ICMP Detector Help

This program is used to automatically detect ICMP attacks, resolve the addresses, and report any matching nicks of that address. It does not require any special version of winsock.

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 designed "ICMP" you off IRC uses the echo method with the UDP-based PING described above.

Ok, now in English...
This is not what ICMP is for, but here's what the lamers on IRC who have no life and nothing better to do than disconnect people from IRC servers do:

They run a program that sends PINGs to the remote IP. It sends them over and over, not giving the remote site a chance to 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 timeframe, which is usually 1 millisecond. The idea is to keep the remote site so busy returning PING replies that his or her 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.

What does this program do?

This program is more than just a connection monitor. It scans all the connections you have and determines which ones appear to be an ICMP. It is not foolproof; it may report an ICMP that is actually some other legitimate connection, but it does work fairly well most of the time.

The echoing you see in Little Star may be more accurate than the list box in the program itself, as Little Star knows who is in DCC Chat/Send/Get/Fserve and the program does not. Also, the program may report an address, coming from your domain but not your exact address, as an ICMP. Little Star will not echo with one of these because it ignores ICMP detections from your own domain (that's the only way I know around this right now, other than to complicate things by making you enter the static IP of the address that is pinging you, which would be confusing for many peopple). The reason you get that is because your internet provider sends you pings to make sure you are still connected.

When an ICMP is detected, Little Star will try to find a nick who matches that address on any of the same channels as you. If it does not find one, it will attempt to resolve the IP and match the host.domain address. If multiple ICMPs are detected at once, they will be resolved and matched one at a time (i.e. it will not attempt to match the 2nd one until the 1st one is done).

The echo might appear something like this:

```
-ICMP Detector- ICMP detected from: 204.216.82.50
-ICMP Detector- matched 204.216.82.50 to nick: Ivan
```

How do I use this program?

1. Select to "Scan Once" or "Auto-Scan"
   Note that you cannot echo to Little Star if you only scan once.
2. If you select "Auto-Scan", select the delay time.
3. Click "Begin Scan". If you are auto-scanning, then End Scan button will be enabled.
4. If you're auto-scanning, you probably want to minimize the program.

That's it... the rest is automatic. If an ICMP is detected, you can select it in the list and click "Resolve" (or just double-click it in the list). It will resolve the IP to host.domain format and attempt to find a nick that matches on any of the same channels you are on.

If you enabled "Alert on new connection", Little Star will echo, as shown above, when an ICMP is detected.

A few things to note here...

1. This is a resource hog! (that's why the most frequent you scan is once every 60 seconds). No, it doesn't actually take the entire 5 seconds from the time you click "scan" until the time it is done, but I made it a 5 second delay to cover the 486 folks out there (otherwise it would start reading data before it was done compiling it). However, it is fairly accurate in detecting ICMPs and even some nuke attacks.

2. For reasons explained above, it will not detect ICMPs from your own domain (if that bothers you, use the "Connection Monitor" instead).
3. Due to the nature of how this program works, connections may still appear in the ICMP list for a short while after they are actually disconnected (detecting UDP connections is weird because there is actually no connection there... it's actually detecting little packets so there has to be some kind of delay there otherwise it would only detect it if it scanned the port the instant a packet was being received)
4. It only automatically finds matches of the person doing the ICMP is on one of the same channels as you.   To find any others, you can try /who *IP or /who *host.domain, but if they are +i like most people are that will not be of any use.

That's it!
It's not perfect yet, but I'll do more work with it if I can.

Help file generated by VB HelpWriter.