一、整体把握

1、协议分级

%93TCP + HTTP

Wireshark · 协议分级统计 · http.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	1001	100.0	125877	9703	0	0	0
Ethernet	100.0	1001	11.1	14014	1080	0	0	0
Internet Protocol Version 6	0.2	2	0.1	80	6	0	0	0
Internet Control Message Protocol v6	0.2	2	0.0	24	1	2	24	1
Internet Protocol Version 4	95.1	952	15.1	19040	1467	0	0	0
User Datagram Protocol	1.6	16	0.1	128	9	0	0	0
Simple Service Discovery Protocol	0.4	4	0.6	696	53	4	696	53
Dynamic Host Configuration Protocol	0.4	4	0.9	1167	89	4	1167	89
Domain Name System	0.8	8	0.4	513	39	8	513	39
Transmission Control Protocol	93.5	936	70.0	88077	6789	609	38475	2965
Transport Layer Security	0.5	5	0.2	194	14	5	194	14
Hypertext Transfer Protocol	32.2	322	45.6	57407	4425	317	55339	4265
Line-based text data	0.3	3	0.3	416	32	3	865	66
Data	0.2	2	0.5	671	51	2	671	51
Address Resolution Protocol	4.7	47	1.7	2090	161	47	2090	161

2、端点统计

192.168.174.138 和 192.168.174.158的传输的流量偏多，且192.168.174.158为已经被屏蔽的IP

Wireshark · Endpoints · http.pcap

Ethernet · 9 | IPv4 · 11 | IPv6 · 3 | TCP · 37 | UDP · 10

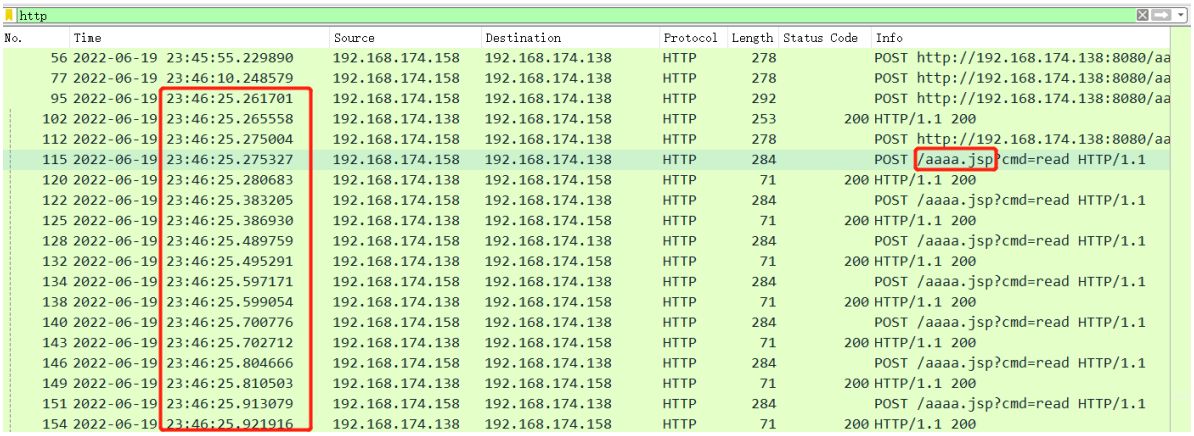
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
0.0.0.1	22	1628	0	0	22	1628	—	—	—	—
34.122.121.32	2	148	0	0	2	148	—	—	—	—
35.224.170.84	7	504	1	60	6	444	—	—	—	—
44.240.216.68	12	884	6	441	6	443	—	—	—	—
192.168.174.1	4	864	4	864	0	0	—	—	—	—
192.168.174.2	8	849	4	519	4	330	—	—	—	—
192.168.174.138	913	119 k	401	48 k	512	70 k	—	—	—	—
192.168.174.158	884	115 k	523	70 k	361	44 k	—	—	—	—
192.168.174.159	44	4710	11	1401	33	3309	—	—	—	—
192.168.174.254	4	1335	2	684	2	651	—	—	—	—
239.255.255.250	4	864	0	0	4	864	—	—	—	—

二、流量分析

1、过滤协议

http

可以看出来在短时间内，192.168.174.138频繁地请求192.168.174.158这个文件



No.	Time	Source	Destination	Protocol	Length	Status Code	Info
56	2022-06-19 23:45:55.229890	192.168.174.158	192.168.174.138	HTTP	278		POST http://192.168.174.138:8080/aa
77	2022-06-19 23:46:10.248579	192.168.174.158	192.168.174.138	HTTP	278		POST http://192.168.174.138:8080/aa
95	2022-06-19 23:46:25.261701	192.168.174.158	192.168.174.138	HTTP	292		POST http://192.168.174.138:8080/aa
102	2022-06-19 23:46:25.265558	192.168.174.138	192.168.174.158	HTTP	253	200	HTTP/1.1 200
112	2022-06-19 23:46:25.275004	192.168.174.158	192.168.174.138	HTTP	278		POST http://192.168.174.138:8080/aa
115	2022-06-19 23:46:25.275327	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
120	2022-06-19 23:46:25.280683	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
122	2022-06-19 23:46:25.383205	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
125	2022-06-19 23:46:25.386930	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
128	2022-06-19 23:46:25.489759	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
132	2022-06-19 23:46:25.495291	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
134	2022-06-19 23:46:25.597171	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
138	2022-06-19 23:46:25.599054	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
140	2022-06-19 23:46:25.700776	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
143	2022-06-19 23:46:25.702712	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
146	2022-06-19 23:46:25.804666	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
149	2022-06-19 23:46:25.810503	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
151	2022-06-19 23:46:25.913079	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
154	2022-06-19 23:46:25.921916	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200

2、查看指纹

```
?cmd=read
?cmd=forward
?cmd=disconnect
```

以上指纹均为HTTP隧道工具reGeorg的命令，说明该192.168.174.138被当作了跳板机，并且通过该跳板机成功访问了192.168.174.158的web服务

916	2022-06-19 23:46:49.630062	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
922	2022-06-19 23:46:49.632234	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
923	2022-06-19 23:46:49.632234	192.168.174.158	192.168.174.138	HTTP	667		POST /aaaa.jsp?cmd=forward HTTP/1.1
925	2022-06-19 23:46:49.632403	192.168.174.138	192.168.174.159	HTTP	401		GET /index.php HTTP/1.1
927	2022-06-19 23:46:49.632546	192.168.174.138	192.168.174.158	HTTP	178	200	HTTP/1.1 200
930	2022-06-19 23:46:49.633170	192.168.174.159	192.168.174.138	HTTP	265	200	HTTP/1.0 200 OK
935	2022-06-19 23:46:49.735855	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
939	2022-06-19 23:46:49.737675	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200 (text/html)
941	2022-06-19 23:46:49.738839	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
946	2022-06-19 23:46:49.740289	192.168.174.158	192.168.174.138	HTTP	272		POST /aaaa.jsp?cmd=disconnect HTTP/
949	2022-06-19 23:46:49.740762	192.168.174.138	192.168.174.158	HTTP	71	200	HTTP/1.1 200
954	2022-06-19 23:46:49.741706	192.168.174.138	192.168.174.158	HTTP	178	200	HTTP/1.1 200
962	2022-06-19 23:46:49.843699	192.168.174.158	192.168.174.138	HTTP	284		POST /aaaa.jsp?cmd=read HTTP/1.1
964	2022-06-19 23:46:49.844905	192.168.174.138	192.168.174.158	HTTP	255	200	HTTP/1.1 200
969	2022-06-19 23:46:49.846324	192.168.174.158	192.168.174.138	HTTP	272		POST /aaaa.jsp?cmd=disconnect HTTP/
971	2022-06-19 23:46:49.848275	192.168.174.138	192.168.174.158	HTTP	253	200	HTTP/1.1 200
982	2022-06-19 23:46:50.297062	192.168.174.158	192.168.174.138	HTTP	278		POST http://192.168.174.138:8080/aa