

Forum:[Hack Forums](#)

Thread: [\[TuT\] Setup VMWare Virtual Machines with Port-Forwarding \[Noob-Friendly\]](#)

beck030 - December 26, 2010, 12:40 am

Setup VMWare Virtual Machines with Port-Forwarding

by beck030

This tutorial is a "Step-By-Step Guide" to create your own VMWare virtual machine and make it fit for use with RAT tools. As this tutorial is tagged "Noob-Friendly", i will start by explaining how to create a VMWare virtual machine.

It's my first tutorial, so if you have any suggestion for improvement, please let me know.

Updated on 27.12.2010

- Have a look at my latest tutorial too: [\[TuT\] Free VPN for RATs \(and more\) with proXPN | No more Port-Forwarding](#)

What you will needAn UpToDate VMWare Player

A Port Listener - For example RJL Port Listener

A Windows XP/Vista/7 ISO or CD

Step 1 - Download and install the VMWare Player

Get the VMware Player here: <http://www.vmware.com/products/player/>

After downloading it, run the setup. Should not be much trouble.

For some reason VMware excluded the very important "Virtual Network Editor" tool from the VMware Player setup. It is still included in the installer package, but not installed automatically. As the "Virtual Network Editor" is needed for port-forwarding, you have to install it manually.

To install the "Virtual Network Editor" manually, we have to extract the VMWare Player installer. To extract it, follow these steps:Open the directory containing your VMWare Player installer

Right-click on the installer and chose "Create Shortcut"

Now right-click on the created shortcut and go to "Shortcut" -> "Target"

Edit the "Target" line and add "/e .\vmplayer" behind the file path. The "Target" line should look kinda like this now: "C:\Path\To\VMware-player-3.1.3-324285.exe /e .\vmplayer"

Now run the shortcut. This will create a new directory named "vmplayer" or however you named it.

After extracting the installer, open the new directory and look for a file named "network.cab". This file contains the "Virtual Network Editor" tool - "vmnetcfg.exe". Extract "network.cab" and copy all files to the directory where you installed the VMWare Player.

To start the "Virtual Network Editor" tool, simply run the "vmnetcfg.exe", which now should be in the same directory as the "vmwareplayer.exe". You will need it later.

Step 2 - Create a virtual machine and install the OS

In this step i will explain how to create a virtual machine.

- Launch your VMWare Player and click on "Create New Virtual Machine."

Spoiler ([Click to View](#))

- The install wizard will popup. In the first step of the wizard you have to chose an ISO or CD to install your OS from.

Spoiler ([Click to View](#))

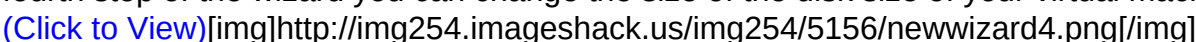
- In the second step you have to provide a CD-Key for your OS and a password which will be used for the admin account.

Spoiler ([Click to View](#))

- In the third step you can change the name of your virtual machine and the directory where it will be stored.

Spoiler ([Click to View](#))

- In the fourth step of the wizard you can change the size of the disk size of your virtual machine.

Spoiler ([Click to View](#))

- In the fifth and last step you will see a summary of the settings for your virtual machines. Click on "Customize Hardware" to increase RAM or use multiple CPUs.

Spoiler ([Click to View](#))

- You should now see a new virtual machine listed in your VMWare player. Click on "Play virtual machine". If you run the machine for the first time, the windows OS setup should start automatically. Just run the setup as usual.

Thats it! After finishing the setup, you should be able to start working with your virtual machine.

Step 3 - Port Forwarding with VMWare

If you want your VMWare virtual machine to run a RAT client like CyberGate, you have to forward the listening port from the host-system (where the VMWare Player is installed) to your virtual machine. in that case this shitty diagram i just made shows what happens:



I know the diagram really looks like crap. I can make a better one later if you guys want me to. But basically it shows what we have to do. The RAT servers on your victims computers try to send data to your RAT client using the listening port you have set. That data will end in nirvana if you dont forward the listening port to the machine, on which your RAT client is running.

In our case the RAT client is running on a virtual machine. So the port forwarding must be like this:

Router -> PC -> Virtual Machine.

Spoiler ([Click to View](#)) i hope that was not too confusing, lol

In this step of my tutorial i will explain how to forward a port from your host-system to your virtual machine.

To do so you first have to find out the your virtual machines IP. At this point i just assume that you know how to find out your IP on a windows OS.

After you got the IP, run VMWare's "Virtual Network Editor" - read Step 1 of this tutorial to find out where to find and how to start it.

- In the "Virtual Network Editor" you will find a list of virtual network adapters. Each virtual network adapter has its own subnet. The IP of the subnet is in the far right column.

Spoiler ([Click to View](#))

- Now you have to select the right virtual network adapter and hit "NAT Settings...". To find out which is the right virtual network adapter your have to compare the IP of your virtual machine with the subnet IP in the far right column.

An example: If the IP of your virtual machine is 192.168.133.15, you have to select the network adapter "VMnet6". If the IP of your virtual machine is 192.168.182.12, you have to select "VMnet8".

Spoiler ([Click to View](#))

- This last step is pretty much self-explaining. Click on "Add" to create a new port forwarding rule. "Host port" is the incoming port of the host where you installed the VMWare Player. "Virtual machine port" is the port of the virtual machine you want to forward to. Normally both ports are the same (For example the listening port of your RAT client).

Create 2 rules for every port. One for TCP and a second for UDP Protocol.

Step 4 - Test the Port-Forwarding

After setting the port forwarding rules, we have to test if it is working right. This is where we need a Port listener. I suggest to use "RJL Port Listener", which can be downloaded here:

<http://www.rjlsoftware.com/software/utility/portlistener/download.shtml>

- Download and run the Port listener on your virtual machine.

- Type in the port you forwarded and click on "Start".

Now go to <http://www.canyouseeme.org>, type in the port you forwarded and click on "check" to perform a port scan.

- Go back to your virtual machine and look at the port-listener tool you started before performing a port scan. You should see a message like this:

Spoiler ([Click to View](#))

If you see that message ("Client connected", "Client disconnected") it means, that the portforwarding was successful and all incoming traffic on the listening port will be forwarded to the

virtual machine!

Something didnt work for me! / I still have questions

Port Forwarding doesnt work?

- Make sure that you have set the firewalls on the host-system and on the virtual machine have the listening port opened.

- If you are behind a router, make sure that you forward the listening port to the host-system.

Feel free to ask your questions in this thread or send me a pm.

willbebacksoon - December 26, 2010, 1:11 am

Very Detailed Tut.Thanks :>

-mothered- - December 26, 2010, 1:35 am

Very well documented and elaborated mate, with supported Illustrations.

I've had a brief look, but will delve Into It In detail, within the next couple of days.
Bookmarked and appreciated.

Fallenbot - December 28, 2010, 3:34 am

Interesting tutorial mate. Thanks for sharing,appreciated!

seskanda - December 28, 2010, 11:06 am

Superb Tut, and pics are always welcome

fidgit - December 30, 2010, 12:38 am

Awesomeness! thanks for the tut...and the pretty pictures....

Dionysos™ - January 5, 2011, 10:53 am

Thanks for tut bro, will try that when I'm finished downloading my Win 7 x64

Akureyri - January 22, 2011, 7:39 am

Wow,very nice tut man,thanks for posting...

Exposer - January 22, 2011, 5:14 pm

Tutorial is very informative and very nice..but im stucked in middle..
im new to this section..vmware and vbox..

can you also give .iso file or link of .iso to download.. i dont want to go to trouble installing the windows of 30 mins..also dont have cd of windows right now with my self...lolz..

please give a link or forward where i can download an image of xp.

Exposer - January 23, 2011, 2:10 am

Hi...i dont know why it even dont work for my port 80

[img]http://imm.io/media/3j/3jDq.png[/img]

<http://imm.io/3jDq>

Loop - February 14, 2011, 5:45 am

Great tutorial, thanks a lot bro. ;)

Zenpest - February 19, 2011, 3:50 am

Thanks for a good tutorial mate :)

Fo0xy.One - February 19, 2011, 5:13 am

I know how to setup VMWare but for newbs this is pretty usefull. The one who does not understand this tutorial is really stupid xD

B33RF3aR - February 24, 2011, 10:59 am

awesome tutorial.... well i am trying to create a botnet very 1st time and its really useful.. Thanks alot...

Riverhead - February 25, 2011, 1:58 pm

Great tutorial, thanks for sharing!

?Exempt - February 25, 2011, 5:08 pm

for those who dont have a Product key :

[http://www.geekblogger.org/2010/03/dont-crackwindows-7-activation-key-wat.html?utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed:+geekbloggerorg+\(Best+Blogging+Tips+and+Templates,Windows+and+Web+Applications+%26+Games\)](http://www.geekblogger.org/2010/03/dont-crackwindows-7-activation-key-wat.html?utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed:+geekbloggerorg+(Best+Blogging+Tips+and+Templates,Windows+and+Web+Applications+%26+Games))

CharleyisHere1 - March 18, 2011, 5:13 am

I just send a pm to get more info on this.

draght - March 19, 2011, 6:04 pm

Thx for the share! Nice tut :D

MotherzStreet - March 27, 2011, 4:31 pm

Great work, i solved my problems with it, thanks for posting!

MouseDesign - March 29, 2011, 8:36 am

You explained every aspect briefly yet so detailed. Good job.

sukhpalsomal - May 13, 2011, 9:12 pm

thank you bro. its awesome tutorial. helped me alot

BiHGamer - October 20, 2011, 9:19 am

It sais * Port 100 - Address already in use: Only one usage of each socket address (protocol/network address/port) is normally permitted.. What have i done wrong ?

younger lean - October 21, 2011, 4:57 pm

Thanks for the great tutorial! You helped me out a lot! I now have VMWare thanks to you!

DeXtroTip - October 22, 2011, 11:32 am

Great tut ^^ I appreciate it

Thanks a lot ^^

bae - October 25, 2011, 9:39 am

Or click on the network adapter under virtual machine settings and select Network connection:"Bridged" which gives you a physical IP on the network using the virtualised NIC. Then simply port forward from the upstream router or pop it into the DMZ if your router supports it.

just-testing - October 26, 2011, 11:00 pm

Thats really cool....thanks mate

ahgggg..message to short, dang it lol

nrd - November 9, 2011, 4:56 pm

this was really helpful but i did mine another way i made it bridged and replicate physical network state then got the local ip for the virtual machine and then port froward that way but i noted if u have at&t routers that u do the ip of the computer ur on not the virtual machines local ip

nawathapriya - November 9, 2011, 11:39 pm

It's a very nice tutorial, thanx for the nice port forwarding tool man...:)

hezzling_me - December 6, 2011, 6:12 am

hi,

thanks, it was a nice tutorial. i m working on setting up RAT since last three weeks. searched alot over internet. everything is perfect. ports are opened, antivirus is off, firewall is off, DUC is running perfectly. but something is wrong. i have tried both cybergate as well as darkcomet, it works fine when i try it on my own laptop but whenever i try to run it on someone else's pc, it stops working. i m not using any type of crypton or binding.

can anyone help me?

Thanks n Regards,

crazyj - December 7, 2011, 12:01 am

Very nice tutorial my friend , thanks....

poonampandey108 - February 20, 2020, 9:41 am

I really appreciate your efforts and time you gave in explaining things better...

Thanks a lot! @beck030

Bastille - February 20, 2020, 10:00 am

(Feb 20, 2020 10:41 AM)poonampandey108 Wrote: [\[CITE\]](#) I really appreciate your efforts and time you gave in explaining things better...

Thanks a lot! @beck030

This in an old thread, please take care each time you post.

Besides there is no more pictures, not very useful anymore

By the way please take a look about the [Help Docs](#) and the Introduction section.

Have a nice day