

赛题名称：MISC03

解题步骤（WriteUp）

第一步：下载附件查看提示，就是受到攻击了，然后找到攻击的 ip。讲实话这种题很简单。打开数据包

No.	Tin Source	Info	Destination	Protocol	Length
1	0. 39.144.218.183	35530 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
2	0. 10.22.0.2	80 → 35530 [SYN, ACK] Seq...	39.144.218.183	TCP	66
3	0. 39.144.218.183	35530 → 80 [ACK] Seq=1 Ac...	10.22.0.2	TCP	54
4	0. 39.144.218.183	GET /xkepxxhnskruchjdrdh...	10.22.0.2	HTTP	258
5	0. 10.22.0.2	80 → 35530 [ACK] Seq=1 Ac...	39.144.218.183	TCP	54
6	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	535
7	0. 39.144.218.183	35530 → 80 [FIN, ACK] Seq...	10.22.0.2	TCP	54
8	0. 39.144.218.183	35531 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
9	0. 10.22.0.2	80 → 35531 [SYN, ACK] Seq...	39.144.218.183	TCP	66
10	0. 10.22.0.2	80 → 35530 [FIN, ACK] Seq...	39.144.218.183	TCP	54
11	0. 39.144.218.183	35531 → 80 [ACK] Seq=1 Ac...	10.22.0.2	TCP	54
12	0. 39.144.218.183	35530 → 80 [ACK] Seq=206 ...	10.22.0.2	TCP	54
13	0. 39.144.218.183	GET / HTTP/1.1	10.22.0.2	HTTP	348
14	0. 10.22.0.2	80 → 35531 [ACK] Seq=1 Ac...	39.144.218.183	TCP	54
15	0. 10.22.0.2	HTTP/1.1 200 OK (text/ht...	39.144.218.183	HTTP	712
16	0. 39.144.218.183	35531 → 80 [FIN, ACK] Seq...	10.22.0.2	TCP	54
17	0. 10.22.0.2	80 → 35531 [FIN, ACK] Seq...	39.144.218.183	TCP	54
18	0. 39.144.218.183	35533 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
19	0. 10.22.0.2	80 → 35533 [SYN, ACK] Seq...	39.144.218.183	TCP	66
20	0. 39.144.218.183	35536 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
21	0. 10.22.0.2	80 → 35536 [SYN, ACK] Seq...	39.144.218.183	TCP	66
22	0. 39.144.218.183	35538 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
23	0. 10.22.0.2	80 → 35538 [SYN, ACK] Seq...	39.144.218.183	TCP	66
24	0. 39.144.218.183	35535 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
25	0. 10.22.0.2	80 → 35535 [SYN, ACK] Seq...	39.144.218.183	TCP	66
26	0. 39.144.218.183	35534 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
27	0. 10.22.0.2	80 → 35534 [SYN, ACK] Seq...	39.144.218.183	TCP	66
28	0. 39.144.218.183	35532 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
29	0. 10.22.0.2	80 → 35532 [SYN, ACK] Seq...	39.144.218.183	TCP	66
30	0. 39.144.218.183	35537 → 80 [SYN] Seq=0 Wi...	10.22.0.2	TCP	66
31	0. 10.22.0.2	80 → 35537 [SYN, ACK] Seq...	39.144.218.183	TCP	66

> Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: 02:42:0a:16:00:02 (02:42:0a:16:00:02), Dst: 02:42:42:00:20:00
> Internet Protocol Version 4, Src: 10.22.0.2, Dst: 39.144.218.183

0000 02 42 42 14 1d e1 02 42 0a 16 00 02 08 00 45 00 -BB---B-----E-
0010 00 28 0d 88 40 00 40 06 20 e9 0a 16 00 02 27 90 -(---@-----P-
0020 da b7 00 50 8a cb ac 67 02 56 35 8e 8d c7 50 10 ---P---g-V5---P-

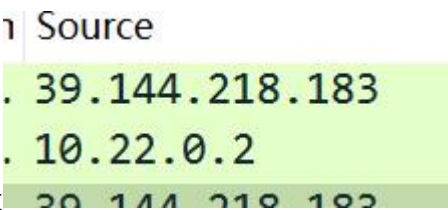
第二步：说实话一眼 http 协议，没什么说的，直接过滤 http

No.	Tin Source	Info	Destination	Protocol	Length
4	0. 39.144.218.183	GET /xkepxxhnskruchjdrdh...	10.22.0.2	HTTP	258
6	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	535
13	0. 39.144.218.183	GET / HTTP/1.1	10.22.0.2	HTTP	348
15	0. 10.22.0.2	HTTP/1.1 200 OK (text/ht...	39.144.218.183	HTTP	712
89	0. 39.144.218.183	GET /a.zip HTTP/1.1	10.22.0.2	HTTP	353
91	0. 39.144.218.183	GET /.svn/entries HTTP/1...	10.22.0.2	HTTP	360
93	0. 39.144.218.183	GET /2015.rar HTTP/1.1	10.22.0.2	HTTP	356
95	0. 39.144.218.183	GET /data.rar HTTP/1.1	10.22.0.2	HTTP	356
97	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	498
101	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	501
102	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	501
103	0. 39.144.218.183	GET /2014.rar HTTP/1.1	10.22.0.2	HTTP	356
104	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	505
107	0. 39.144.218.183	GET /2015.zip HTTP/1.1	10.22.0.2	HTTP	356
109	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	501
110	0. 39.144.218.183	GET /1.gz HTTP/1.1	10.22.0.2	HTTP	352
113	0. 39.144.218.183	GET /oa.rar HTTP/1.1	10.22.0.2	HTTP	354
115	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	501
116	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	497
117	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	499
118	0. 39.144.218.183	GET /web.zip HTTP/1.1	10.22.0.2	HTTP	355
121	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	500
123	0. 39.144.218.183	GET /.hg HTTP/1.1	10.22.0.2	HTTP	351
126	0. 39.144.218.183	GET /backup.rar HTTP/1.1	10.22.0.2	HTTP	358
128	0. 39.144.218.183	GET /www.rar HTTP/1.1	10.22.0.2	HTTP	355
130	0. 10.22.0.2	HTTP/1.1 404 Not Found (...	39.144.218.183	HTTP	496
132	0. 39.144.218.183	GET /2016.rar HTTP/1.1	10.22.0.2	HTTP	356
134	0. 39.144.218.183	GET /admin.rar HTTP/1.1	10.22.0.2	HTTP	357
136	0. 39.144.218.183	GET /WEB-INF/web.xml HTTP...	10.22.0.2	HTTP	363
139	0. 39.144.218.183	GET /2017.zip HTTP/1.1	10.22.0.2	HTTP	356
142	0. 39.144.218.183	GET /123.rar HTTP/1.1	10.22.0.2	HTTP	355

> Frame 13: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
> Ethernet II, Src: 02:42:42:14:1d:e1 (02:42:42:14:1d:e1), Dst: 02:42:0a:16:00:02
> Internet Protocol Version 4, Src: 39.144.218.183, Dst: 10.22.0.2
> Transmission Control Protocol, Src Port: 35531, Dst Port: 80, Seq: 1,
> Hypertext Transfer Protocol

0000 02 42 0a 16 00 02 02 42 42 14 1d e1 08 00 45 48 -B-----B B-----EH
0010 01 4e 9c ef 40 00 6e 06 62 13 27 90 da b7 0a 16 -N-@-n- b'-----
0020 00 02 8a cb 00 50 35 8e 8c a1 ac 67 02 56 50 18 -----P5---g-VP-
0030 01 04 10 f9 00 00 47 45 54 20 2f 20 48 54 54 50 -----GE T / HTTP
0040 2f 31 2e 31 6d 0a 6f 73 74 3a 20 31 32 34 2e /1.1:Ho st: 124.
0050 37 30 2e 39 31 2e 32 30 33 3a 34 34 38 39 39 6d 70,91,20 3:44899-

正常情况下，我们肯定是找请求头看看符不符合恶意的请求特征然后去操作，但是我翻了



很久，数据太多了，所以采用排除法，首先先测试

发现都不是直接过滤

No.	Tin	Source	Info	Destination	Protocol	Length
825	0..	39.144.218.183	GET / HTTP/1.1	10.22.0.2	HTTP	514
36554	1..	39.144.218.183	GET /romaoecpxegtjwofslvq...	10.22.0.2	HTTP	282
36563	1..	39.144.218.183	GET / HTTP/1.1	10.22.0.2	HTTP	297
36642	1..	39.144.218.183	GET /web.zip HTTP/1.1	10.22.0.2	HTTP	304
36646	1..	39.144.218.183	GET /a.zip HTTP/1.1	10.22.0.2	HTTP	302
36648	1..	39.144.218.183	GET /.svn/entries HTTP/1...	10.22.0.2	HTTP	309
36650	1..	39.144.218.183	GET /bak.rar HTTP/1.1	10.22.0.2	HTTP	304
36653	1..	39.144.218.183	GET /2.zip HTTP/1.1	10.22.0.2	HTTP	302
36655	1..	39.144.218.183	GET /.hg HTTP/1.1	10.22.0.2	HTTP	300
36661	1..	39.144.218.183	GET /oa.rar HTTP/1.1	10.22.0.2	HTTP	303
36666	1..	39.144.218.183	GET /.git/config HTTP/1.1	10.22.0.2	HTTP	308
36672	1..	39.144.218.183	GET /WEB-INF/web.xml HTTP...	10.22.0.2	HTTP	312
36680	1..	39.144.218.183	GET /2014.rar HTTP/1.1	10.22.0.2	HTTP	305
36682	1..	39.144.218.183	GET /bbs.rar HTTP/1.1	10.22.0.2	HTTP	304
36684	1..	39.144.218.183	GET /data.rar HTTP/1.1	10.22.0.2	HTTP	305
36688	1..	39.144.218.183	GET /2015.rar HTTP/1.1	10.22.0.2	HTTP	305
36690	1..	39.144.218.183	GET /2015.zip HTTP/1.1	10.22.0.2	HTTP	305
36692	1..	39.144.218.183	GET /1.gz HTTP/1.1	10.22.0.2	HTTP	301
36695	1..	39.144.218.183	GET /123.rar HTTP/1.1	10.22.0.2	HTTP	304
36699	1..	39.144.218.183	GET /back.rar HTTP/1.1	10.22.0.2	HTTP	305
36701	1..	39.144.218.183	GET /bbs.zip HTTP/1.1	10.22.0.2	HTTP	304
36702	1..	39.144.218.183	GET /a.rar HTTP/1.1	10.22.0.2	HTTP	302
36705	1..	39.144.218.183	GET /2017.zip HTTP/1.1	10.22.0.2	HTTP	305
36707	1..	39.144.218.183	GET /2014.zip HTTP/1.1	10.22.0.2	HTTP	305
36710	1..	39.144.218.183	GET /2016.rar HTTP/1.1	10.22.0.2	HTTP	305
36712	1..	39.144.218.183	GET /1.tar.gz HTTP/1.1	10.22.0.2	HTTP	305
36715	1..	39.144.218.183	GET /admin.rar HTTP/1.1	10.22.0.2	HTTP	306
36717	1..	39.144.218.183	GET /123.zip HTTP/1.1	10.22.0.2	HTTP	304
36719	1..	39.144.218.183	GET /2016.zip HTTP/1.1	10.22.0.2	HTTP	305
36721	1..	39.144.218.183	GET /backup.rar HTTP/1.1	10.22.0.2	HTTP	307
36723	1..	39.144.218.183	GET /2.rar HTTP/1.1	10.22.0.2	HTTP	302

也不是

No.	Tin	Source	Info	Destination	Protocol	Length
69380	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69384	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69387	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69390	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69393	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69396	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69399	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69402	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69404	2..	39.168.5.60	GET /static/bootstrap.css...	10.22.0.2	HTTP	44
69412	2..	39.168.5.60	GET /static/cover.css HTT...	10.22.0.2	HTTP	41
69418	2..	39.168.5.60	GET /static/jquery.js HTT...	10.22.0.2	HTTP	41
69427	2..	39.168.5.60	GET /static/bootstrap.js ...	10.22.0.2	HTTP	41
69428	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69465	2..	39.168.5.60	GET /static/bootstrap.css...	10.22.0.2	HTTP	44
69471	2..	39.168.5.60	GET /static/cover.css HTT...	10.22.0.2	HTTP	41
69472	2..	39.168.5.60	GET /static/bootstrap.js ...	10.22.0.2	HTTP	41
69475	2..	39.168.5.60	GET /static/jquery.js HTT...	10.22.0.2	HTTP	41
69512	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69530	2..	39.168.5.60	GET /static/bootstrap.css...	10.22.0.2	HTTP	44
69539	2..	39.168.5.60	GET /static/bootstrap.js ...	10.22.0.2	HTTP	41
69540	2..	39.168.5.60	GET /static/jquery.js HTT...	10.22.0.2	HTTP	41
69545	2..	39.168.5.60	GET /static/cover.css HTT...	10.22.0.2	HTTP	41
69576	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69592	2..	39.168.5.60	GET /static/bootstrap.css...	10.22.0.2	HTTP	44
69601	2..	39.168.5.60	GET /static/cover.css HTT...	10.22.0.2	HTTP	41
69603	2..	39.168.5.60	GET /static/jquery.js HTT...	10.22.0.2	HTTP	41
69604	2..	39.168.5.60	GET /static/bootstrap.js ...	10.22.0.2	HTTP	41
69644	2..	39.168.5.60	GET / HTTP/1.1	10.22.0.2	HTTP	51
69656	2..	39.168.5.60	GET /static/bootstrap.css...	10.22.0.2	HTTP	44
69664	2..	39.168.5.60	GET /static/cover.css HTT...	10.22.0.2	HTTP	41
69666	2..	39.168.5.60	GET /static/bootstrap.js ...	10.22.0.2	HTTP	41

> Frame 69380: 514 bytes on wire (4112 bits), 514 bytes captured (4112 b...
 > Ethernet II, Src: 02:42:42:14:1d:e1 (02:42:42:14:1d:e1), Dst: 02:42:0e...
 > Internet Protocol Version 4, Src: 39.168.5.60, Dst: 10.22.0.2
 > Transmission Control Protocol, Src Port: 34388, Dst Port: 80, Seq: 1...
 0000 02 42 0a 16 00 02 02 42 42 14 1d e1 08 00 45 40 B.....B B.....EH
 0010 01 f4 3a a2 40 00 6d 06 c3 e5 27 80 05 3c 0a 16 ...: @ m<..
 0020 00 02 85 3d 00 50 94 10 0e 32 84 1d a5 ad 50 18P...2...P..
 0030 02 03 e0 a4 00 00 47 45 54 20 2f 20 48 54 50GE T / HTTP

第三步:

测试到 39.168.5.60 成功