**LAB NO: 3** **Date:**

# HPING TOOL

**Objectives:**

In this lab, student will be able to:

- Identify to analyze the TCP/IP protocol.
- Generate packets for auditing and testing of firewalls and networks.
- Exploit the Idle Scan scanning techniques.
- Identify the commands to find and fix problems in their networks

**Description**:
It is a 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.

Hping works a bit like a standard ping command. Use that command, and you will:

- Transmit. You will send an Internet Control Message Protocol (ICMP) echo request.
- Wait. The target for your ping should return your message.
- Analyze. You'll get a great deal of data, including information about how many bytes were sent, how many arrived, and how long the trip took.
- Repeat. You'll go through this process a few times, just to ensure the connection remains consistent.

Hping3 becomes even more powerful when you start exploring its advanced options. You can use it for tasks like:

- Firewall Testing: hping3 can be used to test the resilience of your firewall rules by sending packets with various TCP flags and options.
- Tracerouting: You can use hping3 to trace the path taken by packets to reach their destination.
- Traffic Generation: It can generate network traffic patterns to simulate different types of attacks or load on a network.
- Packet Crafting: Craft custom packets to test how your network devices and applications handle them.
- Fingerprinting: Identify the operating system or device type of a remote host by analyzing its response to crafted packets.

## I. SOLVED EXERCISE:

1) Install Hping tool

Instructions to download hping.
Version 2: go to http://www.hping.org/download.html and download the tar.gz
Version 3 tar.gz: http://www.hping.org/hping3-20051105.tar.gz
Version 3: is inside the CVS repository. Use the following commands:
$ cvs -d :pserver:anonymous@cvs.sourceforge.net:/cvsroot/hping2 login
cvs will ask for the password, just press enter, no password is required. Then type this to download the full source code:
$ cvs -z8 -d :pserver:anonymous@cvs.sourceforge.net:/cvsroot/hping2 checkout hping3s

$ cvs update

2)The identify the IPv4 address using the DNS system using the hostname
hping resolve hostname
The resolve subcommand translate an host name in its IPv4 address using the DNS system. It is basically a gethostname() wrapper, that just returns its input if <hostname> is already an IP address.
Example:
hping3.0.0-alpha> hping resolve www.hping.org
192.70.106.166

## LAB EXERCISES

1. Identify the command to send an ICMP echo request packet to particular IP address.
2. Execute the command to capture packets from the specified interface
3. Do a port scanner: By specifying the TCP flags and port numbers
4. Perform the following attacks using Hping tool
    a. A spoofed scan of the server by the attacker
    b. UDP flood attack
    c. ICMP flood attack
    d. Random Source Attack
    e. SYN flood attack (DDOS attack) on a specified IP address.
5. Identify the command to do the following task
        a. Change TTL of packet
        b. Limit Packet count
        c. Set Packet Flag (SIN,FIN,PUSH,RESET,ACKNOWLEDGE,URG)