ICMP Help

This utlity will send an ICMP echo attack on the IP you specify.
First, you should be aware that ICMP bombs are illegal. No, I'm not saying you will get arrested for icmping somebody off IRC, but most internet providers will discontinue your service if they find out that you're doing it. Additionally, if you have access to T1 or T3 ethernet from a college and think it would be real cool to ICMP from there, I'd urge you to consider the consequences... I'm pretty sure any school would consider an ICMP bomb misuse of computing facilities and, if it got reported, would most likely result in the suspension of your accounts.
With that said...

What is ICMP?

You hear about "icmping" a lot on IRC, yet very few people (including those who use it) really know what it is. This section is for people who want to know a little more about it. It's a bit technical, but don't worry if you don't understand it... you don't have to know how it works to use it. If any of this is not exactly right... sorry, I'm not a programmer, this is just a hobby :P

First, a little about PING...
PING (Packet Internet Groper) is not a protocol, but a simple utility that allows you to test the accessibility of a certain site, as well as to verify the access time of the site. Ping sends out packets of information that go to the system you are pinging and waits for the remote system to return those packets to your system. (Do not confuse this with the PING you see on IRC; they both tell you the time it takes to reach a site, but the kind of PING you do on IRC is an overly simplified approximation of the time it takes for a message to get from you, through the IRC server network, to someone else, and back and tells nothing about efficiency or accuracy of data transfer).

Using the ECHO protocol (RFC 862), Ping can tell you if a connection is possible, how fast the information can be transferred between sites, and the accuracy of the transfer of the data. The ECHO protocol itself is very simple and is based on the master/slave model. In this model, when a query is sent from the master, the slave simply provides a response. With ECHO, the slave simply returns the data that was issued by the originating master.

ECHO has two possible modes of operation: TCP, Transfer Control Protocol, and UDP, User Datagram Protocol (with TCP, you can create and maintain a connection to a remote computer. Using the connection, both computers can stream data between themselves, whereas UDP is a connectionless protocol. Unlike TCP operations, UDP does not establish a connection... packets are sent back and forth). A TCP-based echo service is connection oriented via TCP at service port 7. Once a connection is established, any data received is sent back. The echo operation continues until the master terminates the connection. A UDP-based echo service is a datagram-based UDP operation. A slave listens for UDP datagrams on UDP service port 7 and returns the master's original message to the master; however, there is no connection being maintained.

ICMP, which stands for Internet Control Message Protocol (RFC 792), is a datagram protocol layered above IP and is the error and control message protocol used by the TCP/IP family of protocols. It is used by the kernel to handle and report errors in protocol processing and may also be accessed by programs using the socket interface for the Transport Level Interface (TLI) for network monitoring and diagnostic functions. Some useful purposes include routing, fault isolation, and congestion control.

For user applications, ICMP messages are sent by means of the standard IP packet, with specially

formatted data segments contained within the data portion of the packet. There are two primary packet formats: echo (request/reply) and redirect. An application such as this one uses the echo method with the UDP-based PING described above.

Ok, now in English...
What this program will do is send PINGs to the remote IP. It sends them over and over, waiting only 1 millisecond for a reply before giving up and sending the next one. The remote site will not be able to receive the echo request and reply in that 1 millisecond timeframe. The idea is to keep the remote site so busy returning PING replies that their internet connection becomes severly lagged. When you are connected to an IRC server, the server is constantly sending you "PONGs" and it expects a reply. If you do not reply within a certain amount of time, it assumes the connection is lost and disconnects you with the old "ping timeout" message. The goal of an ICMP bomb (as far as IRC is concerned) is to make someone lagged to this point.

A common misconception is that an ICMP bomb will make you lose connection to your internet provider. An internet provider also sends pings and expects a reply and will drop the connection if a reply is not received in a timely manner; however, usually long before that happens the IRC server pings the person and he/she realizes the internet connection is lagged and will reconnect.

Will it work for me?

Of course, the question is how effective will it be. You cannot expect to do much damage to a connection that is much faster than your own. From a 33.6 modem, you should be able to ICMP someone who is also on a 33.6 modem, but it may take several minutes. Also, because the IRC server gives people time to respond to the PONGs, you may not see them "ping out" for several minutes.

From a modem, do not expect to do much damage to even a medium speed connection, such as ISDN. Also, you will not even put a dent in the lag of a high speed (such as T1, T3, or DS3) connection. For those of you who don't know what all that means, I'll try to put it in perspective this way:

Connection	Speed
33.6 modem	33,600 bps
128k ISDN	128,000 bps
T1	1,500,000 bps
T3	45,000,000 bps
DS3	300,000,000 bps

Obviously, a modem stands no chance against a T1, let alone a DS3. However, from a T1 or higher, you can expect to ICMP a modem connection rather quickly. But, before you go using your ethernet connection at college for this, remember what I said in the beginning... if it gets reported, there is a good chance you will lose your school computer accounts (at the very minimal, you'll have to explain your actions to somebody important).

Ok, so how do you know what kind of connection someone else has? You can usually tell by the host.domain address. Check the persons address. If it appears as an IP (i.e. 127.0.0.1), type /dns <nick> to resolve it.

Domains such as "gym.gymnet.com", "krypton.cs.rit.edu", "client1.frontiernet.net", or "mozart.micro-net.net" are obviously not dialup because they contain no node information. In fact, those are actual address of some of my own accounts (ISDN, triple T3, dual DS3, and T3 connections, respectively).

An address such as ppp-07.har-ct.dialup.lame.net would most likely be a dialup connection and chances are the person is on a modem. Dialup ppp's always have some dynamic element that gives them away, such as the ppp-07 in the example above. This is not guaranteed, but it is a pretty safe bet.

Here are some things you can do to make your ICMP attack more effective:
- have some friends help you by icmping also
- while icmping, limit your internet activity to your IRC connection and the ICMP (i.e. do not use FTP or DCC Send while trying to ICMP)

How do I use this program?

To use this program, simply enter (or paste) an IP into the IP box and click "start". The program will minimize and start ping.exe, an MS-DOS based program that comes with Windows.

To get someone's IP, enter the nick into the "nick" box in the ICMP bomber and click **lookup**. The program will instruct Little Star to verify that the nick is on IRC, check to see if the person's address is already in IP format, and if it is not, it will attempt to resolve the IP. Little Star will report back with the status of the conversion (this all usually happens very quickly) and, if it was successful, the only thing left to do is click **Start**.

Note that the "nick" box is actually a drop-down list that already contains the nicks of anyone you currently have a query window open to and anyone in DCC chat. Also, you can get an IP from Little Star by typing /dns <nick> or using the "DNS" item in the "Whois?" part of the query and channel names list popups.

To stop the ICMP, click the X in the upper right hand corner of the MS-DOS ping window.

How do I know if it's working?

This part also messes people up...
If the ICMP is functioning, you will see "Request timed out" in the MS-DOS ping window. This is because the echo request is timing out after 1 millisecond, which is expected (as explained in the "Ok, now in English" section of "What is ICMP?" above).

You may see an occassional "No resources", which means your internet connection cannot handle the outgoing echo requests. Seeing a few of these is ok. However, if you are seeing more than a few, you will most likely not be effective. Make sure you have no DCC, FTP, or HTTP transfers going at the same time.

Just because the ICMP is functioning does not mean its working. After a few minutes of the ICMP bomb, trying pinging the person on IRC. Their ping reply time should be getting increasingly worse. If it is not, you are not doing any damage, so you might as well just give up (or seek assistance from friends).

7/22/97, updated 9/19/97

Help file generated by VB HelpWriter.