Han Official Protocol and Packet Analyzer

Introduction:

The hoppa portscanner was developed at the HAN in Arnhem in 1998 by a group of second year Information Technology Students. It was part of a project called Network Tools at request of the ICT department. The project consisted of a packet analyzer, a database and the portscanner. Both the portscanner and the packet analyzer should provide information to the database about equipment attached to the school's network like workstations, routers and bridges.

As the deadline of the project became closer and closer, it became clear that not all the features we wanted to include could be implemented. This user manual is about the portscanner, which is a fully functional portscanner, except for the fact it is not yet capable of putting information about ports and services in the database. This will be implemented in the near future, hopefully.

Hardware and Software:

Since scanning ports of a computer is a time consuming process, we have written the application in the way that you can define how many threats will be used to scan the ports. For every port you want to scan, a new thread will be created. Every thread is consuming memory and processor time. You have to try for yourself how many threads suites the best on the hardware you are working with. It is stated clear in the program that working not carefully with this option can lead to a system reset and data loss. On default, the program works with 400 threads, you can change that in any value between 100 and 700. Normally, you don't have to change this value because the portscanner works just fine with 400 threads. If you want to change the number of threads, the possibility is there. The program is tested under Windows 95,Windows 98 en Windows NT 40 and should work fine under these operating systems. Required memory depends on the selected number of threads, but 16 MB will do fine under Windows 95, 32 MB is recommended for Windows NT users.

Installation Procedure:

- Start the setup.exe installation program.
  An installation wizard will guide you through the installation procedure.
- You can choose the destination directory and optionally choose to install the source code of the portscanner.
- Do not forget to read the readme file shown during installation.
- By default the program will be installed on your C hard drive in the subdirectory C:\Hoppa.

The following files will be installed there:

- portscan.exe	the executable (*)
- ports.html	a list of well known and registered port numbers (*)
- rfc1700.txt	the RFC with well known and registered port numbers
- todo.txt	a list with 'todo' remarks (*)
- manual.doc	the manual (*)
- nocopyright.txt	a text file with copyright issues (*)
- services	a text file with port numbers uses by the portscanner
- hosts.hhf	example host file used by the portscanner
- unwise.exe	uninstall program
- install.log	log file used by unwise

Files marked with an '*' do have their own shortcut in the startup program group *hoppa*. If the user chooses to install the program sources then they will be installed in a subdirectory of the main directory of hoppa .A shortcut to the C++ Builder 1.0 project makefile will be added to the hoppa program group.
The *RFC1700* and the *ports.html* where added so you can modify the service file used by the portscanner by adding or deleting entrys, they contain most of the registred ports.

Uninstall:

To remove the installed program, click on the *remove program* icon, which can be found in the control panel.

Starting the application:

You can start the application by clicking on the shortcut, which can be found in the start menu.

OPTIONS:

SCANNING A SINGLE HOST:

Enter your hostname or IP-address in the *Single Host* input box. Before you start scanning, make sure you have selected Single IP by clicking on the checkbox. Press the *P*-button in the left corner of the screen to start scanning.

SCANNING A HOST RANGE:

Enter your hostnames or IP-addresses in the *Host Range* input box. Before you start scanning, make sure you have selected *Host Range* by clicking on the checkbox. Press the *P*-button in the left corner of the screen to start scanning.
If you use hostnames here, be sure that the resolved IP of the ending address is larger then the IP of the beginning IP.

SCANNING A HOSTS FILE:

Select the radio button next to *hosts file*. Extension used here is *hhf.* (hoppa hosts file). You can keep for example a list of both IP numbers and hosts names combined for every subnet.

Before using this option you have to select a hosts file to start with. There are three buttons on the application concerning the editing of the host file.

The second button : select host file
The third button : edit host file
The fourth button : new host file

On selecting *select hostfile* you get a normal *select filename window* to select an existing *.hhf file. When a file is selected the file will be shown on the application form next to the radio group option *hosts file*.

On selecting *edit hostfile* or *new hostfile,* a new window will pop up. If you choose the option *edit hostfile*, a file will be selected. The new windows gives the possibility to *edit, save* and *print* the *hosts file*.

SCANNING A PORTRANGE:

Select the radio button which is stated *port range*. You can enter here any range (or just one port) that has to be scanned. Be sure that the ending port is always a greater value than the beginning port. The ending port has a limit of 65535.

SCANNING THE SERVICE FILE:

Select the radio button which is stated *service file*. This file is a user editable file with port numbers, their official description and room for remarks. The layout of this file is the same as a UNIX or Windows NT service file. All UDP entries will be skipped and all the TCP entries will be used to scan a host. On how to edit this file, read further below.

STARTING TO SCAN:

After you have entered valid IP-numbers or a hostnames in the editboxes click with the mouse on the left button with a 'P' in it. (P stands for portscan and it will start the scanning).

The portscanner will now start to scan the host(s) depending on the choices the user has made. A new popup screen will appear for this job. You can cancel the job by pressing ctrl-c or clicking the cancel button. A new screen will appear to inform you to be patient because all started threads have to end. If the scan is finished the cancel button will change into an OK button. The other two buttons will also be enabled. A choice can be made to save the results to a file or to send them to a printer

EDIT THE SERVICE FILE:

The fifth button on the application is for editing the service file. This file has to be located in the same directory as the application. You can add TCP port numbers and descriptions here. You can edit, save and print the file here.

CHANGING NUMBER OF THREADS:

As already stated, changing this option must happen very carefully. Per default the application uses 400 threads to scan ports. You can change this in any value between 100 and 700.

PING A HOST BEFORE SCANNING:

You can reach this option by choosing *settings* from the application menu.
This option is set on default. It will prevent long time-outs when scanning a host that is not up or doesn’t exist. The host won't be scanned if it doesn't reply to the ping request.

In cases where ping will not get through like in the case a bridges is configured not to let ping request through,you can turn this option off.

COMMENTS,REMARKS & BUGREPORTS (known as eastereggs or special features):

hoppapro@dds.nl

for latest version or our other application or our network analyser & networkdatabase:

http://huizen.dds.nl/~hoppapro
www.surf.to/~hoppa