\s]+\x28\x29\x20\x7b[^\r\n]*\r?$/m"; reference:url,blogs.akamai.com/2014/09/environment-bashing.html; class type:attempted-admin; sid:2019236; rev:3; metadata:created_at 2014_09_25, updated_at 2014_09_25;)
```

3.) 通过分析，这条规则检查内容中的 `| 20 28 29 20 7b|`。这是 suricata 语法，即检查 `raw_bytes`。这 5 个字节对应 “ () { ”。

4.) 点击 Statistics，查看该规则的统计。规则在 24 号和 25 号都触发过，这是因为我们反复用这条攻击做测试。在实战中如果某一规则反复触发，需要特别引起关注。

ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number

References

- Uri: blogs.akamai.com/2014/09/environment-bashing.html

Statistics Information History

Hits by host (last 24h)

Host	Count
SELKS	6

Source IP (last 24h)

Host	Count	Actions
4.3.2.10	6	+

Destination IP (last 24h)

Host	Count	Actions
192.168.10.10	3	+
192.168.20.2	3	+

Activity (last 24h)



5.) 再回到 Kibana, 看一下 Suricata 的规则和对应抓取到的报文。

SN ALERT-EventsList

Time	EveBox	Scirius	alert.category	src_ip	src_port	proto	dest_ip	dest_port	alert.signature	alert.signature_id
December 25th 2017, 17:26:33.827	Correlate Flow	Complete Signature	Attempted Administrator Privilege Gain	4.3.2.10	1,024	TCP	192.168.10.1	80	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number	2,019,236

Field	Value
@timestamp	December 25th 2017, 17:26:33.827
@version	1
# EveBox	Correlate Flow
# Scirius	Complete Signature View
_id	AWM_Ls7YpToGxG0t7rc
_index	Togstash-alert-2017.12.25
_score	-
_type	SELKS
alert.action	allowed
alert.category	Attempted Administrator Privilege Gain
alert.gid	1
alert.rev	3
alert.severity	1
alert.signature	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number
alert.signature_id	2,019,236

http_method 是 GET, payload_printable 的内容触发了规则。

SN ALERT-EventsList

http_method	GET
http_response_body	VEWVVMGu2VjdXjpdHkgTGFicw=
http_response_body_printable	TELUS Security Labs
http_length	20
http_protocol	{ ts!}; echo 'TELUS Security Labs' > /tmp/TSL
http_status	200
http_url	/cgi-bin/ts1-test
in_iface	ens224
packet	A4wpgof7kOK6NDjVCABFAA0BwBAEAGYxEEAwIKwKgcgQAAFbHk<CLFVhdS1AQcABQCQAAAAAAAAA
packet_info.linktype	1
path	/var/log/suricata/eve.json
payload	R0VUIc9j22ktYmluL3RzbC10ZXN0ICgpIIsGdhNs0307IGVjaG8gJlRFTFVTFjFN1Y3VyaXR5IEExhYnMnID4qL3RtcC9U0wNCkhvc3Q6IDE5Mi44XnJmUuMTANCg0K
payload_printable	GET /cgi-bin/ts1-test { ts!}; echo 'TELUS Security Labs' > /tmp/TSL Host: 192.168.10.10
proto	TCP
src_ip	4.3.2.10
src_port	1,024
stream	1
tags	_geoip_lookup_failure
timestamp	December 25th 2017, 17:26:33.827
type	SELKS

可以看出 Suricata 很好的识别了 CVE 2014-6271 破壳漏洞攻击，告警信息正确，完备。