TUGAS COMPUTER FORENSIC

NMAP BEHAVIOR & DDOS ANALYSIS

DATA DIRI ANGGOTA

2540120603
Nicolas Saputra Gunawan

2540124620
Jeffrey Jingga

2540119633
Mikael Wiryamanta Wijaya

2540124740
Satya Kusuma

2540115181
Pitra Winarianto

Introduction

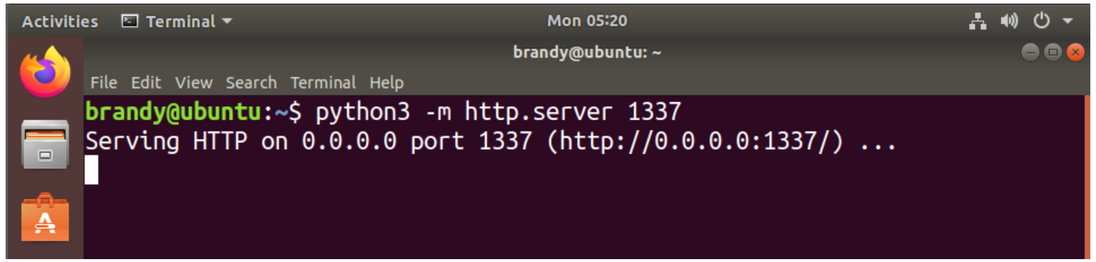
Testing nmap using ubuntu virtual box

1. Host HTTP Server in Ubuntu on port 8888
2. Capture network processes using WIRESHARK
3. NMAP Scan
4. Network packets captured in WIRESHARK

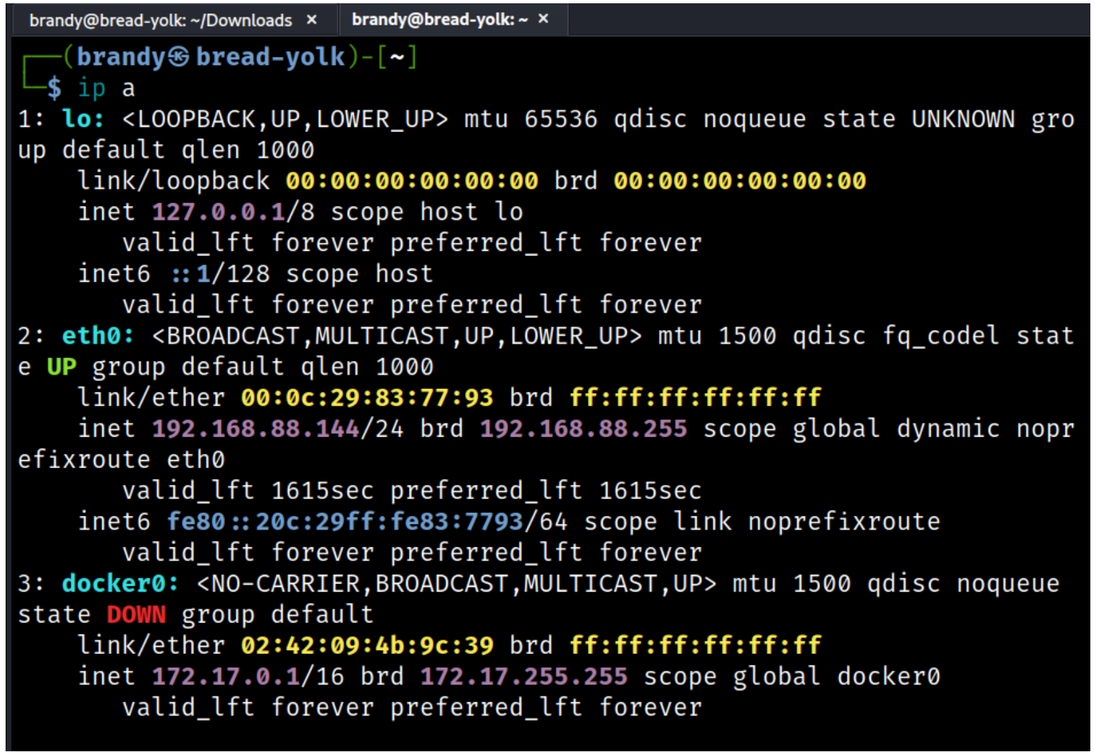
Testing DDOS using Ping of Death

1. Host HTTP Server in Ubuntu on port 8888
2. Capture network processes using WIRESHARK
3. Ping of Death
4. Network packets captured in WIRESHARK

Target [Ubuntu 18.04 Virtual Box]



UBUNTU



KALI LINUX

NMAP

nmap -p- 192.168.88.144/24

```
┌──(brandy㉿bread-yolk)-[~/Downloads]
└─$ nmap -p- 192.168.88.144/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-01 05:20 PST
Nmap scan report for 192.168.88.1
Host is up (0.00027s latency).
Not shown: 65521 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5040/tcp  open  unknown
7680/tcp  open  pando-pub
8834/tcp  open  nessus-xmlrpc
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49671/tcp open  unknown

Nmap scan report for 192.168.88.2
Host is up (0.00018s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
53/tcp filtered domain

Nmap scan report for 192.168.88.144
```

```
7680/tcp  open  pando-pub
8834/tcp  open  nessus-xmlrpc
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49671/tcp open  unknown

Nmap scan report for 192.168.88.2
Host is up (0.00018s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
53/tcp filtered domain

Nmap scan report for 192.168.88.144
Host is up (0.00040s latency).
All 65535 scanned ports on 192.168.88.144 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap scan report for 192.168.88.150
Host is up (0.00057s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
1337/tcp open  waste

Nmap done: 256 IP addresses (4 hosts up) scanned in 58.39 seconds
```

Ubuntu 18.04's IP

Opened port

NMAP

PENJELASAN

Dalam proses pembuktian ini, kami menyalakan dua mesin. Mesin pertama -> Kali Linux dan mesin kedua yaitu Ubuntu 18.04. Lalu kami melakukan nmap scan untuk mengidentifikasi IP dari mesin target.

Pada mesin target kami menyalakan simple python server dengan port 1337. Lalu ketika proses nmap pada mesin Kali Linux dijalankan, diketahui bahwa IP dari mesin target yaitu --> 192.168.88.150. Pernyataan ini didukung dengan port dan service yang dibuka oleh mesin tersebut .

NMAP

nmap -p- -sVC 192.168.88.150 --min-rate 1000

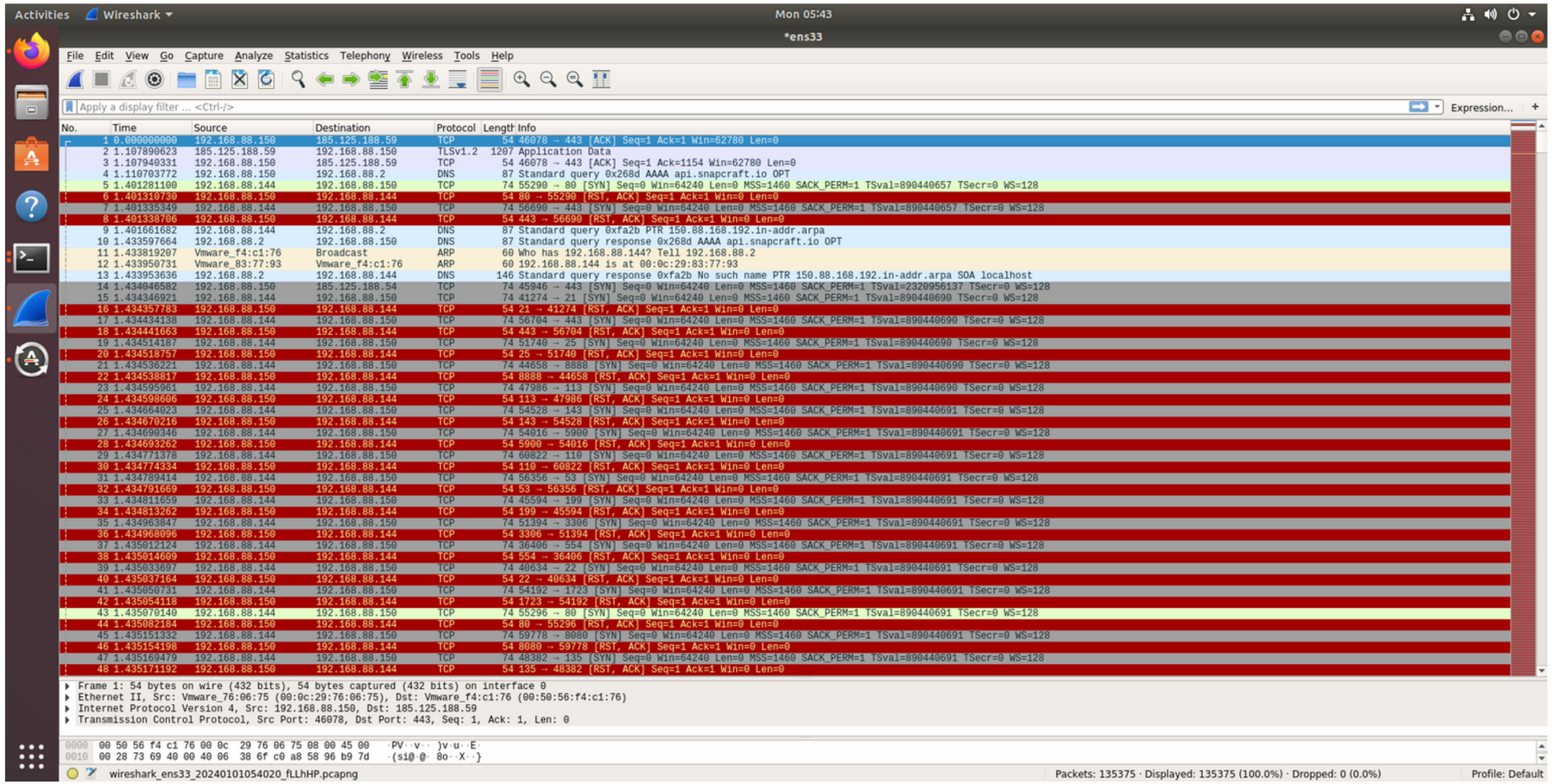
```
┌──(brandy㉿bread-volk)-[~/Downloads]
└─$ nmap -p- -sVC 192.168.88.150 --min-rate 1000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-01 05:40 PST
Nmap scan report for 192.168.88.150
Host is up (0.00050s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
1337/tcp open  http    SimpleHTTPServer 0.6 (Python 3.6.9)
|_http-title: Directory listing for /
|_http-server-header: SimpleHTTP/0.6 Python/3.6.9

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.11 seconds
```

Open port discovered

Wireshark Preview

Wireshark capture in Ubuntu 18.04



Wireshark Preview

Wireshark capture indicating nmap scans

100	1.436285258	192.168.88.150	192.168.88.144	TCP	54	53968 → 52724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	1.436299977	192.168.88.144	192.168.88.150	TCP	74	46430 → 28378 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440692 TSecr=0 WS=128
102	1.436301630	192.168.88.150	192.168.88.144	TCP	54	28378 → 46430 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
103	1.436359406	192.168.88.144	192.168.88.150	TCP	74	37058 → 41305 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440692 TSecr=0 WS=128
104	1.436362322	192.168.88.150	192.168.88.144	TCP	54	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
105	1.436376069	192.168.88.144	192.168.88.150	TCP	74	58022 → 2526 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440692 TSecr=0 WS=128
106	1.436377733	192.168.88.150	192.168.88.144	TCP	54	2526 → 58022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	1.436429887	192.168.88.144	192.168.88.150	TCP	74	40318 → 55072 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440692 TSecr=0 WS=128
108	1.436432151	192.168.88.150	192.168.88.144	TCP	54	55072 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	1.436547422	192.168.88.144	192.168.88.150	TCP	74	46130 → 54881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440692 TSecr=0 WS=128
110	1.436553203	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	1.436570548	192.168.88.144	192.168.88.150	TCP	74	41944 → 32182 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440692 TSecr=0 WS=128
112	1.436573013	192.168.88.150	192.168.88.144	TCP	54	32182 → 41944 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	1.436587201	192.168.88.144	192.168.88.150	TCP	74	35446 → 65364 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
114	1.436588815	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
115	1.436651500	192.168.88.144	192.168.88.150	TCP	74	33018 → 56885 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
116	1.436657282	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
117	1.436674406	192.168.88.144	192.168.88.150	TCP	74	39944 → 17929 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
118	1.436676480	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	1.436694196	192.168.88.144	192.168.88.150	TCP	74	45570 → 61017 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
120	1.436695949	192.168.88.150	192.168.88.144	TCP	54	61017 → 45570 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	1.436762693	192.168.88.144	192.168.88.150	TCP	74	59452 → 36928 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
122	1.436765158	192.168.88.150	192.168.88.144	TCP	54	36928 → 59452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
123	1.436828164	192.168.88.144	192.168.88.150	TCP	74	50708 → 18780 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
124	1.436830509	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	1.436884837	192.168.88.144	192.168.88.150	TCP	74	42248 → 23707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
126	1.436888144	192.168.88.150	192.168.88.144	TCP	54	23707 → 42248 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
127	1.436903675	192.168.88.144	192.168.88.150	TCP	74	34022 → 33243 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
128	1.436905528	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	1.436923294	192.168.88.144	192.168.88.150	TCP	74	54346 → 26721 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
130	1.436924947	192.168.88.150	192.168.88.144	TCP	54	26721 → 54346 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
131	1.437010328	192.168.88.144	192.168.88.150	TCP	74	54070 → 16417 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
132	1.437013044	192.168.88.150	192.168.88.144	TCP	54	16417 → 54070 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	1.437027522	192.168.88.144	192.168.88.150	TCP	74	57054 → 14701 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
134	1.437029236	192.168.88.150	192.168.88.144	TCP	54	14701 → 57054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
135	1.437088324	192.168.88.144	192.168.88.150	TCP	74	58382 → 12566 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
136	1.437092623	192.168.88.150	192.168.88.144	TCP	54	12566 → 58382 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
137	1.437116260	192.168.88.144	192.168.88.150	TCP	74	42070 → 44523 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
138	1.437119286	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
139	1.437214958	192.168.88.144	192.168.88.150	TCP	74	40876 → 52879 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
140	1.437218595	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	1.437232382	192.168.88.144	192.168.88.150	TCP	74	58076 → 19276 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
142	1.437234066	192.168.88.150	192.168.88.144	TCP	54	19276 → 58076 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	1.437256521	192.168.88.144	192.168.88.150	TCP	74	44498 → 43722 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
144	1.437258384	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	1.437320048	192.168.88.144	192.168.88.150	TCP	74	49924 → 25023 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128
146	1.437322503	192.168.88.150	192.168.88.144	TCP	[illegible]	[illegible] [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
147	1.437336992	192.168.88.144	192.168.88.150	TCP	74	37858 → 51380 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890440693 TSecr=0 WS=128

▸ Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

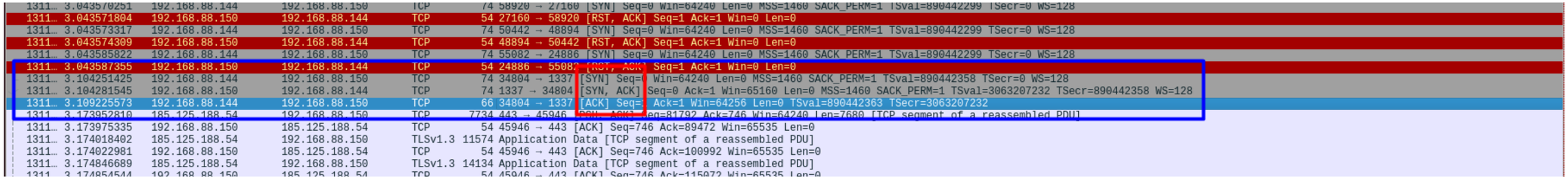
NMAP

PENJELASAN

Pada mulanya, kami menjalankan wireshark capture packets pada mesin target. Setelah itu, kami melakukan nmap scan pada ip mesin target. Setelah port yang terbuka teridentifikasi, kami mematikan capture packets di wireshark.

Berdasarkan hasil yang didapat, diketahui terdapat banyak packet SYN scan dengan packet bytes yang relatif kecil (74). Tidak hanya itu, SYN packets ini terus berdatangan dalam rentan waktu yang berdekatan hal ini mengindikasikan automasi dalam percobaan 3-way handshake.

Pola pada packet ini merupakan contoh behavior dari nmap. Pada akhirnya nmap berhasil melakukan 3-way handshake (menemukan port yang terbuka --> 1337).



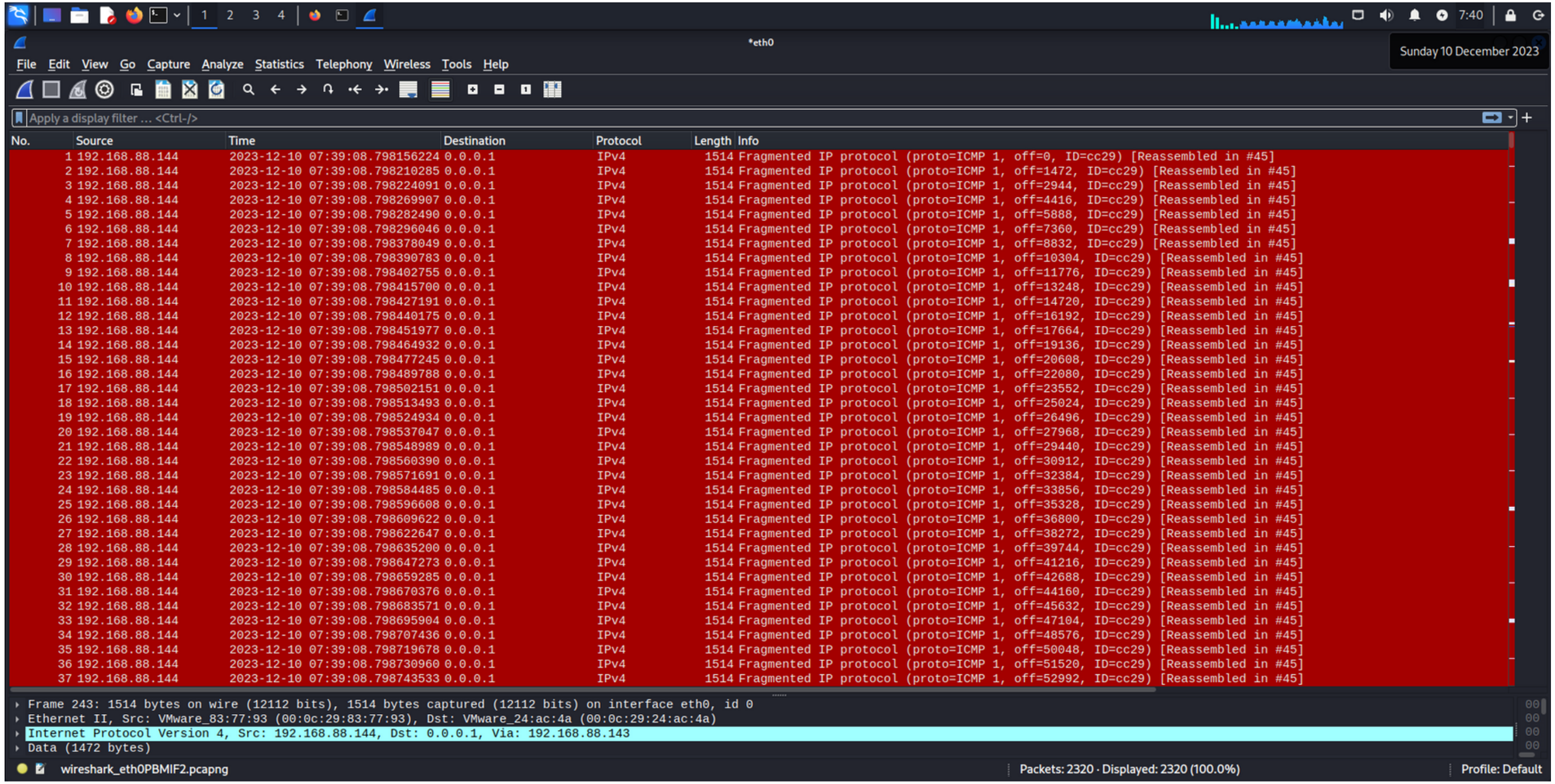
1311…	3.043570251	192.168.88.144	192.168.88.150	TCP	74	58920 → 27160 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890442299 TSecr=0 WS=128
1311…	3.043571804	192.168.88.150	192.168.88.144	TCP	54	27160 → 58920 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1311…	3.043573317	192.168.88.144	192.168.88.150	TCP	74	50442 → 48894 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890442299 TSecr=0 WS=128
1311…	3.043574309	192.168.88.150	192.168.88.144	TCP	54	48894 → 50442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1311…	3.043585822	192.168.88.144	192.168.88.150	TCP	74	55082 → 24886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890442299 TSecr=0 WS=128
1311…	3.043587355	192.168.88.150	192.168.88.144	TCP	54	24886 → 55082 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1311…	3.104251425	192.168.88.144	192.168.88.150	TCP	74	34804 → 1337 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=890442358 TSecr=0 WS=128
1311…	3.104281545	192.168.88.150	192.168.88.144	TCP	74	1337 → 34804 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3063207232 TSecr=890442358 WS=128
1311…	3.109225573	192.168.88.144	192.168.88.150	TCP	66	34804 → 1337 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=890442363 TSecr=3063207232
1311…	3.173952810	185.125.188.54	192.168.88.150	TCP	7734	443 → 45946 [PSH, ACK] Seq=81792 Ack=746 Win=64240 Len=7680 [TCP segment of a reassembled PDU]
1311…	3.173975335	192.168.88.150	185.125.188.54	TCP	54	45946 → 443 [ACK] Seq=746 Ack=89472 Win=65535 Len=0
1311…	3.174018402	185.125.188.54	192.168.88.150	TLSv1.3	11574	Application Data [TCP segment of a reassembled PDU]
1311…	3.174022981	192.168.88.150	185.125.188.54	TCP	54	45946 → 443 [ACK] Seq=746 Ack=100992 Win=65535 Len=0
1311…	3.174846689	185.125.188.54	192.168.88.150	TLSv1.3	14134	Application Data [TCP segment of a reassembled PDU]
1311…	3.174854544	192.168.88.150	185.125.188.54	TCP	54	45946 → 443 [ACK] Seq=746 Ack=115072 Win=65535 Len=0

DDOS using Ping of Death

ping <ip> -s 65000 -t 1 -n 1

```
┌──(brandy㉿bread-yolk)-[~]
└─$ ping 192.168.88.143 -s 65000 -t 1 -n 1
PING 1 (0.0.0.1) 65000(65068) bytes of data.
```

Wireshark Preview



DDOS using Ping of Death

PENJELASAN

Ping of death (PoD) attack adalah salah satu bentuk DDOS, PoD adalah serangan khusus yang dilakukan dengan mengirimkan paket ICMP (Internet Control Message Protocol) yang berukuran lebih besar dari batas maksimum yang diperbolehkan.

Metode yang digunakan disini cukup mudah, yakni dengan melakukan ping ke sebuah alamat IP sebesar 65000 bytes (melewati batas maksimum), hal ini berpotensi menyebabkan kegagalan atau crash pada sistem target yang tidak dapat memproses ukuran paket yang tidak valid,

Serangan ini dapat terdeteksi menggunakan WireShark, untuk mencoba menganalisanya, kami mencoba mengirimkan ping ke sebuah alamat IP sembari menyalakan WireShark. Dan pada gambar diatas terlihat bahwa terdapat sebuah anomali paket yang sama dikirimkan secara berulang.

THANK YOU!