**Metasploit Hacking**

In today’s task, we’re going to hack the Metasploitable2 machine with Metasploit, targeting the **vsftpd service**.

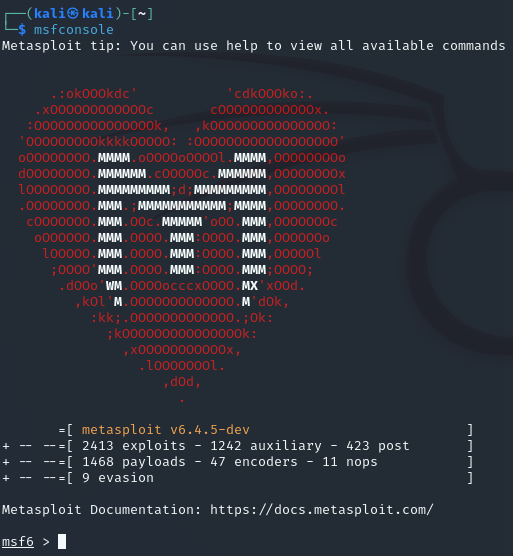
Metasploitable will have **192.168.1.149/24** as its IP address.

First, let’s scan Metasploitable with Nmap, in order to find the port attached to the ftp protocol.

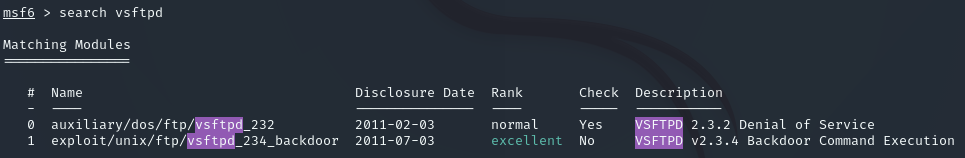


**Port 21** will be our RPORT.

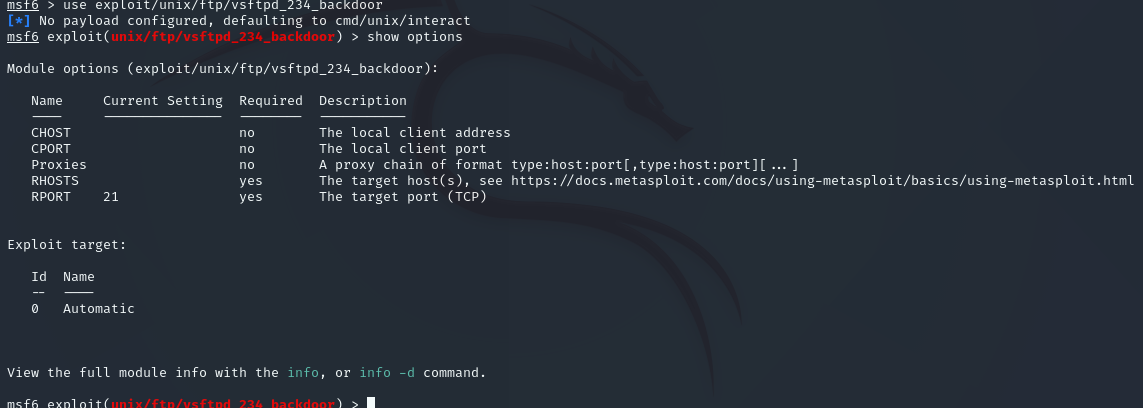
Now, with the command **msfconsole**, we’ll open metasploit.

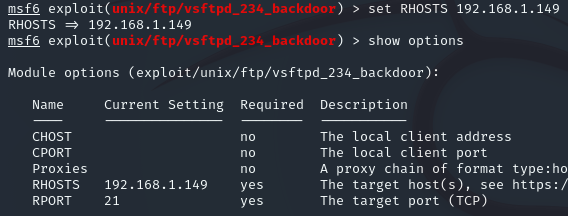


We’ll use the command **search** together with the term **vsftpd** in order to find any exploits related to the service.



With this, we’ve got the vsftpd\_234\_backdoor exploit which will allow us to install a backdoor on metasploitable. Now we’re going to see which options are available to configure so that we can launch the exploit.

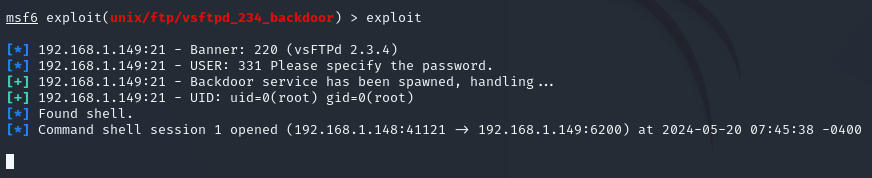


We’ll set the RHOSTS parameter to the 192.168.1.149 IP and we don’t need to set the RPORT since it’s already port 21 by default. 

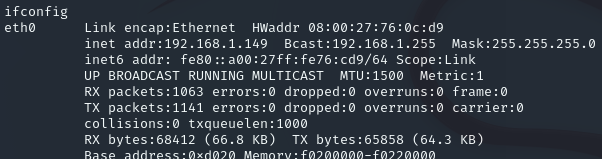
We can see that the RHOSTS has been successfully set.

Since we only have one payload, metasploit will default to it, without having to set it ourselves.

Now we’ll launch the attack with the command **exploit**.

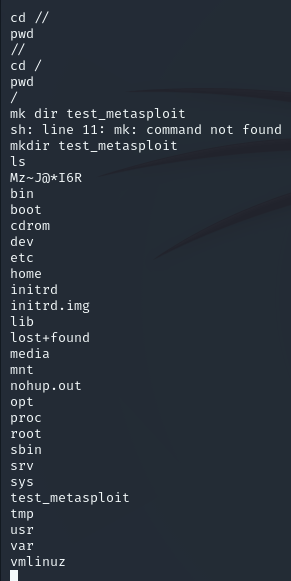


It seems everything went according to plan, let’s check quickly with an **ifconfig** command to see if we are inside the target host.



**Ifconfig** gives us the IP address of metasploitable, confirming our success.

Now we wil move to the root directory (/) and we will create a new directory inside of it named **test\_metasploit.**



Thanks to the ls command we can see which files and directories are present in the root directory. As we can see, we were successful in creating the new directory.