

# INTERLAB

Tel: +331 3971 7337 – Fax: +331 3928 9008

## ISSUE: reverse ssh access over firewall to hosts

Concerned platforms:

OS : Linux

Vernouillet, 14.1.2010

### Issue:

Connect to a remote machine who is hidden behind NAT and or firewall.  
The idea is to build an SSH tunnel from the secured area to give access to your host machine to a user located on the other side.

### Requirements:

DSL access to internet connected, ssh service up and running.  
This supposes that you have a user name and password on the target server, and on the other side the support has your login informations.

### Security issue:

customer running ssh -R must receive a logging. This drills a security hole into Target server. Target administrator would create an account (adduser) and after the job, can delete the user (deluser) in both cases you need to be root.

Here is the procedure in command line

### 1. On the host in trouble machine:

2022 is a supposed free port, [support@www.interlab.fr](mailto:support@www.interlab.fr) is an example of target it can be an ip address. support is the target user name, Enter the password paired with user\_name

```
user@host_in_trouble:~$ ssh -R 2022:localhost:22 support@www.interlab.fr
```

```
support@www.interlab.fr's password:
```

```
Linux target_server 2.6.XX #1 SMP Fri Aug 31 00:24:01 UTC 2007 i686
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

# INTERLAB

Tel: +331 3971 7337 – Fax: +331 3928 9008

```
support@target_server:~$
```

**At this point on the service machine the link is build and will stay till this window stays open and the DSL link is on. Any interruption will cut the link.**

## 2. On the target server the service guy needs:

Connect to the build ssh link on port 2022 to the host\_in\_trouble.

```
support@target_server:/home$ ssh localhost -p 2022
```

```
The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be established.  
RSA key fingerprint is 7b:45:b9:d7:89:a7:2a:c1:3f:c3:2c:77:69:62:6d:99.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '[localhost]:2022' (RSA) to the list of known hosts.  
support@localhost's password:  
Linux host_in_trouble 2.6.xx generic #54-Ubuntu SMP Thu Dec 10 16:20:31 UTC 2009 i686
```

```
Last login: Fri Dec 4 15:20:58 2009  
user@host_in_trouble:~$
```

**Note that at this point the password expected is the host\_in\_touble one.** Mission accomplished you are in.

### Possible trouble:

host id identification failed... Then you will get a message like this:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!  
Someone could be eavesdropping on you right now (man-in-the-middle attack)!  
It is also possible that the RSA host key has just been changed.  
The fingerprint for the RSA key sent by the remote host is  
7b:54:b9:d7:89:a7:2a:c1:3f:c3:3a:66:c9:62:d5:92.  
Please contact your system administrator.  
Add correct host key in /home/support/.ssh/known_hosts to get rid of this message.  
Offending key in /home/support/.ssh/known_hosts:7
```

RSA host key for [localhost]:2022 has changed and you have requested strict checking.  
Host key verification failed.

Action: Edit in in the user account where you are **known\_hosts** located as in hidden directory in **/home/user/.ssh/** rem the concerned line (in this case line 7) by adding ahead of it "#". You can also rename the all known\_hosts to known\_hosts.temp and once work is over rename it back.

```
support@target_server:~$ cd /home/support/.ssh/  
support@target_server:~/ .ssh$ jed known_hosts
```

Once this is done get back to point 2. and run the SSH command:

```
support@target_server:/home$ ssh localhost -p 2022
```

# INTERLAB

**Tel: +331 3971 7337 – Fax: +331 3928 9008**

**ssh: connect to host localhost port 2022: Connection refused :**

If you do not succeed there, most likely the DLS link is broken or the host\_in\_trouble is down or the ssh session is interrupted. Call the operator standing next to the host\_in\_trouble and check.

**Busy port:**

Also port 2022 maybe used or closed, this value is not fixed it can be any number except classical ports dedicated to POP, imap, ftp... feel free to use 1999 as long as both have knowledge of the chosen value. To check if port is free use netstat command as proposed.

```
netstat -a | grep 2022
```

If nothing is returned port is free, grep 2022 command will show only ports containing « 2022 » value.

Pls. send us your feedback.

Rev.1.1 – David