

INTRODUCTION TO DIGITAL FORENSICS ASSIGNMENT 2



Emma van den Broek | s2804859
Aukje Hekstra | s2294184
Rik Helder | s2864010
Inèz Hemme | s2429837
Ewoud Janus | s2395762
Koen Wilms | s1818872

Motivation and Goals

DDoS attacks, short for Distributed Denial of Service attacks, are a type of cyber attack during which an attacker attempts to flood a server with traffic to overwhelm its infrastructure. These attacks are an ever growing problem, with an increasing number of targets falling victim to such attacks. A report from Zayo Group Holdings, Inc. reveals that in the early part of 2023, DDoS attacks were up to 200% in comparison to 2022 (Jackson, 2023). Microsoft alone mitigated upward to 520,000 unique attacks against their global infrastructure in the year 2022 (Azure Network Security Team, 2023). According to Microsoft in 2022, the majority of the DDoS attacks were TCP attack vectors, making up 63% of all attack traffic (Azure Network Security Team, 2023).

There are different types of DDoS attacks. Three categories that can be defined are User Datagram Protocol (UDP)-based attacks, Transmission Control Protocol (TCP)-based attacks and Application layer attacks. During this experiment, a look will be taken at SYN-flood attacks, which fall under the category TCP-based attacks.

Most people do not have the resources to perform a large DDoS attack themselves, but booter and stressor services are easily available online. In order to make use of these illegal services, a user does not have to go to the dark web, as an individual can type in “booter”, “stresser”, “DDoSer” or a similar query into a search engine like Google, and get a list of booter services available to them. A person can then pay these providers a small sum of money, even as little as 5 USD, to perform a DDoS attack on a target.

DDoS attacks happen across a lot of different sectors, like governmental organisations, financial institutions like banks, but also in gaming communities and in schools. These attacks can have a large impact on the workings of these organisations as their services become unavailable when they are DDoS'ed. Making, selling and spreading DDoS attacks is a punishable offence according to the Dutch law. Still, a lot of DDoS attacks are not tracked and punished, either because the victim of the attack does not contact authorities - think of gamers that were DDoS'ed during an online game - or because the perpetrator of the attack cannot be found. This could be either because of a lack of resources or because it can be difficult to trace an attack back to the individual who bought the booter services.

Considering the fact that DDoS attacks are a growing problem that can have severe consequences on society and the lives of individual people, it is important to take action to protect against these attacks. In order to be able to do this, it is important to have a good understanding of how these attacks are performed, how to identify specific kinds of DDoS attacks, how to analyse them and to know which information about the perpetrator and the attack can be found during an analysis. The goal of this experiment is to gain this understanding by performing a DDoS attack and analysing the capture of the attack.

Methodology and Results

In order to investigate and understand the phenomenon of DDoS attacks, a mock-attack was performed on September 27th during the second lecture of Introduction to Digital Forensics for the minor Cybersecurity and Cybercrime. The idea behind this was to give students hands-on experience with DDoS attacks and what happens when an attack is performed. The teacher set up a local network within the University network so the actual University network was not used or damaged in any way.

The software used to perform this attack was the Anon Cannon software, which is a DoS software that allows users to perform a DoS attack on a target. Roughly 17 participants used their laptop with the Anon Cannon software, together performing a DDoS attack on the teacher's router. The 'attackers' all selected the same IP-address of the router, selected the same port, port 80, and at the same time, started to attack the router.

This type of attack, where a port is flooded with connection requests (SYN) packets, is called a SYN flood attack. With this attack, an attacker takes advantage of the three way handshake process of a TCP connection. The attacker exploits the fact that, after sending an initial SYN packet, a server will respond with one or more SYN/ACK packets and will wait for the final step, which is the receiving of the ACK. By sending a lot of SYN packets, the server temporarily has to open a lot of open ports, which results in legitimate users not being able to connect and also possibly to the crashing of the server.

Port 80 is the port number assigned to the Hypertext Transfer Protocol (HTTP) under TCP protocol.

During the attack, the teacher ran a wireshark capture to capture all traffic over the router. The teacher then sent the capture of the attack to their students with the questions below.

1. How many records are in the entire trace?

There are a total of 620304 packets (See Fig. 1).

Statistics

<u>Measurement</u>	<u>Captured</u>
Packets	620304
Time span, s	90.174

Fig. 1. Capture File Properties.

2. What is the duration of the entire trace?

The duration of the entire trace is 90.174052 seconds (see Fig. 1).

3. Add print-screens of 3 examples of packets that are NOT part of the attack. Explain what those packets are.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=0x624d, seq=96/24576, ttl=64 (reply in 2)
2	0.030106	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=0x624d, seq=96/24576, ttl=255 (request in 1)
3	0.036262	192.168.0.115	192.168.0.255	NDNS	92	Name query 00 0040:000
4	0.343125	192.168.0.111	224.0.0.251	NDNS	227	Standard query response 0x0000 TXT, cache flush NSDC, cache flush Haidau's MacBook Air - companion-link_tcp.local
5	0.645839	192.168.0.100	192.168.0.2	DNS	84	Standard query 0x619f HTTPS 1-courier.push.apple.com
6	0.645839	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xb907 HTTPS stocks-data-service.apple.com
7	0.646076	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xa4e7 A stocks-data-service.apple.com
8	0.646105	192.168.0.2	192.168.0.100	ICMP	112	Destination unreachable (Port unreachable)
9	0.646106	192.168.0.2	192.168.0.100	ICMP	112	Destination unreachable (Port unreachable)
10	0.646384	192.168.0.2	192.168.0.100	ICMP	117	Destination unreachable (Port unreachable)
11	0.000331	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=0x624d, seq=97/24832, ttl=64 (reply in 12)
12	1.011237	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=0x624d, seq=97/24832, ttl=255 (request in 11)
13	1.472636	D-LinkIn_12:86:d8	Apple_e1:b0:bd	ARP	42	192.168.0.2 is at 3c:1e:04:12:86:d8
14	1.605340	192.168.0.100	192.168.0.2	DNS	90	Standard query 0xa6dc HTTPS self.events.data.microsoft.com
15	1.605565	192.168.0.100	192.168.0.2	DNS	90	Standard query 0xb1b7 A self.events.data.microsoft.com
16	1.605944	192.168.0.100	192.168.0.2	DNS	80	Standard query 0xb81c AAAA eds-rs-mw.northwave.nl
17	1.607230	192.168.0.2	192.168.0.100	ICMP	118	Destination unreachable (Port unreachable)
18	1.670441	192.168.0.100	192.168.0.2	DNS	97	Standard query 0xb02d HTTPS officecl-mauservice.azurewebsites.net
19	1.670705	192.168.0.100	192.168.0.2	DNS	97	Standard query 0xc091 A officecl-mauservice.azurewebsites.net
20	2.000180	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=0x624d, seq=98/25088, ttl=64 (reply in 21)
21	2.010040	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=0x624d, seq=98/25088, ttl=255 (request in 20)
22	2.597209	192.168.0.110	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.3.0 1.3.6.1.4.1.1602.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.3.1.12.0
23	2.599112	192.168.0.110	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.3.0 1.3.6.1.4.1.1602.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.3.1.12.0
24	2.608712	IntelCor_e2:ed:a7	Broadcast	ARP	42	Who has 192.168.0.17 Tell 192.168.0.101
25	2.745497	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xb907 HTTPS stocks-data-service.apple.com
26	2.745562	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xa4e7 A stocks-data-service.apple.com

Fig. 2. Packet 1, A ping request from Apple_e1:b0:bd to D-LinkIn_12:86:d8.

Fig.2 displays packet 1, which is a ping request from an Apple device to a D-Link device.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=0x624d, seq=96/24576, ttl=64 (reply in 2)
2	0.030106	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=0x624d, seq=96/24576, ttl=255 (request in 1)
3	0.036262	192.168.0.115	192.168.0.255	NDNS	92	Name query 00 0040:000
4	0.343125	192.168.0.111	224.0.0.251	NDNS	227	Standard query response 0x0000 TXT, cache flush NSDC, cache flush Haidau's MacBook Air - companion-link_tcp.local
5	0.645839	192.168.0.100	192.168.0.2	DNS	84	Standard query 0x619f HTTPS 1-courier.push.apple.com
6	0.645839	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xb907 HTTPS stocks-data-service.apple.com
7	0.646076	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xa4e7 A stocks-data-service.apple.com
8	0.646105	192.168.0.2	192.168.0.100	ICMP	112	Destination unreachable (Port unreachable)
9	0.646106	192.168.0.2	192.168.0.100	ICMP	112	Destination unreachable (Port unreachable)
10	0.646384	192.168.0.2	192.168.0.100	ICMP	117	Destination unreachable (Port unreachable)
11	0.000331	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=0x624d, seq=97/24832, ttl=64 (reply in 12)
12	1.011237	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=0x624d, seq=97/24832, ttl=255 (request in 11)
13	1.472636	D-LinkIn_12:86:d8	Apple_e1:b0:bd	ARP	42	192.168.0.2 is at 3c:1e:04:12:86:d8
14	1.605340	192.168.0.100	192.168.0.2	DNS	90	Standard query 0xa6dc HTTPS self.events.data.microsoft.com
15	1.605565	192.168.0.100	192.168.0.2	DNS	90	Standard query 0xb1b7 A self.events.data.microsoft.com
16	1.605944	192.168.0.100	192.168.0.2	DNS	80	Standard query 0xb81c AAAA eds-rs-mw.northwave.nl
17	1.607230	192.168.0.2	192.168.0.100	ICMP	118	Destination unreachable (Port unreachable)
18	1.670441	192.168.0.100	192.168.0.2	DNS	97	Standard query 0xb02d HTTPS officecl-mauservice.azurewebsites.net
19	1.670705	192.168.0.100	192.168.0.2	DNS	97	Standard query 0xc091 A officecl-mauservice.azurewebsites.net
20	2.000180	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=0x624d, seq=98/25088, ttl=64 (reply in 21)
21	2.010040	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=0x624d, seq=98/25088, ttl=255 (request in 20)
22	2.597209	192.168.0.110	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.3.0 1.3.6.1.4.1.1602.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.3.1.12.0
23	2.599112	192.168.0.110	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.3.0 1.3.6.1.4.1.1602.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.1.1.0 1.3.6.1.4.1.1602.1.3.1.12.0
24	2.608712	IntelCor_e2:ed:a7	Broadcast	ARP	42	Who has 192.168.0.17 Tell 192.168.0.101
25	2.745497	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xb907 HTTPS stocks-data-service.apple.com
26	2.745562	192.168.0.100	192.168.0.2	DNS	89	Standard query 0xa4e7 A stocks-data-service.apple.com

Frame 5: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface en0, id 0 (outbound) Section number: 1 Interface id: 0 (en0) Packet flags: 0x00000002 Encapsulation type: Ethernet (1) Arrival time: Oct 4, 2023 14:14:16.044873000 W. Europe Daylight Time [Time shift for this packet: 0.000000000 seconds] Epoch time: 169622956.044873000 seconds [Time delta from previous captured frame: 0.302478000 seconds] [Time delta from previous displayed frame: 0.302478000 seconds] [Time since reference or first frame: 0.645838000 seconds] Frame Number: 5 Frame Length: 84 bytes (672 bits) Capture Length: 84 bytes (672 bits) [Frame is marked: False] [Frame is ignored: False] Point-to-Point Direction: Sent (0) [Protocols in Frame: ethertype:(ip:udp:dns)] [Coloring Rule Name: UDP] [Coloring Rule String: udp]							0000 3c 1e 04 12 86 d8 a4 03 e7 c1 b0 bd 00 00 00 00 0010 00 40 ec 14 00 00 40 11 0c 05 c0 a0 00 64 c0 a0 0020 00 02 f6 ae 00 00 32 bc ae 61 9f 01 00 00 01 0030 00 00 00 00 00 00 31 2d 03 6f 75 2f 69 05 72 0040 04 70 75 61 05 61 70 70 6c 05 03 61 6f 6d 00 0050 00 41 00 00
---	--	--	--	--	--	--	---

Ethernet II, Src: Apple_e1:b0:bd (a4:83:e7:e1:b0:bd), Dst: D-LinkIn_12:86:d8 (3c:1e:04:12:86:d8) Destination: D-LinkIn_12:86:d8 (3c:1e:04:12:86:d8) Source: Apple_e1:b0:bd (a4:83:e7:e1:b0:bd) Type: IPv4 (0x0000) Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.2 Type: IPv4 (0x0000) Version: 4 Header Length: 20 bytes (5)	0000 3c 1e 04 12 86 d8 a4 03 e7 c1 b0 bd 00 00 00 00 0010 00 40 ec 14 00 00 40 11 0c 05 c0 a0 00 64 c0 a0 0020 00 02 f6 ae 00 00 32 bc ae 61 9f 01 00 00 01 0030 00 00 00 00 00 00 31 2d 03 6f 75 2f 69 05 72 0040 04 70 75 61 05 61 70 70 6c 05 03 61 6f 6d 00 0050 00 41 00 00
--	---

Fig. 3. Packet 5, query to the DNS for https connection to 1-courier.push.apple.com.

Fig. 3 shows packet 5, which is a DNS query, requesting an HTTPS connection to “1-courier.push.apple.com”.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=62624, seq=96/24576, ttl=64 (reply in 2)
2	0.030100	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=62624, seq=96/24576, ttl=255 (request in 1)
3	0.836262	192.168.0.115	192.168.0.255	NNNS	92	Name query NS WPAD=000
4	0.343125	192.168.0.111	224.0.0.251	NDNS	227	Standard query response 0x0000 TXT, cache flush NSDC, cache flush Madau's MacBook Air_companion-link_tcp.local
5	0.645683	192.168.0.100	192.168.0.2	DNS	84	Standard query 0x019f HTTPS 1-courier.push.apple.com
6	0.645839	192.168.0.100	192.168.0.2	DNS	89	Standard query 0x0807 HTTPS stocks-data-service.apple.com
7	0.646070	192.168.0.100	192.168.0.2	DNS	89	Standard query 0x04e7 A stocks-data-service.apple.com
8	0.646402	192.168.0.2	192.168.0.100	ICMP	112	Destination unreachable (port unreachable)
9	0.646464	192.168.0.2	192.168.0.100	ICMP	117	Destination unreachable (port unreachable)
10	0.646504	192.168.0.2	192.168.0.100	ICMP	117	Destination unreachable (port unreachable)
11	0.800335	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=62624, seq=97/24832, ttl=64 (reply in 12)
12	0.812327	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=62624, seq=97/24832, ttl=255 (request in 11)
13	1.472636	D-Linkin 12:86:c8	Apple_e1b0:bd	ARP	42	192.168.0.2 is at 3c:1e:84:12:86:c8
14	1.095340	192.168.0.100	192.168.0.2	DNS	90	Standard query 0x04dc HTTPS self.events.data.microsoft.com
15	1.085665	192.168.0.100	192.168.0.2	DNS	90	Standard query 0x02b7 A self.events.data.microsoft.com
16	1.085944	192.168.0.100	192.168.0.2	DNS	88	Standard query 0x0b1c AAAA eds-ms-northwest-nl
17	0.650291	192.168.0.2	192.168.0.100	ICMP	112	Destination unreachable (port unreachable)
18	1.670441	192.168.0.100	192.168.0.2	DNS	97	Standard query 0x0e2d HTTPS officeci-mauservice.azurewebsites.net
19	1.670795	192.168.0.100	192.168.0.2	DNS	97	Standard query 0x0c91 A officeci-mauservice.azurewebsites.net
20	1.001848	192.168.0.100	192.168.0.2	ICMP	98	Echo (ping) request id=62624, seq=98/25088, ttl=64 (reply in 21)
21	2.018040	192.168.0.2	192.168.0.100	ICMP	98	Echo (ping) reply id=62624, seq=98/25088, ttl=255 (request in 20)
22	2.597289	192.168.0.110	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1002.1.3.1.13.0 1.3.6.1.4.1.1002.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1002.1.1.1.0 1.3.6.1.4.1.1002.1.3.1.12.0
23	2.599112	192.168.0.110	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1002.1.3.1.13.0 1.3.6.1.4.1.1002.1.2.1.8.1.3.1.1 1.3.6.1.4.1.1002.1.1.1.0 1.3.6.1.4.1.1002.1.3.1.12.0
24	2.698712	IntelCor_e2:08:a7	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.101
25	2.745497	192.168.0.100	192.168.0.2	DNS	89	Standard query 0x0807 HTTPS stocks-data-service.apple.com
26	2.745662	192.168.0.100	192.168.0.2	DNS	89	Standard query 0x04e7 A stocks-data-service.apple.com

Length: 56	
Checksum: 0x1810 [unverified]	
Checksum Status: Unverified	
[Stream index: 5]	
UDP payload (48 bytes)	
[Timestamps]	
Domain Name System (query)	
Transaction ID: 0x04dc	
Flags: 0x0180 Standard query	
0... .. = Response: Message is a query	
0000 0... .. = Opcode: Standard query (0)	
.... 0... .. = Truncated: Message is not truncated	
.... 1... .. = Recursion desired: Do query recursively	
.... 0... .. = Z: reserved (0)	
.... 0... .. = Non-authenticated data: Unacceptable	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
Queries	
self.events.data.microsoft.com: type HTTPS, class IN	
Name: self.events.data.microsoft.com	
Name Length: 30	
[Label Count: 5]	
Type: HTTPS (HTTPS Specific Service Endpoints) (65)	
Class: IN (0x0001)	

0000	3c 1e 04 12 86 c8 a4 83 e7 e1 00 bd 00 00 45 00	<-----E
0010	00 4c a2 ef 00 00 40 11 56 7b c8 a0 00 64 c0 a0	...-E V(.d
0020	00 02 f5 19 00 35 00 38 18 18 66 6c 02 00 00 81	...S-----
0030	00 00 00 00 00 00 34 73 65 6c 66 06 65 76 65 64	-----+elfeven
0040	0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----+elfeven
0050	74 65 63 6f 64 03 00 41 00 01	-----+com>A>

Fig. 4. Packet 14, query to the DNS for https connection to self.events.data.microsoft.com.

In Fig. 4, a packet can be seen that is a DNS query requesting an HTTPS connection to “self.events.data.microsoft.com”

- What are the characteristics of the attack (aka fingerprint)? Remember: the fingerprint are the characteristics that most repeats targeting a single destination IP. Traffic FROM the victim to the IP addresses in the network trace are NOT part of the attack. Tip: isolate 1 source and 1 destination IP and see if the same pattern applies to the other source IP addresses.

The attack’s fingerprint can be marked by several characteristics. Firstly, all the source addresses that are coming from the same Network ID, 192.168.0, indicate that it is a coordinated attack from people from the same network. Secondly, traffic to the IP address all uses the Transmission Control Protocol (TCP) as its main communication protocol. Lastly, the attack only targets the destination port 80.

- How a Wireshark filter of the attack looks like?

In order to filter for the attack, a filter needs to be made for SYN packets without an acknowledgement. This means that the the filter needs to look for packets that do contain a SYN, but that do not contain an acknowledgement:

tcp.flags.syn == 1 and tcp.flags.ack == 0

- What is the target (destination) IP of the attack?

The target IP of the attack is 192.168.0.100.

7. How many records are part of the attack?

When we filter for the attack in specific, we can see that a total of 308074 packets have been sent in the attack (see Fig.5).

Wireshark · Protocol Hierarchy Statistics · attack.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
▼ Frame	100.0	308074	100.0	21977340	2252 k 0	0	0	0	308074
▼ Ethernet	100.0	308074	23.0	5056044	518 k 0	0	0	0	308074
▼ Internet Protocol Version 4	100.0	308074	28.0	6161480	631 k 0	0	0	0	308074
▼ Transmission Control Protocol	100.0	308061	49.0	10758168	1102 k 307972	10754996	1102 k	308061	
VSS Monitoring Ethernet trailer	0.0	89	0.0	712	72 89	712	72	89	
Internet Control Message Protocol	0.0	13	0.0	936	95 13	936	95	13	

Display filter: tcp.flags.syn == 1 and tcp.flags.ack == 0

Fig. 5, The Protocol Hierarchy with the aforementioned filter shows that 308074 packets were sent in the attack.

8. How many unique (source) IP addresses performed the attack?

Wireshark · Source and Destination Addresses · attack.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Source IPv4 Addresses	308074				3.9473	100%	79.3500	84.029
192.168.0.117	42845				0.5490	13.91%	24.2000	80.986
192.168.0.104	31431				0.4027	10.20%	21.4800	84.037
192.168.0.107	30389				0.3894	9.86%	17.2500	77.947
192.168.0.108	29190				0.3740	9.47%	26.5300	84.029
192.168.0.110	27744				0.3555	9.01%	14.7300	62.034
192.168.0.116	27109				0.3473	8.80%	26.5600	87.104
192.168.0.112	24783				0.3175	8.04%	21.6500	87.103
192.168.0.106	18883				0.2419	6.13%	20.4300	89.468
192.168.0.109	15058				0.1929	4.89%	7.0000	47.674
192.168.0.111	14635				0.1875	4.75%	6.6100	87.104
192.168.0.102	14072				0.1803	4.57%	7.4300	13.017
192.168.0.114	13866				0.1777	4.50%	11.9800	58.995
192.168.0.115	8057				0.1032	2.62%	8.8400	58.993
192.168.0.101	5857				0.0750	1.90%	6.1700	13.557
192.168.0.105	4114				0.0527	1.34%	6.1900	78.213
192.168.0.100	28				0.0004	0.01%	0.0100	45.287
192.168.0.2	13				0.0002	0.00%	0.0100	45.331
▼ Destination IPv4 Addresses	308074				3.9473	100%	79.3500	84.029
192.168.0.100	308046				3.9469	99.99%	79.3500	84.029
5.79.104.167	28				0.0004	0.01%	0.0100	45.287

Display filter: tcp.flags.syn == 1 and tcp.flags.ack == 0

Fig. 6. IPv4 Source and Destination Addresses of the attack.

Looking at the IPv4 statistics from the source and destination addresses and filtering on the attack (see Fig. 6), it can be seen that a total of 17 unique IP addresses performed the attack.

9. Which top 3 source IP addresses sent more packets in the attack?

The top 3 source IP addresses that sent the most packets in the attack are:

192.168.0.117

192.168.0.104

192.168.0.107

10. What is the distribution of vendors related to the source IP addresses involved in the attack? Tip: use MAC address to Vendor. Ask Google or ChatGPT

14:4f:8a:dc:a0:87 = Intel

64:6e:e0:cf:6b:c4 = Intel

a4:83:e7:26:69:86 = Apple

d4:57:63:d3:6b:02 = Apple

10:6f:d9:2f:32:a9 = Cloud network technology singapore

14:85:7f:e2:e8:a7 = Intel

14:85:7f:e3:99:14 = Intel

14:85:7f:e3:99:41 = Intel

34:cf:f6:f9:a3:12 = Intel

3c:1e:04:12:86:d8 = D-Link international

3c:22:fb:62:ad:66 = Apple

80:65:7c:d5:2a:2b = Apple

8a:04:32:9a:ed:63 = Not Found -This device has a Locally Administered Address, instead of a Globally Unique Address like the other devices. This is likely why the vendor of the address cannot be found.

94:e2:3c:87:a3:6b = Intel

a4:34:d9:4e:0b:88 = Intel

a4:83:e7:e1:b0:bd = Apple

b0:a4:60:f4:14:60 = Intel

There are 9 MAC addresses linked to Intel devices, 5 to Apple devices, 1 to D-Link international, 1 to Cloud Network Technology Singapore and 1 not found.

11. What is/are the source and destination port(s) involved in the attack?

The attack is targeted at destination port 80, the source ports involved in the attack have a very large range of ports.

12. Why there are many packets from the victim to the attackers?

There are many packets from the victim to the attackers, because those consist of the second step of the TCP handshake, where the victim sends SYN/ACK packets after receiving SYN packets.

13. How this attack could have been more successful?

Several strategies could have been implemented to make the attack more successful. Firstly, increasing the amount of packets. Secondly, increasing the amount of devices participating in the attack could have boosted the attack's impact. Moreover, increasing the length of the attack could have increased its chances of success.

14. How much was the data rate peak of the attack [Mbits/second]?

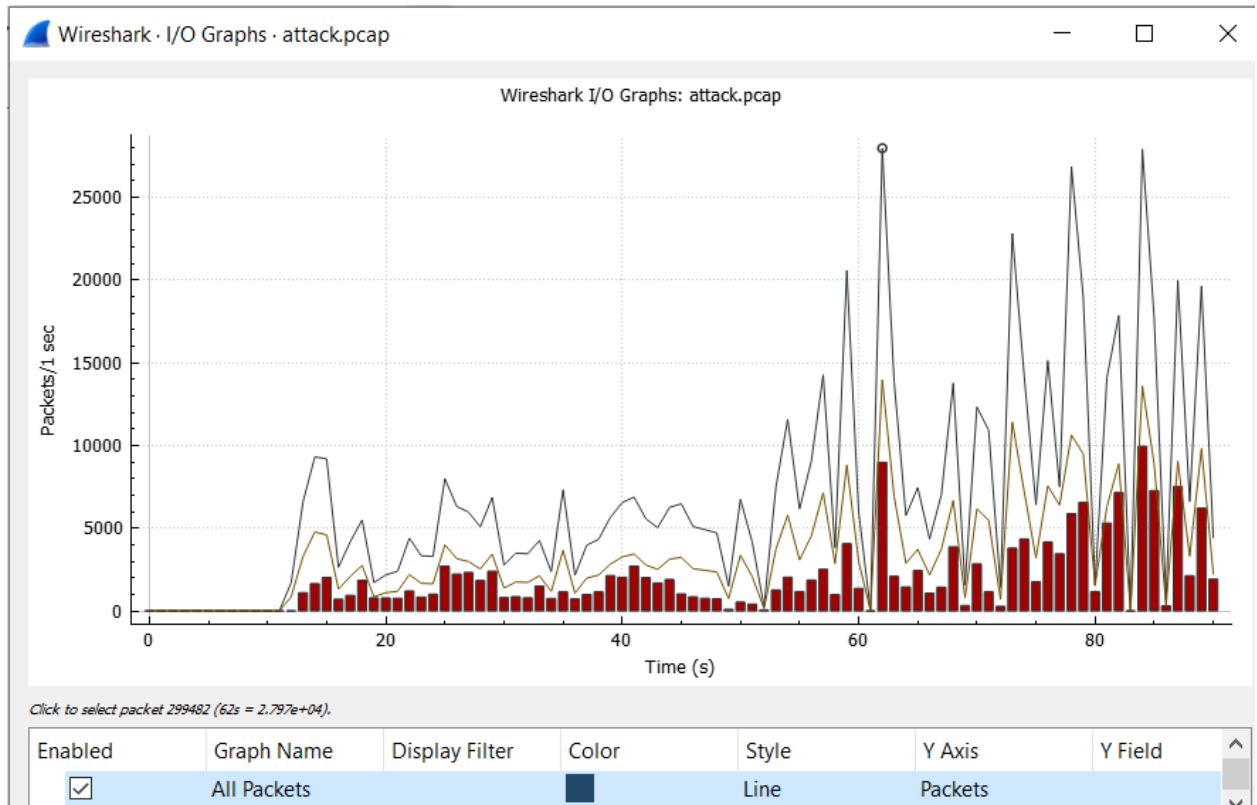


Fig. 7. An overview of the amount of packets that were sent per second.

At the 62nd second, 7.8 Mbits/s was the highest amount of Mbits/s during this attack (see Fig. 7).

15. What is the distribution/frequency of TCP flags involved in the attack?

The total number of TCP packets was 619,412 packets.

`tcp.flags.ack == 1` results in 311,351 packets.

The filter `tcp.flags.syn == 1` results in 308,061 packets.

$311,351 + 308,061 = 619,412$ packets, so these flags combined result in all of the packets.

Therefore, the distribution of TCP flags in the attack was:

`tcp.flags.ack == 1` : 50.3%

`tcp.flags.syn == 1` : 49.7%

16. What is the distribution/frequency of packet length ("total length")?

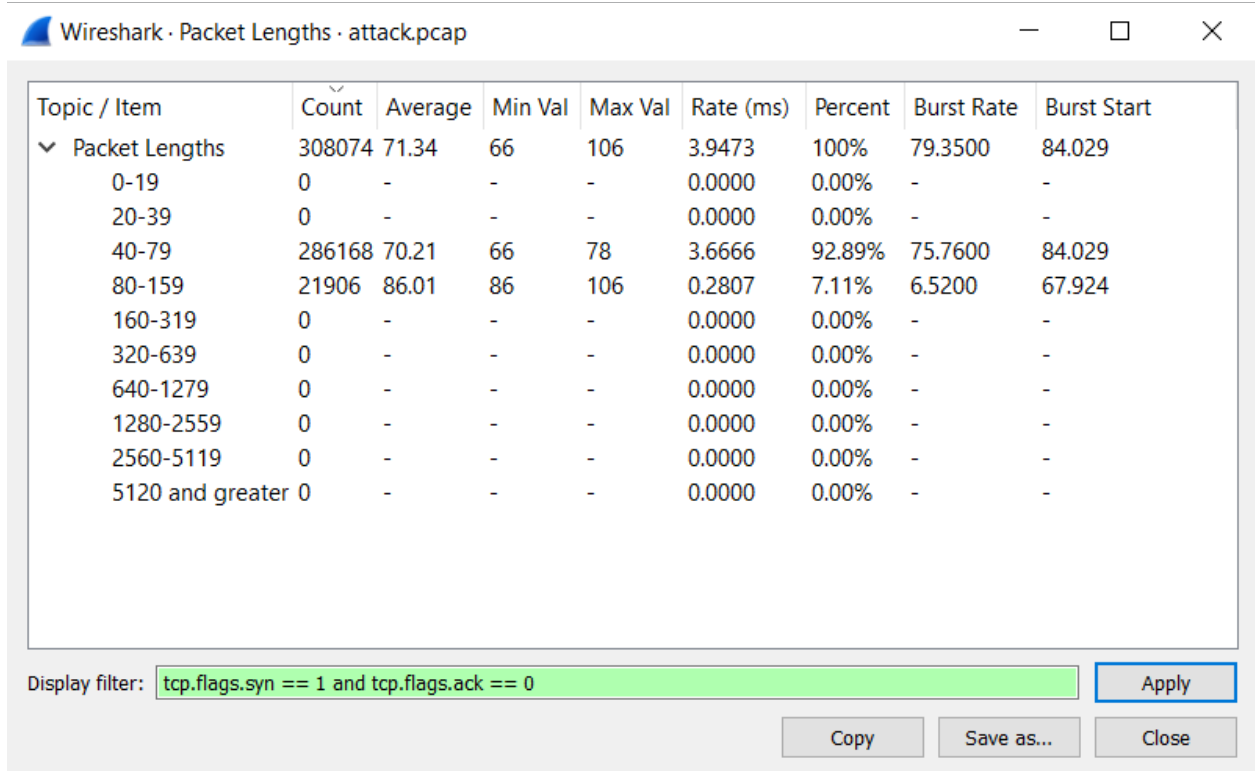


Fig. 8. Statistics of Packet Lengths in Wireshark.

Looking at the statistics of the packet lengths and filtering on the attack (see Fig. 8), it can be seen that the majority of the packets have a length between 40-79, the remaining packets have a length between 80-159.

17. What source IP address sent more packets? and why?

The IP address that sent the most packets is 192.168.0.100, this is the local router against which the attack was performed. It makes sense that a large quantity of packets were sent from here, because the router had to send SYN/ACK packets after all of the received SYN packets.

Conclusion & Reflection

The goal of this experiment was to gain an understanding of how DDoS attacks are performed, how to identify specific kinds of DDoS attacks, how to analyse them and how to know which information about the perpetrator of the attack can be found during an analysis. This goal was tried to be achieved by performing a DDoS attack and analysing the capture of this attack.

In conclusion, the research into the simulated DDoS attack gave insight into how to identify, analyse and find helpful information about these kinds of attacks. With the use of

Wireshark attack characteristics, source and target IP address, top attackers and MAC addresses could be identified.

This assignment showed how easily a DDoS attack can be performed, a group of people can set up an attack by using easily available tools. Therefore, this indicates the importance of cybersecurity measures to combat these attacks.

Because only a singular type of DDoS attack was analysed, most understanding was gained for this type of attack. Doing an experiment that also included other types of attacks could have ensured an understanding of multiple types of attacks and therefore also a greater understanding of DDoS attacks in general.

Furthermore, the way this attack was performed, using a relatively small amount of laptops on one network differs from how most real DDoS attacks are performed. Analysing and finding information about a real world DDoS attack that for example made use of a botnet, might still prove difficult, even with the knowledge gained during this experiment. Additionally, IP-addresses were relatively easy to find during this attack considering no attempts to conceal IP-addresses were made. Analysing this attack did not supply a basis with which an attack that uses a VPN or IP-spoofing could be analysed. Moreover, a lot of DDoS attacks are instigated with the use of a booter service. During this experiment, no further understanding about this phenomenon was gained.

Still, considering the size and timeframe of this experiment and the fact that it served as more of an introduction to DDoS attacks, it might be for the better that all points in the above mentioned paragraph were not added. Adding these other factors might have made the level of experience and understanding needed for this experiment too high and would also mean that the analysis or other ways of acquiring knowledge would take a significantly longer time, which would not be realistic.

References

Azure Network Security Team. (2023, February 21). *2022 in review: DDoS attack trends and insights*. Microsoft. Retrieved October 18, 2023, from <https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/>

Jackson, A. (2023, August 27). *Zayo Group: 200% Surge in DDoS Attacks*. Cyber Magazine. Retrieved October 18, 2023, from <https://cybermagazine.com/cyber-security/zayo-group-confirms-ddos-attacks-in-2023-are-up-200>