一、整体把握

1、协议分级

100%TCP + HTTP

Wireshark · 协议分级统计 · dir.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	91894	100.0	14508468	1991 k	0	0	0
Ethernet	100.0	91894	8.9	1286516	176 k	0	0	0
Internet Protocol Version 6	0.0	1	0.0	40	5	0	0	0
Internet Control Message Protocol v6	0.0	1	0.0	16	2	1	16	2
Internet Protocol Version 4	100.0	91875	12.7	1837500	252 k	0	0	0
User Datagram Protocol	0.0	4	0.0	32	4	0	0	0
Simple Service Discovery Protocol	0.0	4	0.0	696	95	4	696	95
Transmission Control Protocol	100.0	91871	78.5	11382858	1562 k	74475	4140178	568 k
Hypertext Transfer Protocol	18.9	17396	57.2	8303770	1140 k	8706	2606154	357 k
Line-based text data	9.5	8684	28.1	4072853	559 k	8684	5679273	779 k
Data	0.0	6	0.1	17137	2352	6	18343	2518
Address Resolution Protocol	0.0	18	0.0	810	111	18	810	111

2、端点统计

192.168.174.158（陌生主机）
192.168.174.159（自己主机）

Wireshark · Endpoints · dir.pcap

Ethernet · 6 | IPv4 · 4 | IPv6 · 2 | TCP · 8702 | UDP · 2

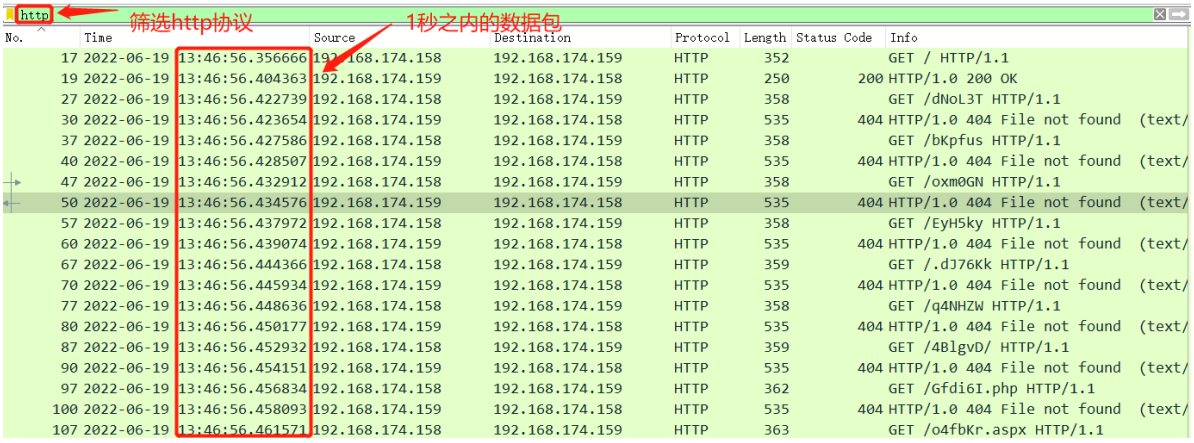
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.174.1	4	864	4	864	0	0	—	—	—	—
192.168.174.158	91,871	14 M	45,993	5709 k	45,878	8796 k	—	—	—	—
192.168.174.159	91,871	14 M	45,878	8796 k	45,993	5709 k	—	—	—	—
239.255.255.250	4	864	0	0	4	864	—	—	—	—

二、过滤筛选

1、过滤协议

http

发现一秒之内发送了几十个HTTP请求，并且都是不同目录，确定为IP：192.168.174.158发起的目录扫描

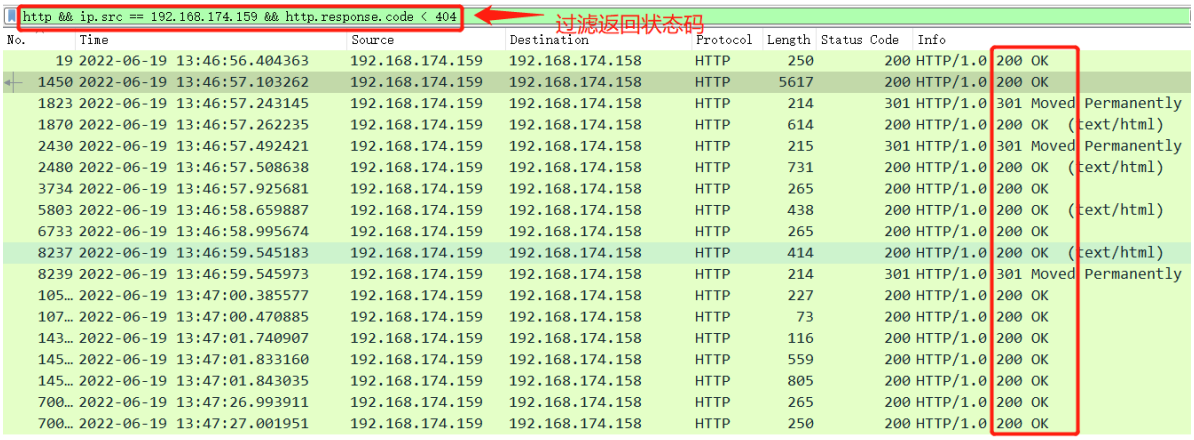


No.	Time	Source	Destination	Protocol	Length	Status Code	Info
17	2022-06-19 13:46:56.356666	192.168.174.158	192.168.174.159	HTTP	352		GET / HTTP/1.1
19	2022-06-19 13:46:56.404363	192.168.174.159	192.168.174.158	HTTP	250	200	HTTP/1.0 200 OK
27	2022-06-19 13:46:56.422739	192.168.174.158	192.168.174.159	HTTP	358		GET /dNoL3T HTTP/1.1
30	2022-06-19 13:46:56.423654	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
37	2022-06-19 13:46:56.427586	192.168.174.158	192.168.174.159	HTTP	358		GET /bKpfus HTTP/1.1
40	2022-06-19 13:46:56.428507	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
47	2022-06-19 13:46:56.432912	192.168.174.158	192.168.174.159	HTTP	358		GET /oxm0GN HTTP/1.1
50	2022-06-19 13:46:56.434576	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
57	2022-06-19 13:46:56.437972	192.168.174.158	192.168.174.159	HTTP	358		GET /EyH5ky HTTP/1.1
60	2022-06-19 13:46:56.439074	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
67	2022-06-19 13:46:56.444366	192.168.174.158	192.168.174.159	HTTP	359		GET /.dJ76Kk HTTP/1.1
70	2022-06-19 13:46:56.445934	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
77	2022-06-19 13:46:56.448636	192.168.174.158	192.168.174.159	HTTP	358		GET /q4NHZW HTTP/1.1
80	2022-06-19 13:46:56.450177	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
87	2022-06-19 13:46:56.452932	192.168.174.158	192.168.174.159	HTTP	359		GET /4BlgvD/ HTTP/1.1
90	2022-06-19 13:46:56.454151	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
97	2022-06-19 13:46:56.456834	192.168.174.158	192.168.174.159	HTTP	362		GET /Gfdi6I.php HTTP/1.1
100	2022-06-19 13:46:56.458093	192.168.174.159	192.168.174.158	HTTP	535	404	HTTP/1.0 404 File not found (text/
107	2022-06-19 13:46:56.461571	192.168.174.158	192.168.174.159	HTTP	363		GET /o4fbKr.aspx HTTP/1.1

2、过滤状态码

```
http && ip.src == 192.168.174.159 && http.response.code < 404
```

能够发现哪些目录被扫描成功



No.	Time	Source	Destination	Protocol	Length	Status Code	Info
19	2022-06-19 13:46:56.404363	192.168.174.159	192.168.174.158	HTTP	250	200	HTTP/1.0 200 OK
1450	2022-06-19 13:46:57.103262	192.168.174.159	192.168.174.158	HTTP	5617	200	HTTP/1.0 200 OK
1823	2022-06-19 13:46:57.243145	192.168.174.159	192.168.174.158	HTTP	214	301	HTTP/1.0 301 Moved Permanently
1870	2022-06-19 13:46:57.262235	192.168.174.159	192.168.174.158	HTTP	614	200	HTTP/1.0 200 OK (text/html)
2430	2022-06-19 13:46:57.492421	192.168.174.159	192.168.174.158	HTTP	215	301	HTTP/1.0 301 Moved Permanently
2480	2022-06-19 13:46:57.508638	192.168.174.159	192.168.174.158	HTTP	731	200	HTTP/1.0 200 OK (text/html)
3734	2022-06-19 13:46:57.925681	192.168.174.159	192.168.174.158	HTTP	265	200	HTTP/1.0 200 OK
5803	2022-06-19 13:46:58.659887	192.168.174.159	192.168.174.158	HTTP	438	200	HTTP/1.0 200 OK (text/html)
6733	2022-06-19 13:46:58.995674	192.168.174.159	192.168.174.158	HTTP	265	200	HTTP/1.0 200 OK
8237	2022-06-19 13:46:59.545183	192.168.174.159	192.168.174.158	HTTP	414	200	HTTP/1.0 200 OK (text/html)
8239	2022-06-19 13:46:59.545973	192.168.174.159	192.168.174.158	HTTP	214	301	HTTP/1.0 301 Moved Permanently
105…	2022-06-19 13:47:00.385577	192.168.174.159	192.168.174.158	HTTP	227	200	HTTP/1.0 200 OK
107…	2022-06-19 13:47:00.470885	192.168.174.159	192.168.174.158	HTTP	73	200	HTTP/1.0 200 OK
143…	2022-06-19 13:47:01.740907	192.168.174.159	192.168.174.158	HTTP	116	200	HTTP/1.0 200 OK
145…	2022-06-19 13:47:01.833160	192.168.174.159	192.168.174.158	HTTP	559	200	HTTP/1.0 200 OK
145…	2022-06-19 13:47:01.843035	192.168.174.159	192.168.174.158	HTTP	805	200	HTTP/1.0 200 OK
700…	2022-06-19 13:47:26.993911	192.168.174.159	192.168.174.158	HTTP	265	200	HTTP/1.0 200 OK
700…	2022-06-19 13:47:27.001951	192.168.174.159	192.168.174.158	HTTP	250	200	HTTP/1.0 200 OK

三、异常检测

1、暂无异常