It's me (IM)

Current Version: **V1.9d**
Last Update: **Monday, 09-Jan-2006 10:27:02 CET**

DISCLAIMER

THIS SITE INCLUDING ALL CONTENT (TEXT, PICTURES, BINARIES ETC.) IS NOT ALLOWED TO BE USED IN CRIMINAL, ILLEGAL ACTIVITIES! THE PURPOSE OF THIS SITE IS TO DESCRIBE THE SOFTWARE "It's me (IM)" WHICH IS A PORT KNOCKING CLIENT. USE THIS SOFTWARE ONLY AGAINST HOSTS WHERE YOU ARE ALLOWED TO DO SO. I AM IN NO WAY RESPONSIBLE FOR ANY PROBLEMS OR DAMAGES YOU MAY ENCOUNTER BY USING CONTENT OF THIS SITE. YOU USE THIS SITE AND ALL OF ITS CONTENT AT YOUR OWN RISK! BY USING THIS SITE AND ITS CONTENT YOU HAVE ACCEPTED THIS DISCLAIMER.

- **Table of contents**

- **What's "It's me"?**
  IM is a Windows portknocking client. Portknocking is used to change Firewall rules via blocked Firewall ports. Portknocking is NOT a way to break or spy firewalls and NO, portknocking is NOT portscanning! You can read more about portknocking under

http://www.portknocking.org

IM does not need to be installed. Just place the binary and config file wherever you want it, for example on a USB stick and you are done. IM has the following features:

- Knock sequences up to 1024 knocks
- Up to 1024 variable user parameters
- Variable parameters for date/time/IP
- Checksum
- Blowfish encryption
- No installation necessary
- Creates a default config file if non exists
- Small footprint (about 20k) - ideal for removeable media like USB sticks or Floppies

---

- **Download**
  The current version is 1.9d ItsMe_V1.9d.zip

- **Configuration**
  IM looks for a config file in the current directory with the same name as the binary. If the IM binary is named im.exe then it looks for a configfile with named im.ini.

  The contents of such a config file might look like this:

```
[General]
Debug=2

[Default]

[myhost]
HOST=127.0.0.1
RANGE=50000-50255
CRYPT=1
PASSWORD=mypassword
KNOCK1=LIP1-1
KNOCK2=LIP1-2
KNOCK3=LIP1-3
KNOCK4=LIP1-4
KNOCK5=P-1
KNOCK6=42
KNOCK7=P-2
KNOCK7=CRC
```

  This configfile specifies a host profile called **myhost**. When starting you specify the host profile you want to knock as the last argument on the command line. If no host to knock is specified IM tries to knock a host specified in a profile called **Default**. In the **General** section the **RANGE**, **SLEEP**, **CRYPT**, **PASSWORD** and **DEBUG** parameters can be specified. They act as defaults for all other congiguration sections in a config file as long as there is no other **RANGE**, **CRYPT** or **PASSWORD** statement. An exception is the **DEBUG** parameter which is additive. This means that every occurance of a debug parameter adds the value to the debug level. The higher the debug level the more debug output is generated. For example: specifying -d -d on the command line, Debug=2 in the GENERAL section and DEBUG=3 in the myhost section gives a debug level of 7.

  The **HOST** parameter specifies the IP address of the target host. You can also use a DNS name here.

  RANGE specifies the allowed port range IM can use to knock. The format is RANGE=StartPort-EndPort. If there is no RANGE statement in a given host configuration then the program tries to find a RANGE statement in the **General**

section. If there is also none found then an error occures.

You can specify more than one range by using numbered RANGE statements but only the RANGE statement without a following number will be taken from the General section!. For example:

```
RANGE=20000-21000
RANGE1=1000-2000
RANGE2=1500-2500
```

If ranges overlap they are merged. This means that RANGE1 and RANGE2 in the previous example becomes RANGE1=1000-2500.

The bitlength of the sum of all ports specified by RANGE statements defines how knock values are mapped. See http://www.portknocking.org/view/details/knocklength or http://www.portknocking.org/view/documentation#Example to find out how this is done.

With the **CRYPT** paramater you specify the type of encryption that should be used for this knock sequence. For the moment the following encryptions are available more may come in the future:

- 0) No encryption
- 1) Blowfish encryption

A Password can be specified with the **PASSWORD** parameter. If the encryption specified with the **CRYPT** parameter does not use a passowrd this parameter is ignored.

SLEEP specifies the time in milliseconds to wait between knocks. The Default is 0.

KNOCK1 - **KNOCKn** specify the knock sequence. You specify the portnumber for a specific knock in this sequence of knocks. To knock port 237 as the 7 step in this sequence is written as KNOCK7=237. The knock sequence stops when there are no mor knocks in a sequence or when the sequence is brocken. For example:

```
...
KNOCK7=42
KNOCK8=130
KNOCK10=200
...
```

This sequence stops at knock 8.

Ports are automaticaly remaped to the port range selected with the **RANGE** parameter. By using RANGE=50000-50255 the above sequence becomes 50042, 500130, 50200. This remapping is done modulo range size!

You can use special port variables like P1 or IP1-1. The values of these special variables is used as the port value to knock. Below you will find a list of all special variables - more may come:

IP-n-q	Specifies part q of local hosts IP

	address n. For example: If the local host has two IP addresses (192.168.1.10 and 192.168.200.20) then IP-2-3 specifies the 3rd part of the 2nd IP address which is 200
CRC-n	Defines which CRC method to use and also specifies the position in the knock sequence to which the CRC should be created. For example: Specifying this parameter as KNOCK5 means create a CRC of type n for the knocks 1-4. Knocks after this are not included in the CRC. You can also specify more than 1 CRC in a knock sequence. Available CRC types: 0=simple CRC (sum of all knocks mod 255). More CRC types my come. If only CRC is found, CRC-0 is assumed for this knock value
DAY	Inserts the current day (01-31)
MON	Inserts the current month (01-12)
YEAR	Inserts the year (00-99)
HR	Inserts the current hour (00-23
MIN	Inserts the current minute (00-59)
SEC	Inserts the current second (00-59)
P-n	Inserts the nth command line argument -p. For example: With the command line argument *im.exe -p 42 -p 11 -p 0 myhost*, **P-2** results in the value 11
K-n	References knock number n for this knock. This works forward and backward.
RND	Inserts a random number within the boundaries of **RANGE** for this knock.

- **Usage**
  To start IM it is best to create batch files with all required parameters so that by

just simple clicking on the batch files the required actions will take place. For example:

To start SSH Port for 15 Minutes

```
@echo off
cls
im.exe -p 22 -p 15 MyHost
```

and to close the SSH port afterwards

```
@echo off
cls
im.exe -p 22 -p 0 MyHost
```

The following command line parameters are available:

im.exe [-h | -p | -n .....] ProfileName

-h, -?	Displays this help screen.
-v	Shows the program version.
-s	Silent mode - dont print out anything. (works only if not in debug mode)
-p value	Defines up to 1024 parameter values for usage within knock sequences. Value range 0-255.
-i	Ignore knocks refering to nonexisting -p parameters. If this parameter is used such knocks are treated as 0, if not used these knocks are removed from the knock sequence and a warning is printed.
-n host	Defines a default target host name which can be a name or IP address. If there is also a **HOST** entry found in the given profile then this parameter is ignored.
ProfileName	Specifies the section within the portknock.ini configuration file from where to read settings and the knock sequence.

The ProfileName must be the last parameter in the command line. Anything after the ProfileName will be ignored. -h, -? and -v only show help or version information and cancel the normal program execution thus they should not be

used in combination with the other parameters.

- **Limitations** / **Problems** / **Bugs** / **Comments**

There are the following limitations/problems/bugs in the current version of IM:

2004-07-28

First release of IM Version 1.0. Portranges must be continuous and must not be larger than 255 ports.

2004-09-23

Some people have reported that knocks are done three or more times. This results from the fact that Windows automaticaly retries a TCP/IP connection attempt if this attempt was unsuccessfully. This happens three times (the default). This behaviour can easily be changed via the Windows registry.

More information can be found in the Microsoft Knowledge Base article **Q175523**

You can download this registry file, change it with notepad (if necessary) and double click it to change these registry parameters.

2004-09-24

A new version (1.5) has been released. New fetures include unlimited, non continous portranges of any size and a new configuration paramater **SLEEP** which specifies the time in ms to wait between knocks (default is 0).

2005-05-06

A new version (1.6) has been released. This versions fixes some bugs with crypted knocks and some range mapping bugs.

2006-01-09

A new version (1.9d) has been released. This versions fixes some minor bugs and introduces two new command line parameters: **-n** and **-i**.

If you have any questions or suggestions to make IM better just drop me line at Richard Prinz / MIN.at

Last Updated: Monday, 09-Jan-2006 10:27:02 CET