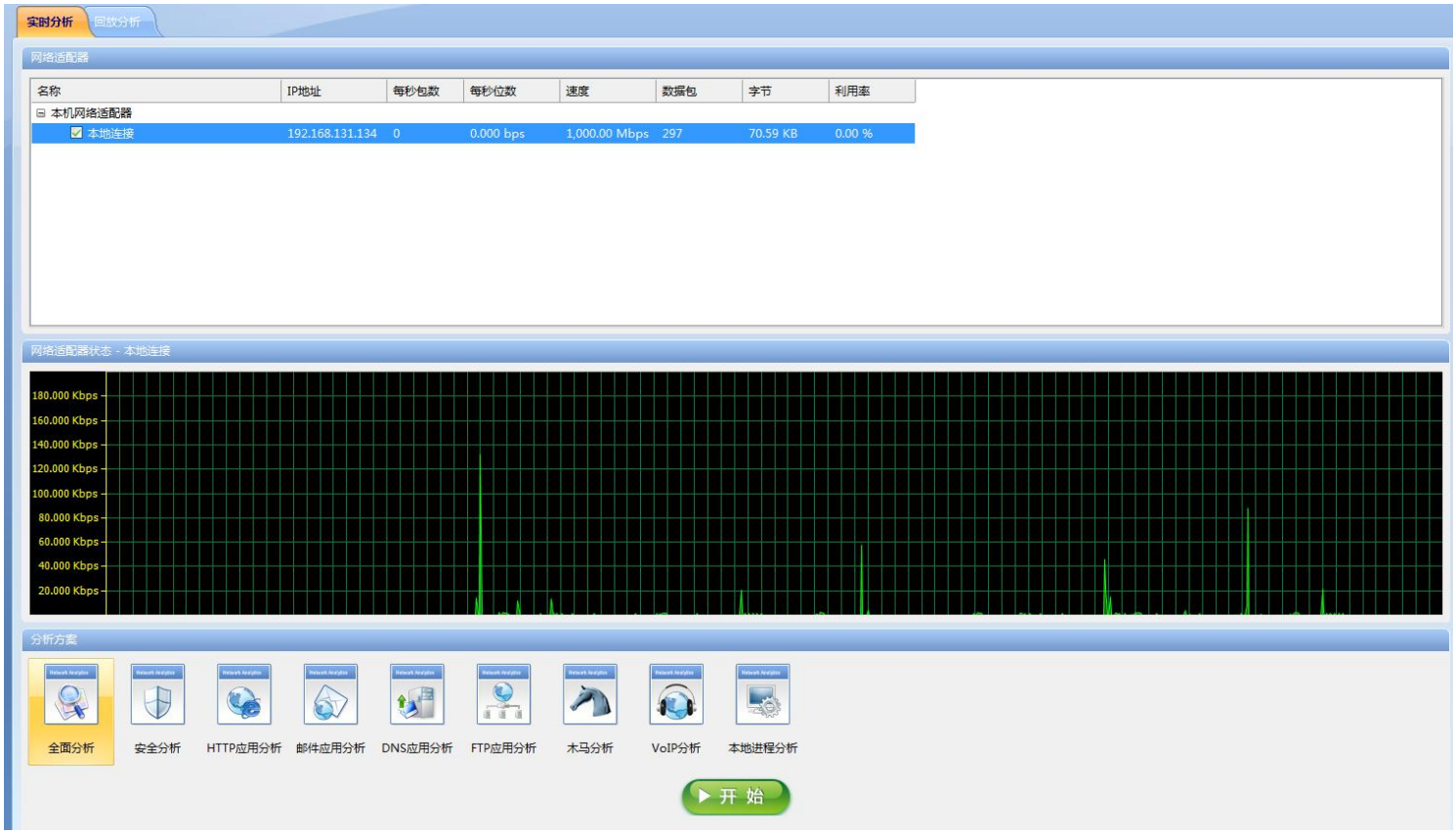
网络流量安全分析

——发现端口扫描 by.ATTOT.豆

我们知道，许多入侵行为是从扫描开始的，本期分享如何在网络流量分析中发现端口扫描行为

实验结构图

首先在 windows7 中开启科来网络分析系统，在网络适配器中选择你需要监测的网卡，开始全面分析



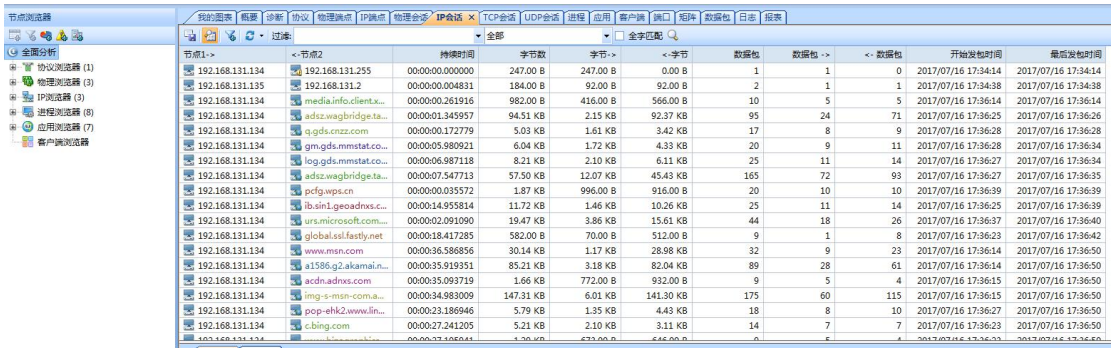
Kali 开启 nmap 对目标机器进行端口扫描

```
root@kali:~# nmap -PE -Pn 192.168.131.134

Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-16 05:34 EDT
Nmap scan report for 192.168.131.134
Host is up (0.00050s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 00:0C:29:F9:8F:0C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds
```

回到 win7 这边，可以看到有非常多的 IP 会话



首先要从中发现攻击者的 IP 会话，扫描有什么特征？数据包数量大，字节数非常小，通常情况下如果一个 IP 会话 数据包平均字节数<=72B 那么认为是有问题的

我们来对 IP 会话的数据包数量排个序

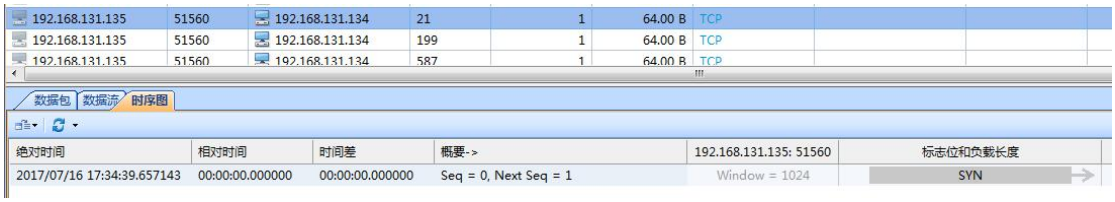
节点1->	<-节点2	持续时间	字节数	字节->	<-字节	数据包	数据包 ->	<- 数据包	开始发包时间	最后发包时间
192.168.131.134	192.168.131.135	00:03:27.680086	125.79 KB	680.00 B	125.13 KB	2,007	5	2,002	2017/07/16 17:34:38	2017/07/16 17:38:05
192.168.131.134	aeu.alicdn.com.da...	00:00:24.216939	609.29 KB	31.66 KB	577.63 KB	727	215	512	2017/07/16 17:36:26	2017/07/16 17:36:50
192.168.131.134	aeu.alicdn.com.da...	00:00:23.499604	417.21 KB	21.19 KB	396.02 KB	518	165	353	2017/07/16 17:36:27	2017/07/16 17:36:50
192.168.131.134	img-s-msn-com.a...	00:00:34.983009	147.31 KB	6.01 KB	141.30 KB	175	60	115	2017/07/16 17:36:15	2017/07/16 17:36:50
192.168.131.134	adsz.wagbridge.ta...	00:00:07.547713	57.50 KB	12.07 KB	45.43 KB	165	72	93	2017/07/16 17:36:27	2017/07/16 17:36:35
192.168.131.134	192.168.131.2	00:10:17.390083	19.97 KB	5.44 KB	14.53 KB	103	61	42	2017/07/16 17:34:38	2017/07/16 17:44:55
192.168.131.134	adsz.wagbridge.ta...	00:00:01.345957	94.51 KB	2.15 KB	92.37 KB	95	24	71	2017/07/16 17:36:25	2017/07/16 17:36:26
192.168.131.134	a1586.g2.akamai.n...	00:00:35.919351	85.21 KB	3.18 KB	82.04 KB	89	28	61	2017/07/16 17:36:14	2017/07/16 17:36:50
192.168.131.134	passport2.chaoxin...	00:00:15.285929	49.38 KB	8.91 KB	40.47 KB	88	33	55	2017/07/16 17:36:35	2017/07/16 17:36:50
192.168.131.134	aeu.alicdn.com.da...	00:00:22.212827	40.80 KB	2.59 KB	38.21 KB	59	21	38	2017/07/16 17:36:28	2017/07/16 17:36:50
192.168.131.134	all.cnzz.com.danu...	00:00:22.903270	24.56 KB	2.34 KB	22.22 KB	46	17	29	2017/07/16 17:36:27	2017/07/16 17:36:50
192.168.131.134	urs.microsoft.com....	00:00:02.091090	19.47 KB	3.86 KB	15.61 KB	44	18	26	2017/07/16 17:36:37	2017/07/16 17:36:40
192.168.131.134	data-collector-link...	00:00:26.537239	15.07 KB	2.63 KB	12.43 KB	42	18	24	2017/07/16 17:36:24	2017/07/16 17:36:50
192.168.131.134	gtms02.alicdn.com...	00:00:23.590150	14.68 KB	2.36 KB	12.32 KB	36	16	20	2017/07/16 17:36:27	2017/07/16 17:36:50
192.168.131.134	otf.msn.com	00:00:26.914830	15.88 KB	11.52 KB	4.36 KB	32	15	17	2017/07/16 17:36:23	2017/07/16 17:36:50
192.168.131.134	www.msn.com	00:00:36.586856	30.14 KB	1.17 KB	28.98 KB	32	9	23	2017/07/16 17:36:14	2017/07/16 17:36:50
192.168.131.1	239.255.255.250	00:10:03.027897	6.23 KB	6.23 KB	0.00 B	30	30	0	2017/07/16 17:34:55	2017/07/16 17:44:58
192.168.131.134	sh.wagbridge.alib...	00:00:20.132175	11.27 KB	2.42 KB	8.85 KB	26	11	15	2017/07/16 17:36:30	2017/07/16 17:36:50

发现本机（192.168.131.134）和 192.168.131.135 之间的会话非常可疑，数据包多，字节数小，收到的包远多于发出的包

从右键菜单定位到 192.168.131.135 这个可疑 IP 的节点浏览界面

节点1->	端口1->	<-节点2	<-端口2	数据包	字节数	协议
192.168.131.135	51559	192.168.131.134	80	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	993	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	443	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	1720	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	143	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	135	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	111	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	5900	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	110	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	1025	1	64.00 B	TCP
192.168.131.135	51560	192.168.131.134	1025	1	64.00 B	TCP
192.168.131.135	51560	192.168.131.134	110	1	64.00 B	TCP
192.168.131.135	51560	192.168.131.134	5900	1	64.00 B	TCP

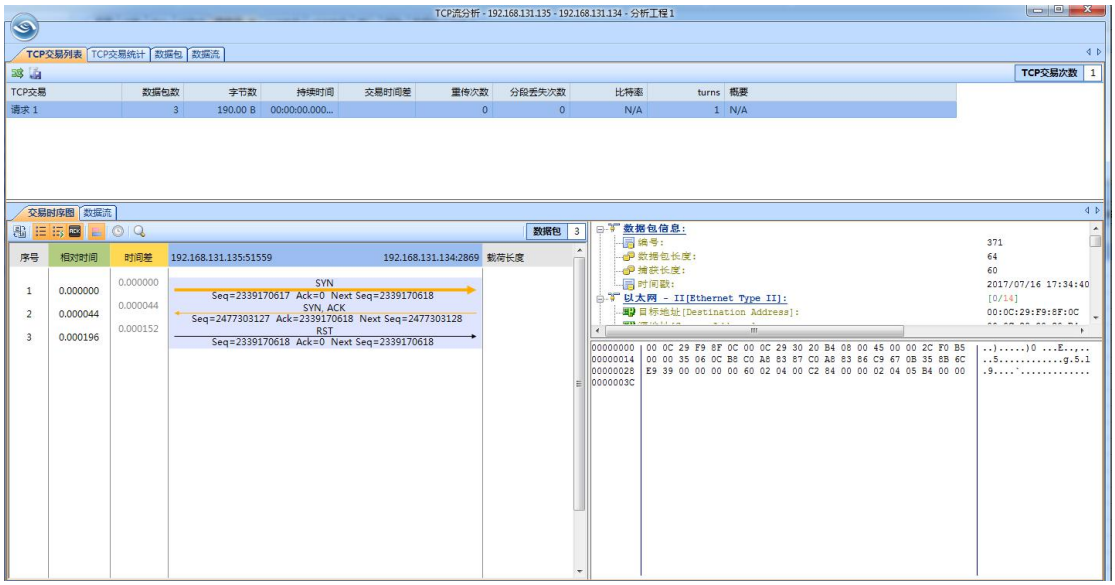
察看两个 IP 之间的 TCP 会话我们发现，135->134 访问了非常多的端口，正常的会话是不会出现这种情况的，点开任意 tcp 会话可以看到基本都是一个 SYN 包有来无回，典型的端口探测数据包



到这已经坐实了 192.168.131.135 的扫描行为，那要是我们想知道它扫描的结果呢？对 TCP 会话的数据包进行排序，可以看到 2869 和 445 端口是有不止一个包的

节点1->	端口1->	<-节点2	<-端口2	数据包	字节数	协议
192.168.131.135	51559	192.168.131.134	2869	3	190.00 B	TCP
192.168.131.135	51559	192.168.131.134	445	3	190.00 B	TCP
192.168.131.135	51570	192.168.131.134	445	3	190.00 B	TCP
192.168.131.135	51559	192.168.131.134	993	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	443	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	1720	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	143	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	135	1	64.00 B	TCP
192.168.131.135	51559	192.168.131.134	111	1	64.00 B	TCP

双击察看 TCP 会话详细情况能看到 192.168.131.134 回复了 SYN+ACK 包，这就说明它扫描到了 2869 端口是开放的



这样，我们就分析出 192.168.131.134 开放了 445 和 2869 两个端口

以上通过一个小实验介绍了在网络流量分析中发现扫描行为的简单方法，读者可以借此练习一下，也许你就发现有人在扫你的机子呢