

Forum:[Hack Forums](#)

Thread: [\[TUT\] SSH Reverse Tunneling](#)

DarkDelta - July 14, 2011, 3:46 pm

Hello and welcome to this small tutorial.

What is reverse tunneling?

Reverse tunneling is connecting a server behind a inbound-blocking firewall to another server or computer.

Wikipedia article about reverse connections: http://en.wikipedia.org/wiki/Reverse_connection

see it like this:

Source = random, non firewalled, server

Destination = the firewalled server (e.g. home computer)

PC = well...you know that.

you connect like this:

PC -> Source <- Destination

So, if you for instance, create a port 80 tunnel to browse the webserver on the Destination, and use the local port 2000 on the Source, it will look like this.

PC -> Source:2000 <- Destination:80

port 2000 is the tunnel to port 80.

But, how do i do this?

Step 1:

Edit your sshd_config file (usually found in /etc/ssh)

Add below "Port 22"

Code GatewayPorts yes

then issue:

Code Ubuntu:

/etc/init.d/sshd restart

Arch:

/etc/rc.d/sshd restart

Step 2:

Set up the tunnel

Code ssh -R source_port:localhost:destination_port user@source

Let's break it down.

ssh

The SSH Client Command

-R

Reverse Connection

source_port:localhost:destination_port

it will look something like this..

Code 2000:localhost:80..if you want to forward port 2000 to port 80.

You can do this with port 22 (SSH) too.

Code 2000:localhost:22

then on the source server, ssh to:

ssh -l destination_user -p 2000 localhost

now you are ssh'ing into the destination server, where otherwise it would have been impossible.

if you're on another computer, and you normally SSH into your source server via port 22, you can now SSH into your destination server via SSH too, just connect to source server's hostname or IP and then port 2000 (or other when you've changed it.)

user@source

the connection info to where the tunnel should lead.

e.g.

Code root@hackforums.net

I hope you have learned from this.

to see the tunnel in action:

<http://n01p.com:2001/~remon/microtime.php>

yes, that runs on a firewalled server, normally unreachable from the outside.

Ui Hirasawa - July 14, 2011, 3:51 pm

Good tutorial, will be useful!

Alison Wonderland - July 14, 2011, 5:10 pm

Could you explain this (what it is usefull for)

i didnt quite understand the wikipedia explanation