

Forum:[Hack Forums](#)

Thread: [\[TUT-PICS\]Extreme Anonymity Dual SSH on your windows VPS](#)

Gr33nDemon - August 2, 2011, 11:30 pm

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.[1] The two major versions of the protocol are referred to as SSH1 or SSH-1 and SSH2 or SSH-2. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, rendering them susceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.

OK guys in this TUT we will make a dual "SSH + Socks5 server with authorization. In your provide Logs you will connect to one IP but you will work from another one, not yours and not from your vps.

Attention!

If you are unsure of your actions, or you do not hand out of the place (God forgive me), as described in the article, it is not recommended!

Attention!

This article was written for educational purposes, the author responsible for the unlawful use of materials of this article can not be held.

OK for our DualSSH we need:

- 1) 1 VPS with direct IP, good speed, high uptime.
- 2) 1 VPS for socks5 server with authorization, high uptime and without NAT.
- 3) Soft WinSSHD for making our SSH server
- 4) socks5 proxy-server
- 5) Proxifier 2,9 and Entunnel

OK, let's start

Step 1

We connect to our vps with RDP connection from windows, download WinSSHD and start installing.....

[img]http://s001.radikal.ru/i196/1003/91/b13aca19a16b.jpg[/img]

Do it like in the pictures and press "Install".... After that in the next window, select personal edition, press OK now you need to put your initials put what you want it doesn't matter Finishing install.

After the Install finish the control panel of WinSSHD start ok what to do here just look at the screens

Port 22 but here in this windows all conf a default

[img]http://s002.radikal.ru/i200/1003/fd/29837e48db71.jpg[/img]

ok, press next (Windows account) here are the accounts with ssh access, here are used the windows account, make one account to use for ssh with limited user access, like, login ssh_user and pass - ssh_pass, and put it here in for SSH access:

[img]http://i082.radikal.ru/1003/a7/fb9f7e78eeba.jpg[/img]

Press next and next and we finish with out default config.

Go to WinSSHD control panel select Setting -> Edit advanced setting, and in option Logging unselect like here:

[img]http://i055.radikal.ru/1003/0a/5bc6d12b44d0.jpg[/img]

Press OK ...

Configuration of SSH server is almost finished, only small tweak.

1) WinSSHD at install maked some changes to the system and for our safety we need to delete them, like autostart

go Start -> Run -> regedit

go to the following adress:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

and find the WinSSHD autostart setting:

Persistent WinSSHD Control Panel "C:\WINDOWS\addins\ssh\sshdctrl.exe" -startMinimized
and delete this key

2) WinSSHD is working like a service, you will find shortcuts in Start -> Control Panel -> Administrative Tools

delete the WinSSHD shortcut

then find all the shortcuts in Start -> All Programs

and delete them.

OK now you can start the WinSSHD control panel and start the WinSSHD server.

Step 2

Now, when we finished with WinSSHD server we can terminate the connsnction with our 1 vps ...
now we need the client to connect to our SSH server we will use Entunnel.

After we installed Entunnel and cracked it :) start Entunnel, press " Create a new session", and write like in the screen:

[img]http://img685.imageshack.us/img685/2447/etunnel.jpg[/img]

Attention: Don't put now the password for your SSH server.

For now setting up Etunnel we finished, press OK. Now select your connection SSH and press Connect, if you do all right it will ask for your password, type it and press OK now we are connected to our SSH server.

Step 3

OK, now we need to configure our socks5 with authorization protocol :)

Here the process is simple, download the socks5 archive on your 2 vps and unpack it in
C:\Windows\

We see 3 files:

Start.bat - used to test if our socks 5 is working

Socks5.reg - just write our socks to autostart.

svchost.exe - socks5 server

Let's start to configure it:

Edit start.bat we see:

```
svchost.exe -p 1080 -user admin -pass password -b 127.0.0.1
```

where:

-p is port

-user is login

-pass is pass

-b external ip if in the system we have more network connections

Example: I want to do a proxy on port 51510, with login PrOxY, and password TeSt:

```
svchost.exe -p 51510 -user PrOxY -pass TeSt -b 82.140.126.15
```

Now save Start.bat.....

Open Socks.reg, we see

Windows Registry Editor Version 5.00

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
```

```
"svchost"="C:\\Windows\\svchost.exe"
```

we need only this:

```
"svchost"="C:\\Windows\\svchost.exe"
```

OK here edit like this:

Windows Registry Editor Version 5.00

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
```

```
"svchost"="C:\\WINDOWS\\svchost.exe -p 51510 -user PrOxY -pass TeSt -b 82.140.126.15"
```

and save Socks.reg.

Well, everything seems to be ready? Then run Start.bat a window running the cmd with socks5-proxy keys, if cmd is closed immediately, than you do something wrong, reread again step 3, and if the window appeared and is not closed, it means that we do all right, then we can safely close Start.bat, and import the registry data from Socks.reg (double click and click on Socks.reg click "OK") after this procedure we can delete Start.bat and Socks.reg

Step 4

OK, it's almost all done. Now we need to configure Entunnel and put Proxifire 2.9

Open Entunnel, double click on our connection SSH, go to "Port Forwarding" .. click "Add" and put like in screen:

[img]http://img543.imageshack.us/img543/4348/etunnel2.jpg[/img]

Now install Proxifire, after the install click:

Options -> Proxy settings click add and put the socks5 server
here we need to put the login and password that we do earlier.

Finish, It's a long TUT but it's very needed when we need a good anonymity online and have some extra windows VPS:)

Now Download links:

Socks5:

<http://www.mediafire.com/?uc032eb9n832giy>

Entunnel:

<http://www.mediafire.com/?7j07fg2n3yiy7w5>

WinSSHD:

<http://www.bitvise.com/download-area>

Proxify:

<http://www.mediafire.com/?5q5tx6bb9x19drv>

P.S.: Sorry for my bad english I will try my best for this forum :)

bombasschicken - August 3, 2011, 2:41 am

What kinda performance hit do you take with this?

Gr33nDemon - August 3, 2011, 3:58 am

it's depend on vps, if you have good speed on them then it will work like a charm :)

Doxter - August 4, 2011, 8:32 am

I think I have to have port 22 open on the window VPS, am I right?

Gr33nDemon - August 4, 2011, 8:42 am

Yes how I said in tut you need VPS with direct IP without nat, or you have access to router and can open ports.

Doxter - August 4, 2011, 8:59 am

How do I check if it has NAT enabled or not?

Gr33nDemon - August 4, 2011, 10:21 am

ipconfig /all

if you get 1 network card with VPS Internet IP then its without NAT, but if you get the following IP: 192.168.*.* then it's nat

Anonymous.7654 - August 4, 2011, 10:44 am

Very nice and big Tutorial :) Thanks

Gr33nDemon - August 4, 2011, 10:48 am

Thanks :) Just trying to be a good member and to share something with community :)

? NEO ? - August 4, 2011, 11:03 am

Nice tutorial.

Thanks for the share.

.

Gr33nDemon - November 11, 2011, 5:30 pm

For nothing :) I'm making one right now :)

Guys only one problem in proxifire put not the ip of the socks5 server but 127.0.0.1:80 and the socks5 user and pass. Sorry for this, can someone update the first post?