WIRESHARK ANALYSIS

Calvin Winata
Elang Wisanggeni
Darren
Nicole Theresiana
Yochana

NMAP ATTACKER

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted].127.128	[redacted]127.55	TCP	74	58806 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3720518658 TSecr=0 WS=128
2	0.000113	[redacted].127.128	[redacted]127.56	TCP	74	57148 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3574497966 TSecr=0 WS=128
3	0.000169	[redacted].127.128	[redacted]127.57	TCP	74	59570 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1980214267 TSecr=0 WS=128
4	0.000222	[redacted].127.128	[redacted]127.58	TCP	74	48322 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3110115304 TSecr=0 WS=128
5	0.000278	[redacted].127.128	[redacted]127.59	TCP	74	43840 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1210534177 TSecr=0 WS=128
6	0.000319	[redacted].127.128	[redacted]127.60	TCP	74	34194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2365606389 TSecr=0 WS=128
7	0.000371	[redacted].127.128	[redacted]127.61	TCP	74	33480 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1872126804 TSecr=0 WS=128
8	0.000425	[redacted].127.128	[redacted]127.62	TCP	74	60496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=646200492 TSecr=0 WS=128
9	0.000481	[redacted].127.128	[redacted]127.63	TCP	74	46412 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=997906366 TSecr=0 WS=128
10	0.000559	[redacted].127.128	[redacted]127.64	TCP	74	42994 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1048417369 TSecr=0 WS=128
11	0.462452	[redacted]c0:00:08	[redacted]st	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
12	1.002101	[redacted].127.128	[redacted]127.41	TCP	74	50828 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2571620632 TSecr=0 WS=128
13	1.002207	[redacted].127.128	[redacted]127.42	TCP	74	50210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2659289698 TSecr=0 WS=128
14	1.002278	[redacted].127.128	[redacted]127.43	TCP	74	49556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=556167172 TSecr=0 WS=128
15	1.002359	[redacted].127.128	[redacted]127.44	TCP	74	48074 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3122118354 TSecr=0 WS=128
16	1.002424	[redacted].127.128	[redacted]127.45	TCP	74	48618 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3849525472 TSecr=0 WS=128
17	1.002480	[redacted].127.128	[redacted]127.46	TCP	74	33210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1053317916 TSecr=0 WS=128
18	1.002544	[redacted].127.128	[redacted]127.47	TCP	74	44650 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2788113261 TSecr=0 WS=128
19	1.002609	[redacted].127.128	[redacted]127.48	TCP	74	35664 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2930977157 TSecr=0 WS=128
20	1.002668	[redacted].127.128	[redacted]127.49	TCP	74	57670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4009253454 TSecr=0 WS=128
21	1.002729	[redacted].127.128	[redacted]127.50	TCP	74	57444 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1166637827 TSecr=0 WS=128

Request time

Disini ada berberapa redflags yang bisa kita lihat, pertama pada request yang memiliki jangka waktu yang sangat kecil. Sepersekian milisecond ada request ke ip yang baru dari 1 individu yang sama.

NMAP ATTACKER

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted]127.128	[redacted]127.55	TCP	74	58806 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3720518658 TSecr=0 WS=128
2	0.000113	[redacted]127.128	[redacted]127.56	TCP	74	57148 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3574497966 TSecr=0 WS=128
3	0.000169	[redacted]127.128	[redacted]127.57	TCP	74	59570 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1980214267 TSecr=0 WS=128
4	0.000222	[redacted]127.128	[redacted]127.58	TCP	74	48322 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3110115304 TSecr=0 WS=128
5	0.000278	[redacted]127.128	[redacted]127.59	TCP	74	43840 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1210534177 TSecr=0 WS=128
6	0.000319	[redacted]127.128	[redacted]127.60	TCP	74	34194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2365606389 TSecr=0 WS=128
7	0.000371	[redacted]127.128	[redacted]127.61	TCP	74	33480 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1872126804 TSecr=0 WS=128
8	0.000425	[redacted]127.128	[redacted]127.62	TCP	74	60496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=646200492 TSecr=0 WS=128
9	0.000481	[redacted]127.128	[redacted]127.63	TCP	74	46412 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=997906366 TSecr=0 WS=128
10	0.000559	[redacted]127.128	[redacted]127.64	TCP	74	42994 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1048417369 TSecr=0 WS=128
11	0.462452	[redacted]:0:00:08	[redacted]st	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
12	1.002101	[redacted]127.128	[redacted]127.41	TCP	74	50828 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2571620632 TSecr=0 WS=128
13	1.002207	[redacted]127.128	[redacted]127.42	TCP	74	50210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2659289698 TSecr=0 WS=128
14	1.002278	[redacted]127.128	[redacted]127.43	TCP	74	49556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=556167172 TSecr=0 WS=128
15	1.002359	[redacted]127.128	[redacted]127.44	TCP	74	48074 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3122118354 TSecr=0 WS=128
16	1.002424	[redacted]127.128	[redacted]127.45	TCP	74	48618 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3849525472 TSecr=0 WS=128
17	1.002480	[redacted]127.128	[redacted]127.46	TCP	74	33210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1053317916 TSecr=0 WS=128
18	1.002544	[redacted]127.128	[redacted]127.47	TCP	74	44650 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2788113261 TSecr=0 WS=128
19	1.002609	[redacted]127.128	[redacted]127.48	TCP	74	35664 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2930977157 TSecr=0 WS=128
20	1.002668	[redacted]127.128	[redacted]127.49	TCP	74	57670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4009253454 TSecr=0 WS=128
21	1.002729	[redacted]127.128	[redacted]127.50	TCP	74	57444 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1166637827 TSecr=0 WS=128

Destination IP

IP tujuan yang di request dari source diatas juga bisa kita lihat terlihat sedang melakukan recon, kita lihat dia mencoba untuk melihat dari ip tersebut apakah ada open port 80 atau biasanya protocol HTML.

NMAP ATTACKER

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	[redacted] 127.128	[redacted] 127.55	TCP	74	58806 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3720518658 TSecr=0 WS=128
2	0.000113	127.128	127.56	TCP	74	57148 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3574497966 TSecr=0 WS=128
3	0.000169	127.128	127.57	TCP	74	59570 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1980214267 TSecr=0 WS=128
4	0.000222	127.128	127.58	TCP	74	48322 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3110115304 TSecr=0 WS=128
5	0.000278	127.128	127.59	TCP	74	43840 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1210534177 TSecr=0 WS=128
6	0.000319	127.128	127.60	TCP	74	34194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2365606389 TSecr=0 WS=128
7	0.000371	127.128	127.61	TCP	74	33480 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1872126804 TSecr=0 WS=128
8	0.000425	127.128	127.62	TCP	74	60496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=646200492 TSecr=0 WS=128
9	0.000481	127.128	127.63	TCP	74	46412 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=997906366 TSecr=0 WS=128
10	0.000559	127.128	127.64	TCP	74	42994 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1048417369 TSecr=0 WS=128
11	0.462452	:0:00:08	st	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
12	1.002101	127.128	127.41	TCP	74	50828 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2571620632 TSecr=0 WS=128
13	1.002207	127.128	127.42	TCP	74	50210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2659289698 TSecr=0 WS=128
14	1.002278	127.128	127.43	TCP	74	49556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=556167172 TSecr=0 WS=128
15	1.002359	127.128	127.44	TCP	74	48074 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3122118354 TSecr=0 WS=128
16	1.002424	127.128	127.45	TCP	74	48618 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3849525472 TSecr=0 WS=128
17	1.002480	127.128	127.46	TCP	74	33210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1053317916 TSecr=0 WS=128
18	1.002544	127.128	127.47	TCP	74	44650 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2788113261 TSecr=0 WS=128
19	1.002609	127.128	127.48	TCP	74	35664 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2930977157 TSecr=0 WS=128
20	1.002668	127.128	127.49	TCP	74	57670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4009253454 TSecr=0 WS=128
21	1.002729	127.128	127.50	TCP	74	57444 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1166637827 TSecr=0 WS=128

Port Tujuan

Seperti yang sudah kami mention diatas, kita bisa lihat kalo penyerang sedang melakukan enumeration untuk mencari open html protocol yang ada di target. TIdak hanya http, tetapi attacker juga melihat port 443 yang biasanya merupakan https protocol

NMAP ATTACKER

No.	Time	Source	Destination	Protocol	Length	Info
548	32.069812	.127.128	127.12	TCP	74	39100 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3003342202 TSecr=0 WS=128
549	32.069887	.127.128	127.16	TCP	74	58430 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1453425703 TSecr=0 WS=128
550	32.069947	.127.128	127.17	TCP	74	38470 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3450559677 TSecr=0 WS=128
551	32.070016	.127.128	127.18	TCP	74	57490 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2643510878 TSecr=0 WS=128
552	32.070115	.127.128	127.19	TCP	74	35298 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=61369184 TSecr=0 WS=128
553	32.070180	.127.128	127.20	TCP	74	41818 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2606348614 TSecr=0 WS=128
554	32.070249	.127.128	127.21	TCP	74	47932 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1824955898 TSecr=0 WS=128
555	32.070460	.127.128	127.24	TCP	74	43600 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=417055054 TSecr=0 WS=128
556	32.070565	.127.128	127.25	TCP	74	42974 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=584606977 TSecr=0 WS=128
557	33.072084	.127.128	127.28	TCP	74	53640 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3806676910 TSecr=0 WS=128
558	33.072223	.127.128	127.29	TCP	74	58578 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2020281225 TSecr=0 WS=128
559	33.072289	.127.128	127.30	TCP	74	57668 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1293835123 TSecr=0 WS=128
560	33.072422	.127.128	127.31	TCP	74	59124 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1186428831 TSecr=0 WS=128
561	33.072607	.127.128	127.32	TCP	74	34862 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1896926972 TSecr=0 WS=128
562	33.072673	127.146	.127.128	TCP	60	80 → 55202 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
563	33.072676	.127.128	127.33	TCP	74	36340 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2673737268 TSecr=0 WS=128
564	33.072674	127.141	.127.128	TCP	60	80 → 35476 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
565	33.072674	127.147	.127.128	TCP	60	80 → 37170 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
566	33.072674	127.148	.127.128	TCP	60	80 → 43560 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
567	33.072674	127.145	.127.128	TCP	60	80 → 39436 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
568	33.072674	127.143	.127.128	TCP	60	80 → 36960 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

Port Tujuan

Berikut adalah pembuktian statement yang kita buat diatas.

Mungkin its worth to mention juga, dibagian highlight merah pada hasil pcap diatas menunjukan bahwa portnya close. Diketahui dari response RST, ACK dari server.

DDOS

overview

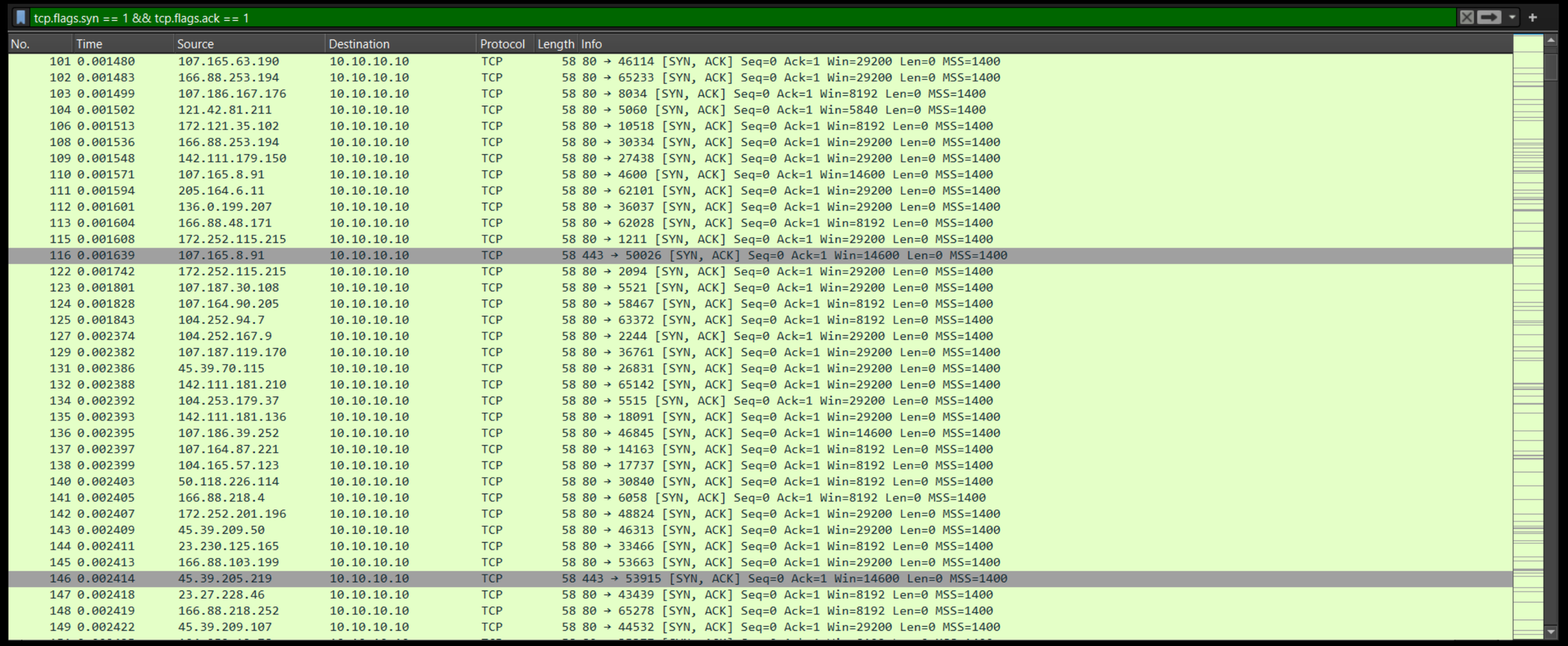
Kalo kita lihat semua request yang ada di pcap ini kita mulai bisa melihat kejanggalan, dimana ada massive flood dari syn ack request.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	136.0.86.165	10.10.10.10	TCP	58	80 → 52085 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
2	0.000003	172.120.24.143	10.10.10.10	TCP	58	80 → 17530 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
3	0.000006	166.88.89.117	10.10.10.10	TCP	58	80 → 29172 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
4	0.000044	136.0.86.229	10.10.10.10	TCP	58	80 → 57064 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
5	0.000047	136.0.86.135	10.10.10.10	TCP	58	80 → 8314 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
6	0.000049	23.230.239.35	10.10.10.10	TCP	58	80 → 41411 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
7	0.000112	136.0.86.144	10.10.10.10	TCP	58	80 → 31853 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
8	0.000115	136.0.199.199	10.10.10.10	TCP	58	80 → 25204 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
9	0.000142	104.253.194.126	10.10.10.10	TCP	58	80 → 53874 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
10	0.000155	50.118.154.113	10.10.10.10	TCP	58	80 → 34133 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
11	0.000181	142.252.218.157	10.10.10.10	TCP	58	80 → 58114 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
12	0.000185	107.186.8.171	10.10.10.10	TCP	58	80 → 59214 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
13	0.000238	166.88.253.65	10.10.10.10	TCP	58	80 → 25493 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
14	0.000261	142.111.211.144	10.10.10.10	TCP	58	80 → 22177 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
15	0.000264	142.252.99.198	10.10.10.10	TCP	58	80 → 36379 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
16	0.000266	50.118.149.36	10.10.10.10	TCP	58	80 → 20679 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
17	0.000273	50.118.149.36	10.10.10.10	TCP	58	80 → 32060 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
18	0.000276	107.164.205.51	10.10.10.10	TCP	58	80 → 1819 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
19	0.000277	142.111.211.144	10.10.10.10	TCP	58	80 → 38508 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
20	0.000280	107.187.84.84	10.10.10.10	TCP	58	443 → 46065 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
21	0.000283	107.173.155.30	10.10.10.10	TCP	58	443 → 11232 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400
22	0.000285	107.187.84.84	10.10.10.10	TCP	58	443 → 17852 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
23	0.000288	142.111.211.241	10.10.10.10	TCP	58	80 → 62123 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
24	0.000293	104.164.137.115	10.10.10.10	TCP	58	80 → 836 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
25	0.000296	107.175.44.68	10.10.10.10	TCP	58	80 → 33253 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
26	0.000318	136.0.160.222	10.10.10.10	TCP	58	80 → 12635 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
27	0.000324	142.252.105.94	10.10.10.10	TCP	58	80 → 23424 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
28	0.000327	166.88.52.57	10.10.10.10	TCP	58	80 → 41653 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
29	0.000336	107.165.252.39	10.10.10.10	TCP	58	80 → 6917 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
30	0.000384	172.121.138.79	10.10.10.10	TCP	58	80 → 60369 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
31	0.000396	172.121.138.79	10.10.10.10	TCP	58	80 → 18719 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
32	0.000435	23.230.10.251	10.10.10.10	TCP	58	443 → 7399 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400
33	0.000444	104.252.167.152	10.10.10.10	TCP	58	80 → 24850 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
34	0.000450	45.38.180.102	10.10.10.10	TCP	54	443 → 21575 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	0.000457	104.253.64.173	10.10.10.10	TCP	54	80 → 16632 [RST] Seq=1 Win=0 Len=0
36	0.000487	107.165.240.21	10.10.10.10	TCP	54	80 → 52109 [RST] Seq=1 Win=0 Len=0

DDOS

overview

Seperti yang kita ketahui, SynAck merupakan response server setelah menerima syn request, dan dikarenakan ada banyak request SynAck ini bisa kita asumsikan bahwa server sedang di serang



No.	Time	Source	Destination	Protocol	Length	Info
101	0.001480	107.165.63.190	10.10.10.10	TCP	58	80 → 46114 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
102	0.001483	166.88.253.194	10.10.10.10	TCP	58	80 → 65233 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
103	0.001499	107.186.167.176	10.10.10.10	TCP	58	80 → 8034 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
104	0.001502	121.42.81.211	10.10.10.10	TCP	58	80 → 5060 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400
106	0.001513	172.121.35.102	10.10.10.10	TCP	58	80 → 10518 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
108	0.001536	166.88.253.194	10.10.10.10	TCP	58	80 → 30334 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
109	0.001548	142.111.179.150	10.10.10.10	TCP	58	80 → 27438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
110	0.001571	107.165.8.91	10.10.10.10	TCP	58	80 → 4600 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
111	0.001594	205.164.6.11	10.10.10.10	TCP	58	80 → 62101 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
112	0.001601	136.0.199.207	10.10.10.10	TCP	58	80 → 36037 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
113	0.001604	166.88.48.171	10.10.10.10	TCP	58	80 → 62028 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
115	0.001608	172.252.115.215	10.10.10.10	TCP	58	80 → 1211 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
116	0.001639	107.165.8.91	10.10.10.10	TCP	58	443 → 50026 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
122	0.001742	172.252.115.215	10.10.10.10	TCP	58	80 → 2094 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
123	0.001801	107.187.30.108	10.10.10.10	TCP	58	80 → 5521 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
124	0.001828	107.164.90.205	10.10.10.10	TCP	58	80 → 58467 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
125	0.001843	104.252.94.7	10.10.10.10	TCP	58	80 → 63372 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
127	0.002374	104.252.167.9	10.10.10.10	TCP	58	80 → 2244 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
129	0.002382	107.187.119.170	10.10.10.10	TCP	58	80 → 36761 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
131	0.002386	45.39.70.115	10.10.10.10	TCP	58	80 → 26831 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
132	0.002388	142.111.181.210	10.10.10.10	TCP	58	80 → 65142 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
134	0.002392	104.253.179.37	10.10.10.10	TCP	58	80 → 5515 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
135	0.002393	142.111.181.136	10.10.10.10	TCP	58	80 → 18091 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
136	0.002395	107.186.39.252	10.10.10.10	TCP	58	80 → 46845 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
137	0.002397	107.164.87.221	10.10.10.10	TCP	58	80 → 14163 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
138	0.002399	104.165.57.123	10.10.10.10	TCP	58	80 → 17737 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
140	0.002403	50.118.226.114	10.10.10.10	TCP	58	80 → 30840 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
141	0.002405	166.88.218.4	10.10.10.10	TCP	58	80 → 6058 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
142	0.002407	172.252.201.196	10.10.10.10	TCP	58	80 → 48824 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
143	0.002409	45.39.209.50	10.10.10.10	TCP	58	80 → 46313 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
144	0.002411	23.230.125.165	10.10.10.10	TCP	58	80 → 33466 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
145	0.002413	166.88.103.199	10.10.10.10	TCP	58	80 → 53663 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
146	0.002414	45.39.205.219	10.10.10.10	TCP	58	443 → 53915 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
147	0.002418	23.27.228.46	10.10.10.10	TCP	58	80 → 43439 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
148	0.002419	166.88.218.252	10.10.10.10	TCP	58	80 → 65278 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400
149	0.002422	45.39.209.107	10.10.10.10	TCP	58	80 → 44532 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400

BRUTEFORCE

tcp.stream eq 0

Disini kita ikutin flownya setiap stream TCPnya, klo kita lihat di TCP iterattion 0 dia ada nyoba password 1 buat user Bro

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	192.168.56.101	TCP	78	54017 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489244036 TSecr=0 SACK_PERM
2	0.000043	192.168.56.101	192.168.56.1	TCP	74	21 → 54017 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=2590583 TSecr=489244036 WS=128
3	0.000454	192.168.56.1	192.168.56.101	TCP	66	54017 → 21 [ACK] Seq=1 Ack=1 Win=131768 Len=0 TSval=489244036 TSecr=2590583
4	0.006031	192.168.56.101	192.168.56.1	FTP	135	Response: 220 redmint FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
5	0.006495	192.168.56.1	192.168.56.101	TCP	66	54017 → 21 [ACK] Seq=1 Ack=70 Win=131696 Len=0 TSval=489244042 TSecr=2590584
6	0.006512	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
7	0.006586	192.168.56.101	192.168.56.1	TCP	66	21 → 54017 [ACK] Seq=70 Ack=11 Win=14592 Len=0 TSval=2590585 TSecr=489244042
8	0.009093	192.168.56.101	192.168.56.1	FTP	98	Response: 331 Password required for bro.
9	0.009550	192.168.56.1	192.168.56.101	TCP	66	54017 → 21 [ACK] Seq=11 Ack=102 Win=131664 Len=0 TSval=489244045 TSecr=2590585
10	0.009567	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 1
11	0.046780	192.168.56.101	192.168.56.1	TCP	66	21 → 54017 [ACK] Seq=102 Ack=19 Win=14592 Len=0 TSval=2590595 TSecr=489244045
12	2.371080	192.168.56.101	192.168.56.1	FTP	88	Response: 530 Login incorrect.
13	2.371535	192.168.56.1	192.168.56.101	TCP	66	54017 → 21 [ACK] Seq=19 Ack=124 Win=131640 Len=0 TSval=489246393 TSecr=2591176
14	2.371558	192.168.56.1	192.168.56.101	FTP	72	Request: QUIT
15	2.371667	192.168.56.101	192.168.56.1	TCP	66	21 → 54017 [ACK] Seq=124 Ack=25 Win=14592 Len=0 TSval=2591176 TSecr=489246393
16	2.371849	192.168.56.101	192.168.56.1	FTP	80	Response: 221 Goodbye.
17	2.371999	192.168.56.1	192.168.56.101	TCP	66	54017 → 21 [ACK] Seq=25 Ack=138 Win=131624 Len=0 TSval=489246393 TSecr=2591176
18	2.372007	192.168.56.1	192.168.56.101	TCP	66	54017 → 21 [FIN, ACK] Seq=25 Ack=138 Win=131624 Len=0 TSval=489246393 TSecr=2591176
19	2.372771	192.168.56.101	192.168.56.1	TCP	66	21 → 54017 [FIN, ACK] Seq=138 Ack=26 Win=14592 Len=0 TSval=2591176 TSecr=489246393

Hasil follow tcp.stream eq 0

Wireshark · Follow TCP Stream (tcp.stream eq 0) · bruteforce.pcap

```
220 redmint FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
USER bro
331 Password required for bro.
PASS 1
530 Login incorrect.
QUIT
221 Goodbye.
```

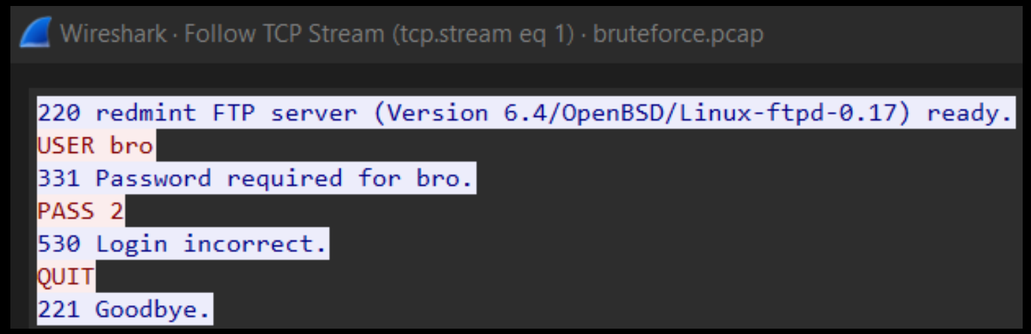
BRUTEFORCE

tcp.stream eq 1

Nah di TCP iterasi ke 1 kita bisa lihat ada reqeust buat user bro dan menggunakan passwordnya 2. Disini kita sudah mulai bisa mencium bau bau bruteforce

No.	Time	Source	Destination	Protocol	Length	Info
21	2.377150	192.168.56.1	192.168.56.101	TCP	78	54018 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489246397 TSecr=0 SACK_PERM
22	2.377194	192.168.56.101	192.168.56.1	TCP	74	21 → 54018 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=2591177 TSecr=489246397 WS=128
23	2.377417	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [ACK] Seq=1 Ack=1 Win=131768 Len=0 TSval=489246397 TSecr=2591177
24	2.382200	192.168.56.101	192.168.56.1	FTP	135	Response: 220 redmint FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
25	2.382251	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [ACK] Seq=1 Ack=70 Win=131696 Len=0 TSval=489246402 TSecr=2591178
26	2.382326	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
27	2.382338	192.168.56.101	192.168.56.1	TCP	66	21 → 54018 [ACK] Seq=70 Ack=11 Win=14592 Len=0 TSval=2591179 TSecr=489246402
28	2.384485	192.168.56.101	192.168.56.1	FTP	98	Response: 331 Password required for bro.
29	2.384574	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [ACK] Seq=11 Ack=102 Win=131664 Len=0 TSval=489246404 TSecr=2591179
30	2.384678	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 2
31	2.422066	192.168.56.101	192.168.56.1	TCP	66	21 → 54018 [ACK] Seq=102 Ack=19 Win=14592 Len=0 TSval=2591189 TSecr=489246404
32	4.827475	192.168.56.101	192.168.56.1	FTP	88	Response: 530 Login incorrect.
33	4.827936	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [ACK] Seq=19 Ack=124 Win=131640 Len=0 TSval=489248833 TSecr=2591790
34	4.828223	192.168.56.1	192.168.56.101	FTP	72	Request: QUIT
35	4.828302	192.168.56.101	192.168.56.1	TCP	66	21 → 54018 [ACK] Seq=124 Ack=25 Win=14592 Len=0 TSval=2591790 TSecr=489248833
36	4.828526	192.168.56.101	192.168.56.1	FTP	80	Response: 221 Goodbye.
37	4.828975	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [ACK] Seq=25 Ack=138 Win=131624 Len=0 TSval=489248833 TSecr=2591790
38	4.828995	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [FIN, ACK] Seq=25 Ack=138 Win=131624 Len=0 TSval=489248833 TSecr=2591790
39	4.829324	192.168.56.101	192.168.56.1	TCP	66	21 → 54018 [FIN, ACK] Seq=138 Ack=26 Win=14592 Len=0 TSval=2591790 TSecr=489248833
40	4.829965	192.168.56.1	192.168.56.101	TCP	66	54018 → 21 [ACK] Seq=26 Ack=139 Win=131624 Len=0 TSval=489248834 TSecr=2591790

Hasil follow tcp.stream eq 1



BRUTEFORCE

tcp.stream eq 29

TCP streamnya berlanjut terus hingga ke 30 yang berisi dia coba pass 30 pada user Bro. Dengan demikian bisa kita konklusikan kalo memang ini sebuah bruteforce attempt

No.	Time	Source	Destination	Protocol	Length	Info
587	57.448053	192.168.56.1	192.168.56.101	TCP	78	54048 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489301119 TSecr=0 SACK_PERM
588	57.448098	192.168.56.101	192.168.56.1	TCP	74	21 → 54048 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=2604945 TSecr=489301119 W
589	57.448344	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [ACK] Seq=1 Ack=1 Win=131768 Len=0 TSval=489301119 TSecr=2604945
590	57.454920	192.168.56.101	192.168.56.1	FTP	135	Response: 220 redmint FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
591	57.455145	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [ACK] Seq=1 Ack=70 Win=131696 Len=0 TSval=489301125 TSecr=2604947
592	57.455383	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
593	57.455461	192.168.56.101	192.168.56.1	TCP	66	21 → 54048 [ACK] Seq=70 Ack=11 Win=14592 Len=0 TSval=2604947 TSecr=489301125
594	57.457293	192.168.56.101	192.168.56.1	FTP	98	Response: 331 Password required for bro.
595	57.457335	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [ACK] Seq=11 Ack=102 Win=131664 Len=0 TSval=489301127 TSecr=2604947
596	57.457335	192.168.56.1	192.168.56.101	FTP	75	Request: PASS 30
597	57.494048	192.168.56.101	192.168.56.1	TCP	66	21 → 54048 [ACK] Seq=102 Ack=20 Win=14592 Len=0 TSval=2604957 TSecr=489301127
598	59.116920	192.168.56.101	192.168.56.1	FTP	88	Response: 530 Login incorrect.
599	59.117299	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [ACK] Seq=20 Ack=124 Win=131640 Len=0 TSval=489302782 TSecr=2605362
600	59.117344	192.168.56.1	192.168.56.101	FTP	72	Request: QUIT
601	59.117416	192.168.56.101	192.168.56.1	TCP	66	21 → 54048 [ACK] Seq=124 Ack=26 Win=14592 Len=0 TSval=2605362 TSecr=489302782
602	59.117560	192.168.56.101	192.168.56.1	FTP	80	Response: 221 Goodbye.
603	59.117660	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [ACK] Seq=26 Ack=138 Win=131624 Len=0 TSval=489302782 TSecr=2605362
604	59.117791	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [FIN, ACK] Seq=26 Ack=138 Win=131624 Len=0 TSval=489302782 TSecr=2605362
605	59.118113	192.168.56.101	192.168.56.1	TCP	66	21 → 54048 [FIN, ACK] Seq=138 Ack=27 Win=14592 Len=0 TSval=2605362 TSecr=489302782
606	59.118300	192.168.56.1	192.168.56.101	TCP	66	54048 → 21 [ACK] Seq=27 Ack=139 Win=131624 Len=0 TSval=489302783 TSecr=2605362

Hasil follow tcp.stream eq 29

Wireshark · Follow TCP Stream (tcp.stream eq 29) · bruteforce.pcap

```
220 redmint FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
USER bro
331 Password required for bro.
PASS 30
530 Login incorrect.
QUIT
221 Goodbye.
```