

**F-RESPONSE VIA
NETWORK ADDRESS TRANSLATION
OR PORT REDIRECTION
JUNE 2008**



Table of Contents

Welcome to F-Response.....	3
Terminology.....	3
Target.....	3
Initiator.....	3
Summary	3
Scenario.....	4
Step by Step Process.....	5
Step1 – Start and configure F-Response Software.....	5
Step 2 – Configure Remote Firewall/Router	5
Step 3 – Perform the initial Discovery Phase.....	5
Step 4 – Open Microsoft iSCSI Command Line Interface.....	6
Step 5 – Login using iscsicli interface and external IP address.....	6
Step 6 – List Sessions (Optional)	7
Step 7 – Using F-Response	8
Step 8 – Logout using the iscsicli interface (Optional).....	9
Support	10
Appendix A – Legal Notices	11
Legal Notice	11
Trademarks.....	11
Statement of Rights	11
Disclaimer	11

Welcome to F-Response

Thank you for purchasing F-Response. You have now extended the capabilities of your existing arsenal of tools to enable them to work over an IP network. F-Response accomplishes this through the use of a Patent Pending process; a part of which includes leveraging the Internet Small Computer Systems Interface (iSCSI) protocol standard as defined in RFC 3720 (<http://www.ietf.org/rfc/rfc3720.txt>).

Terminology

The iSCSI terms “Target” and “Initiator” are used throughout this manual. The choice of “initiator” and “target” verbiage in the iSCSI definitions may prove confusing to forensics practitioners because “target” carries a different definition in the field of computer forensics versus iSCSI. In computer forensics, the system to be analyzed is generally referred to as the “subject” system, whereas the system to which forensically sound data is collected is generally referred to as the “target” system. In this manual, the forensic “subject” is an iSCSI “target”, i.e. F-Response Target code is executed on the machine to be analyzed. For this reason, we want to make clear that the use of the word “target” in this manual refers to the iSCSI definition, and not the forensics definition. The definitions for Target and Initiator used in this manual are as follows:

Target

F-Response Target code is to be executed on the machine(s) to be analyzed. All references to “target” in this manual refer to the machine(s) being analyzed using F-Response target code.

Initiator

An iSCSI “initiator” is used to establish network connections to machines running F-Response Target code. iSCSI initiator software must be installed on the machine from which analysis is to be conducted over the network. F-Response Target code has been tested with Microsoft iSCSI Initiator 2.0 software, included by default with newer Windows operating systems, and freely available for download from the Microsoft web site.

Summary

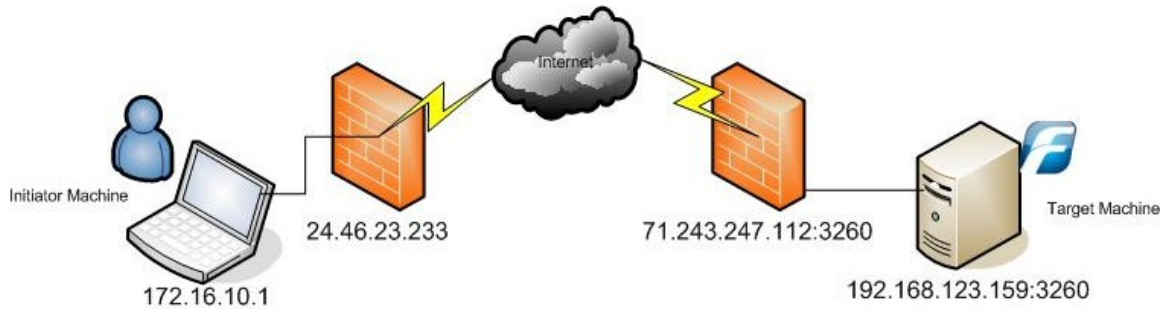
The iSCSI protocol contains certain limitations when communicating over a Network Address Translation or “NAT” device. In particular, the Discovery phase provides a local IP address for the remote target, which does not take into account the potential for address translation. However, there is a workaround available when using the Microsoft iSCSI Initiator command line that will allow for the creation of an iSCSI session over a NAT translation or Port Redirection router.

In the following example we will describe the process, identify the Microsoft iSCSI command line client options, and create a simple command line sequence for enabling the connection quickly and easily.

Important Note

While this workaround enables F-Response iSCSI traffic to traverse the Internet, this traffic will NOT be encrypted and should be considered potentially subject to monitoring or capture.

Scenario



External investigator or analyst has a laptop configured with the Microsoft iSCSI Initiator and multiple computer forensics analysis tools. This laptop is configured with a local non-routable address, 172.16.10.1. The remote computer has a copy of F-Response (any version) running; this remote computer will be the target of our analysis. The remote computer is located behind a port redirecting firewall, the firewall is assigned a fully routable address on its external interface, this address is 71.243.247.112. The firewall has been configured to redirect Internet traffic on port TCP port 3260 to the local Target computer, 192.168.123.159 TCP port 3260.

Step by Step Process

Step 1 – Start and configure F-Response Software

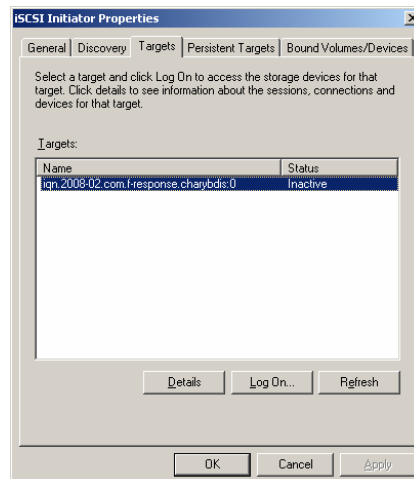
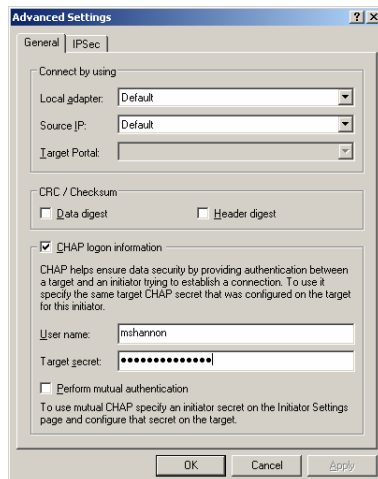
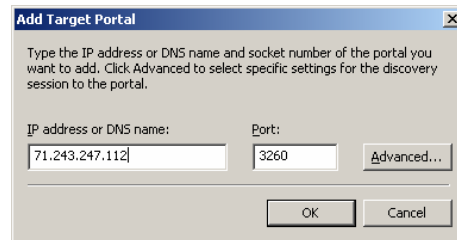
F-Response (Field Kit, Consultant, or Enterprise) should be running on the remote target computer. In this example that computer is 192.168.123.159.

Step 2 – Configure Remote Firewall/Router

The remote firewall (if existing) should be configured to allow inbound traffic on TCP port 3260 to be forwarded from the external firewall address 71.243.247.112 to the internal address 192.168.123.159.

Step 3 – Perform the initial Discovery Phase

The Initiator machine initiates a “Discovery” session using the external IP address assigned to the remote firewall, in this instance that address is 71.243.247.112.



Microsoft iSCSI Initiator Discovery Process

Following a completed Discovery session a Target will appear within the Targets tab of the Microsoft iSCSI Initiator, however this target is not actually valid, attempting to login to this Target using the Microsoft iSCSI Initiator GUI will NOT be successful. This happens due to a design decision related to the iSCSI protocol that requires the Target to return its configured IP address after a valid Discovery request. In this instance however the Target's configured IP address is an internal, non routable address (192.168.123.159).

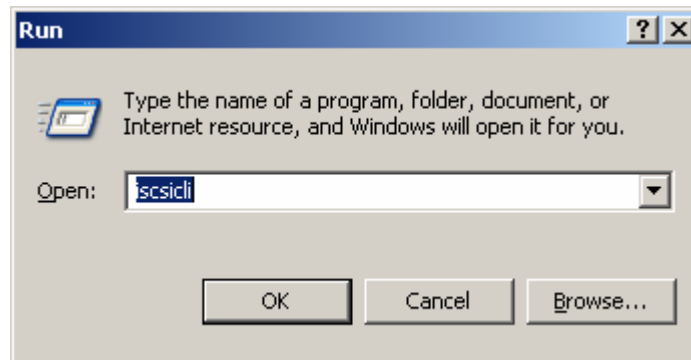
```
.0.?8x..|.h..E.  
..A*@.{.>G..p..  
....., ..*,=.P.  
.....Ta rgetName  
=iqn.200 8-02.com  
.f-respo nse.char  
ybdis:0. TargetAd  
dress=19 2.168.12  
3.159:32 60,1..
```

Selection of Network Traffic indicating Internal Non-routable IP Address

Therefore, in order to access the remote F-Response Target we must configure the proper IP address manually using the Microsoft iSCSI Initiator Command Line interface, `iscscli.exe`.

Step 4 – Open Microsoft iSCSI Command Line Interface.

Open the Microsoft iSCSI Command Line interface, Start-> Run-> `iscscli.exe`.



Start-> Run input box with `iscscli`

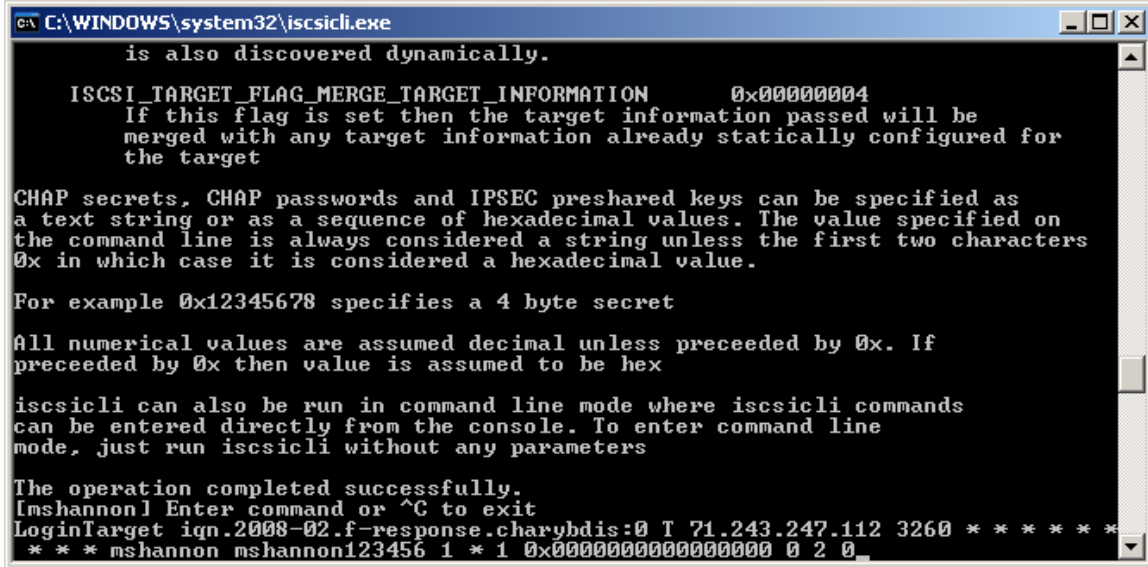
Step 5 – Login using `iscscli` interface and external IP address

Login to the Target via command line using the following syntax:

```
LoginTarget <TargetName> T <TargetExternalIP> <Port> * * * * * * * * * *  
<username> <password> 1 * 1 0x0000000000000000 0 2 0
```

In our example the command line would resemble the following:

```
LoginTarget iqn.2008-02.com.f-response.charybdis:0 T 71.243.247.112
3260 * * * * * mshannon mshannon123456 1 * 1 0x0000000000000000
0 2 0
```



```
is also discovered dynamically.

ISCSI_TARGET_FLAG_MERGE_TARGET_INFORMATION      0x00000004
If this flag is set then the target information passed will be
merged with any target information already statically configured for
the target

CHAP secrets, CHAP passwords and IPSEC preshared keys can be specified as
a text string or as a sequence of hexadecimal values. The value specified on
the command line is always considered a string unless the first two characters
0x in which case it is considered a hexadecimal value.

For example 0x12345678 specifies a 4 byte secret

All numerical values are assumed decimal unless preceeded by 0x. If
preceeded by 0x then value is assumed to be hex

iscscli can also be run in command line mode where iscscli commands
can be entered directly from the console. To enter command line
mode, just run iscscli without any parameters

The operation completed successfully.
[mshannon] Enter command or ^C to exit
LoginTarget iqn.2008-02.f-response.charybdis:0 T 71.243.247.112 3260 * * * * *
* * * mshannon mshannon123456 1 * 1 0x0000000000000000 0 2 0
```

Screen capture of the iscscli.exe LoginTarget syntax

Step 6 – List Sessions (Optional)

If the command completed successfully you should be returned to the iscscli.exe command line and be able to list the valid sessions using the command “SessionList”.

```
[mshannon] Enter command or ^C to exit
```

```
SessionList
```

```
Total of 1 sessions
```

```
Session Id           : ffffffff86592864-4000013700000009
Initiator Node Name  : mshannon
Target Node Name     : (null)
Target Name          : iqn.2008-02.com.f-response.charybdis:0
ISID                 : 40 00 01 37 00 00
TSID                 : 00 00
Number Connections   : 1
```

Connections:

```
Connection Id       : ffffffff86592864-8
Initiator Portal    : 0.0.0.0/1291
Target Portal       : 71.243.247.112/3260
CID                 : 01 00
```

Devices:

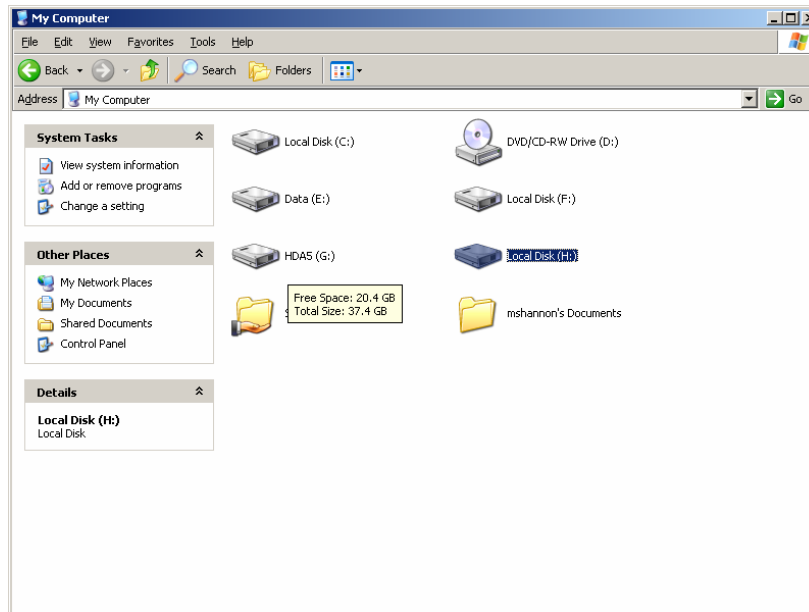
```
Device Type         : Disk
Device Number       : 2
Storage Device Type : 7
Partition Number    : 0
```

```

Device      Friendly Name      : FRES      CHARYBDIS      SCSI Disk
Device Description : Disk drive
Reported Mappings : Port 2, Bus 0, Target Id 2, LUN 0
Location        : Bus Number 0, Target Id 2, LUN 0
Initiator Name   : Root\SCSIADAPTER\0000_0
Target Name      : iqn.2008-02.com.f-response.charybdis:0
Device Interface Name :
\\?\scsi#disk&ven_fres____&prod_charybdis_____
_&rev_0____#1&2afd7d61&0&000200#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Legacy Device Name : \\.\PhysicalDrive2
Device Instance    : 0x830
Volume Path Names  :
                  G:\
                  F:\
                  H:\
    
```

Step 7 – Using F-Response

You may now begin using the drive normally, as you would any other F-Response drive. Refer to the appropriate F-Response manual for additional information.



Step 8 – Logout using the iscsicli interface (Optional)

When you are finished performing analysis you may disconnect the Target using either the standard GUI process, or using the command line. The command line syntax is as follows:

```
LogoutTarget <Session ID>
```

In our example the command line would resemble the following:

```
LogoutTarget ffffffff86592864-4000013700000009
```

The iscsicli responds with:

```
Logout Target 0xffffffff86592864-0x4000013700000009  
The operation completed successfully.
```

Support

We take pride in providing prompt attention to your support needs, and will support your F-Response product for the period of your license term. F-Response support can be reached via

Email: support@f-response.com

Website: www.f-response.com

Software and documentation updates will be made available for download to registered users on the F-Response web site. E-mail support is available to licensed software users. We typically respond to your queries within 1 business day of receiving your request.

Appendix A – Legal Notices

Legal Notice

Copyright © 2008 Agile Risk Management, LLC. All rights reserved.
This document is protected by copyright with all rights reserved.

Trademarks

F-Response is a trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.