一、整体把握

1、协议分级

```
99.7%TCP + 71.5%SSH
```

Wireshark · 协议分级统计 · ssh.pcap

协议	按分组百分比	分组	按字节百分比	字节	比特/秒	结束 分组	结束 字节	结束 位/秒
Frame	100.0	1300	100.0	16097863	9741 k	0	0	0
Ethernet	100.0	1300	0.1	18200	11 k	0	0	0
Internet Protocol Version 4	100.0	1300	0.2	26000	15 k	0	0	0
User Datagram Protocol	0.3	4	0.0	32	19	0	0	0
Domain Name System	0.3	4	0.0	230	139	4	230	139
Transmission Control Protocol	99.7	1296	99.7	16053377	9714 k	366	574952	347 k
SSH Protocol	71.5	930	96.0	15448665	9348 k	930	15448665	9348 k

2、端点统计

```
已被屏蔽的外网IP：192.168.174.158 居然跟自己有交互
```

Wireshark · Endpoints · ssh.pcap

Ethernet · 6 | IPv4 · 6 | IPv6 | TCP · 17 | UDP · 11

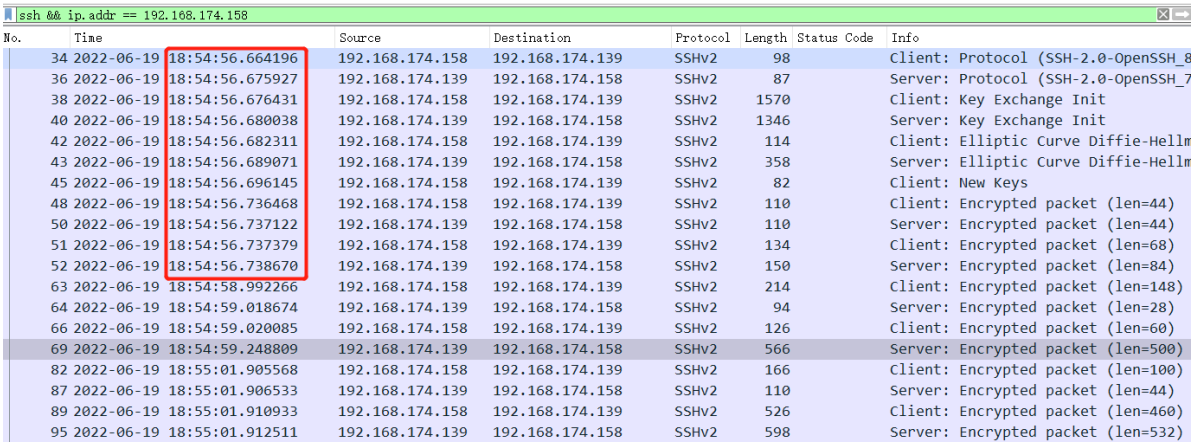
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
18.65.185.96	4	240	2	120	2	120	—	—	—	—
34.107.221.82	23	1702	0	0	23	1702	—	—	—	—
192.168.174.2	28	3812	14	2628	14	1184	—	—	—	—
192.168.174.139	1,982	30 M	1,171	16 M	811	14 M	—	—	—	—
192.168.174.158	1,300	16 M	430	35 k	870	16 M	—	—	—	—
192.168.174.159	643	14 M	373	14 M	270	19 k	—	—	—	—

二、流量分析

1、过滤协议

```
ssh && ip.addr == 192.168.174.158
```

```
数量角度：1秒之内产生了11个ssh数据包
IP角度：此IP已被屏蔽，还能产生交互
```

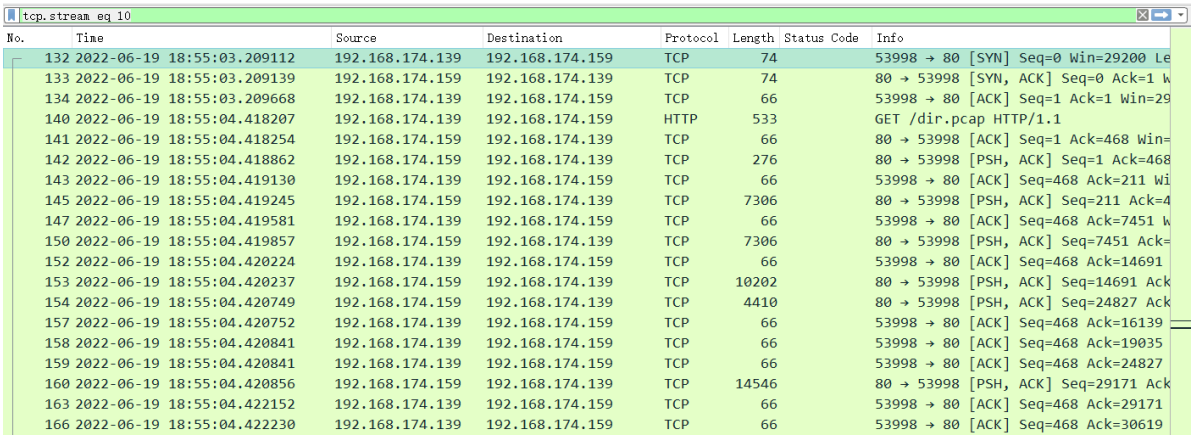


ssh && ip.addr == 192.168.174.158

No.	Time	Source	Destination	Protocol	Length	Status Code	Info
34	2022-06-19 18:54:56.664196	192.168.174.158	192.168.174.139	SSHv2	98		Client: Protocol (SSH-2.0-OpenSSH_8
36	2022-06-19 18:54:56.675927	192.168.174.139	192.168.174.158	SSHv2	87		Server: Protocol (SSH-2.0-OpenSSH_7
38	2022-06-19 18:54:56.676431	192.168.174.158	192.168.174.139	SSHv2	1570		Client: Key Exchange Init
40	2022-06-19 18:54:56.680038	192.168.174.139	192.168.174.158	SSHv2	1346		Server: Key Exchange Init
42	2022-06-19 18:54:56.682311	192.168.174.158	192.168.174.139	SSHv2	114		Client: Elliptic Curve Diffie-Hellm
43	2022-06-19 18:54:56.689071	192.168.174.139	192.168.174.158	SSHv2	358		Server: Elliptic Curve Diffie-Hellm
45	2022-06-19 18:54:56.696145	192.168.174.158	192.168.174.139	SSHv2	82		Client: New Keys
48	2022-06-19 18:54:56.736468	192.168.174.158	192.168.174.139	SSHv2	110		Client: Encrypted packet (len=44)
50	2022-06-19 18:54:56.737122	192.168.174.139	192.168.174.158	SSHv2	110		Server: Encrypted packet (len=44)
51	2022-06-19 18:54:56.737379	192.168.174.158	192.168.174.139	SSHv2	134		Client: Encrypted packet (len=68)
52	2022-06-19 18:54:56.738670	192.168.174.139	192.168.174.158	SSHv2	150		Server: Encrypted packet (len=84)
63	2022-06-19 18:54:58.992266	192.168.174.158	192.168.174.139	SSHv2	214		Client: Encrypted packet (len=148)
64	2022-06-19 18:54:59.018674	192.168.174.139	192.168.174.158	SSHv2	94		Server: Encrypted packet (len=28)
66	2022-06-19 18:54:59.020085	192.168.174.158	192.168.174.139	SSHv2	126		Client: Encrypted packet (len=60)
69	2022-06-19 18:54:59.248809	192.168.174.139	192.168.174.158	SSHv2	566		Server: Encrypted packet (len=500)
82	2022-06-19 18:55:01.905568	192.168.174.158	192.168.174.139	SSHv2	166		Client: Encrypted packet (len=100)
87	2022-06-19 18:55:01.906533	192.168.174.139	192.168.174.158	SSHv2	110		Server: Encrypted packet (len=44)
89	2022-06-19 18:55:01.910933	192.168.174.158	192.168.174.139	SSHv2	526		Client: Encrypted packet (len=460)
95	2022-06-19 18:55:01.912511	192.168.174.139	192.168.174.158	SSHv2	598		Server: Encrypted packet (len=532)

2、追踪流

```
tcp.stream eq 10
```



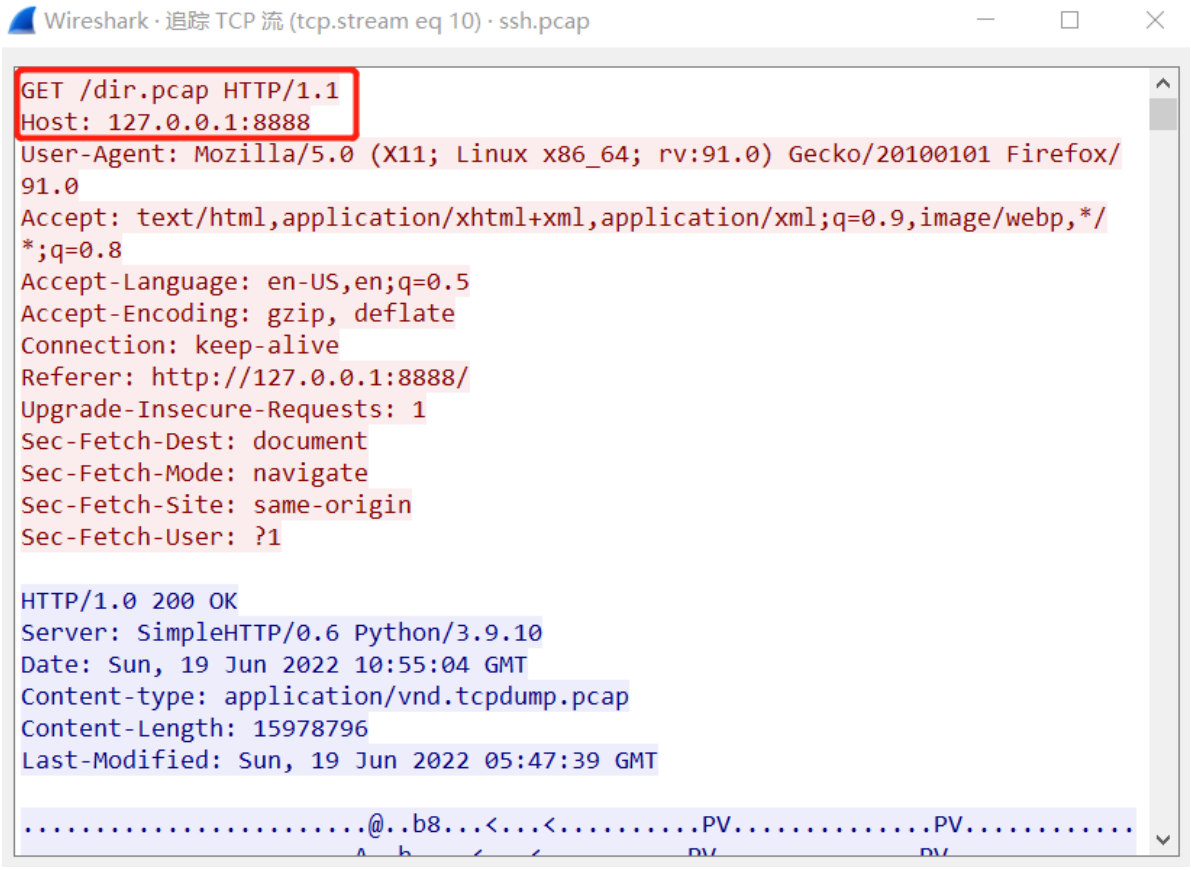
tcp.stream eq 10

No.	Time	Source	Destination	Protocol	Length	Status Code	Info
132	2022-06-19 18:55:03.209112	192.168.174.139	192.168.174.159	TCP	74		53998 → 80 [SYN] Seq=0 Win=29200 Le
133	2022-06-19 18:55:03.209139	192.168.174.159	192.168.174.139	TCP	74		80 → 53998 [SYN, ACK] Seq=0 Ack=1 W
134	2022-06-19 18:55:03.209668	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=1 Ack=1 Win=29
140	2022-06-19 18:55:04.418207	192.168.174.139	192.168.174.159	HTTP	533		GET /dir.pcap HTTP/1.1
141	2022-06-19 18:55:04.418254	192.168.174.159	192.168.174.139	TCP	66		80 → 53998 [ACK] Seq=1 Ack=468 Win=
142	2022-06-19 18:55:04.418862	192.168.174.159	192.168.174.139	TCP	276		80 → 53998 [PSH, ACK] Seq=1 Ack=468
143	2022-06-19 18:55:04.419130	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=211 Wi
145	2022-06-19 18:55:04.419245	192.168.174.159	192.168.174.139	TCP	7306		80 → 53998 [PSH, ACK] Seq=211 Ack=4
147	2022-06-19 18:55:04.419581	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=7451 W
150	2022-06-19 18:55:04.419857	192.168.174.159	192.168.174.139	TCP	7306		80 → 53998 [PSH, ACK] Seq=7451 Ack=
152	2022-06-19 18:55:04.420224	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=14691
153	2022-06-19 18:55:04.420237	192.168.174.159	192.168.174.139	TCP	10202		80 → 53998 [PSH, ACK] Seq=14691 Ack
154	2022-06-19 18:55:04.420749	192.168.174.159	192.168.174.139	TCP	4410		80 → 53998 [PSH, ACK] Seq=24827 Ack
157	2022-06-19 18:55:04.420752	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=16139
158	2022-06-19 18:55:04.420841	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=19035
159	2022-06-19 18:55:04.420841	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=24827
160	2022-06-19 18:55:04.420856	192.168.174.159	192.168.174.139	TCP	14546		80 → 53998 [PSH, ACK] Seq=29171 Ack
163	2022-06-19 18:55:04.422152	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=29171
166	2022-06-19 18:55:04.422230	192.168.174.139	192.168.174.159	TCP	66		53998 → 80 [ACK] Seq=468 Ack=30619

三、异常检测

1、端口被转发

查看具体数据包详情，对方通过访问了我本地的8888端口，查看了我80端口的文件


Wireshark · 追踪 TCP 流 (tcp.stream eq 10) · ssh.pcap
GET /dir.pcap HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://127.0.0.1:8888/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.10
Date: Sun, 19 Jun 2022 10:55:04 GMT
Content-type: application/vnd.tcpdump.pcap
Content-Length: 15978796
Last-Modified: Sun, 19 Jun 2022 05:47:39 GMT
.....@..b8...<...<.....PV.....PV.....