

流量监测

笔记本： 应急

创建时间： 2022/12/19 11:44

一、概述

在和别人交流时突然被问道，linux的流量监测工具有哪些，当时虽然也能简单说一些，但是还是觉得说的不够全面，所以正好趁着居家办公，简单对windows、linux下的一些常用工具简单总结下。

二、工具使用

windows:

最简单就是执行netstat -anto

wireshark: 这是最先推荐的工具，直接进行流量分析，缺点就是可视化差一点，并且真的就只是抓取了流量；

下载地址：

<https://www.wireshark.org/download.html>

科莱网络分析系统：页面更友好，会自动进行进程分析，还会对自动识别ip归属地，使用起来更方便，另外科莱还有很多小工具比较好用，比如ping工具或是mac地址扫描工具，都可以对网络存活主机进行判断。

下载地址：

<https://www.colasoft.com.cn/download.php>

火绒剑：个人认为还是比较好用的，可以查看启动项、网络、服务、文件、注册表等相关信息，并且还能查看进程的内存信息等数据。

下载地址

<https://www.huorong.cn/>

linux:

tcpdump

指定网络接口：tcpdump -i eth1

监视指定主机的数据包: tcpdump host x.x.x.x

监测A和B直接数据: tcpdump host A and B

指定协议和端口: tcpdump tcp port 22

保存流量: tcpdump -w xxx.pcap

捕获的流量同样可以利用wireshark打开或是科莱分析打开，同样也能利用python脚本分

析。

iftop:

这个工具之前也没用过，是查的时候找到的，linux下安装yum install iftop

Ubuntu安装: apt-get install iftop

源码安装下载地址:

<http://www.ex-parrot.com/pdw/iftop/download/>

下载之后编译安装即可

编译: ./configure

安装: make && make install

使用: 直接执行iftop, 可看到机器的所有连接, 还是比较直观的

file edit view search terminal help								
	19.1Mb	38.1Mb	57.2Mb	76.3Mb	95.4Mb			
localhost.localdomain	=>	223.99.251.38	18.8Kb	3.79Kb	2.09Kb			
	<=		4.22Mb	863Kb	231Kb			
localhost.localdomain	=>	223.99.251.35	1.38Kb	20.4Kb	6.61Kb			
	<=		42.3Kb	329Kb	110Kb			
localhost.localdomain	=>	180.101.212.231	69.3Kb	25.0Kb	6.24Kb			
	<=		7.02Kb	31.2Kb	7.81Kb			
localhost.localdomain	=>	223.109.81.134	18.1Kb	3.63Kb	929b			
	<=		177Kb	35.3Kb	8.83Kb			
localhost.localdomain	=>	182.61.200.166	20.3Kb	10.8Kb	2.71Kb			
	<=		2.27Kb	25.6Kb	6.39Kb			
localhost.localdomain	=>	182.61.200.6	160b	8.60Kb	11.2Kb			
	<=		184b	10.3Kb	87.3Kb			
localhost.localdomain	=>	110.242.68.204	0b	5.22Kb	1.31Kb			
	<=		0b	5.02Kb	1.25Kb			
localhost.localdomain	=>	gateway	1.27Kb	1.35Kb	1.75Kb			
	<=		2.66Kb	3.11Kb	4.18Kb			
localhost.localdomain	=>	182.61.200.178	0b	1.05Kb	1.31Kb			
	<=		0b	1.90Kb	6.20Kb			
TX:	cum:	305KB	peak:	133Kb	rates:	130Kb	83.5Kb	60.9Kb
RX:		4.74MB		4.44Mb		4.44Mb	1.28Mb	971Kb
TOTAL:		5.04MB		4.57Mb		4.57Mb	1.36Mb	1.01Mb

有很多的使用方法可以使用-h查看

```
MAC address is: 00:0c:29:0c:57:5a
[root@localhost ~]# iftop -h
iftop: display bandwidth usage on an interface by host

Synopsis: iftop -h | [-npblNBP] [-i interface] [-f filter code]
          [-F net/mask] [-G net6/mask6]

-h          display this message
-n          don't do hostname lookups
-N          don't convert port numbers to services
-p          run in promiscuous mode (show traffic between other
          hosts on the same network segment)
-b          don't display a bar graph of traffic
-B          display bandwidth in bytes
-a          display bandwidth in packets
-i interface listen on named interface
-f filter code use filter code to select packets to count
          (default: none, but only IP packets are counted)
-F net/mask show traffic flows in/out of IPv4 network
-G net6/mask6 show traffic flows in/out of IPv6 network
-l          display and count link-local IPv6 traffic (default: off)
```

指定监测端口 -i ens33

现实端口: -p

SHIFT+S 或 SHIFT+D会选择过滤源端口或是目的端口

对源地址进行过滤: `iftop -F 192.168.13.146/24 -n`

只显示192.168.13.0/24对外发起的连接

File	Edit	View	Search	Terminal	Help
		12.5Kb	25.0Kb	37.5Kb	50.0Kb
192.168.13.146			=>	49.7.36.173	
192.168.13.146			<=		
192.168.13.146			=>	183.60.95.183	
192.168.13.146			<=		
192.168.13.146			=>	123.126.45.35	
192.168.13.146			<=		

更多的用法可以参考<https://www.unixmen.com/iftop-a-network-bandwidth-monitoring-tool-for-linux/>

但是这个工具真的是只是监测网络连接，如果需要定位进程可能还需要在进一步做查询操作，如采用`netstat -antp | grep "56368"`进一步定位到系统进程

```
nterface: ens33
P address is: 192.168.13.146
AC address is: 00:0c:29:0c:57:5a
root@localhost ~]# netstat -antp | grep "56368"
cp      0      0 192.168.13.146:56368    49.7.36.173:443      ESTABLISHED 2954/firefox
root@localhost ~]# netstat -antpx | grep "56368"
```

从网上查了下linux下的工具没有windows这么丰富，没发现有一步到位的软件，类似火绒剑的还真没发现能装在linux系统上。

其实工具还是有很多的，并不一定每个工具都知道，只要能找到适合自己的工具，关键时候能用就行了。