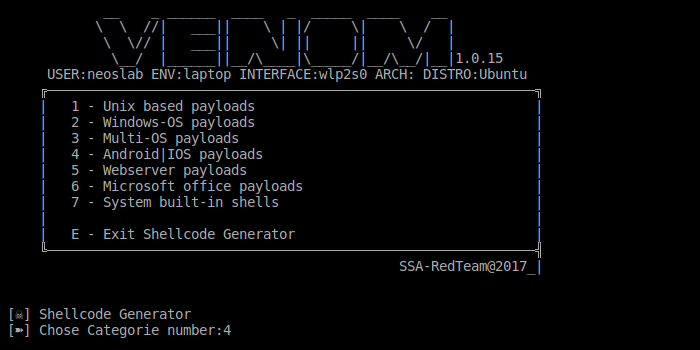
**LAUNCH VENOM**

|  |
| --- |
| $ sudo ./venom.sh |

Once the tool has been launched, it will prompt you to press “Enter” to continue for proceed further options.

[click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

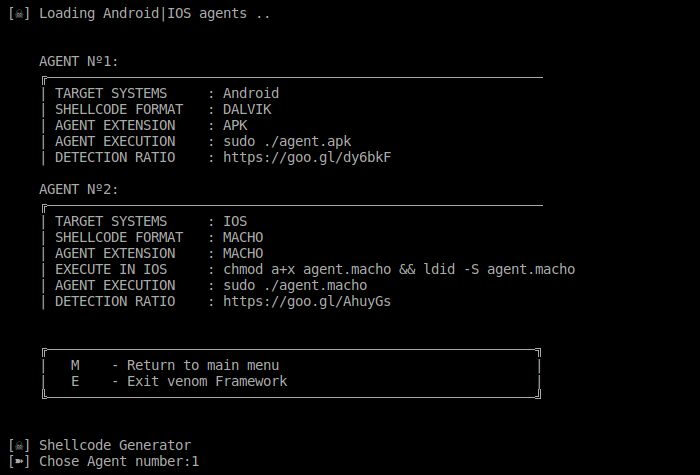
The next screen will show you the information about the Option Built, the target machine, the payload format and the and output. There is 7 differents type of option builds shellcode listed. We are going to use the shellcode “**number 4**” for the purpose of this demonstration.

[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

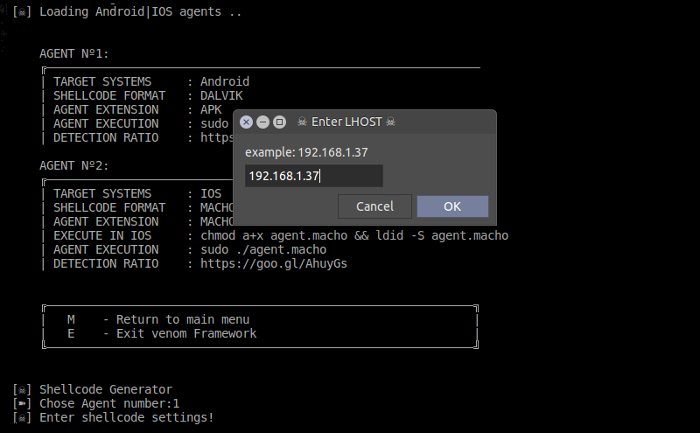
Simply choose the Venom shellcode “**number 4**” and press “enter” to continue.

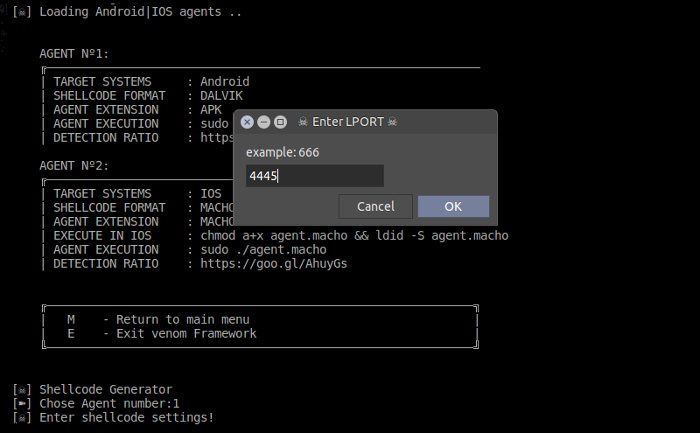
**PAYLOAD CONFIGURATION**

You will need now to choose your agent referal. For this payload Venom offer you two options. Select the one that you want to use between Android and IOS. On our side we will select the agent “**number 1**” for the purpose of this demonstration.

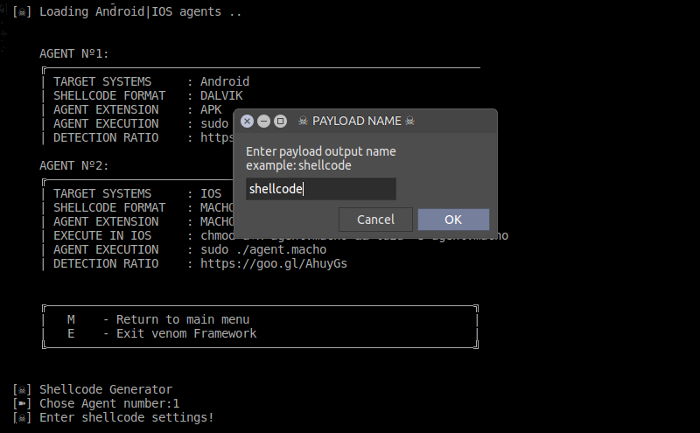
[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

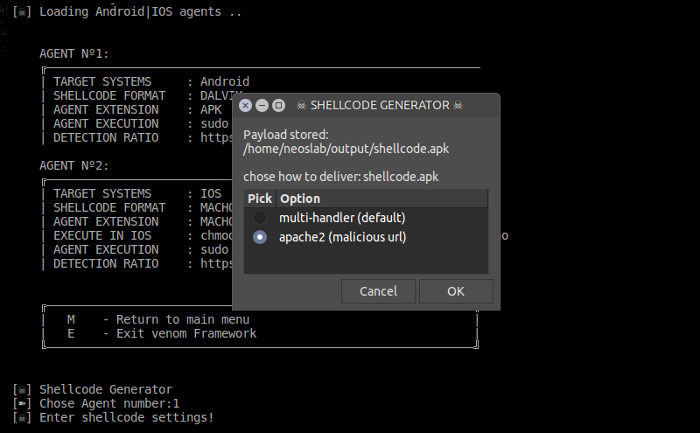
We will need now to setup the local host IP address along with the local port. Now enter your local machine IP address and local port which will be used by the payload for listening. For your information local IP address and local port are amways refered as “**LHOST**” and “**LPORT**” exactly like Metasploit.

[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

It’s now the time to give a name to our payload which will be used to save it and to define the way we want the payload to be deliver.

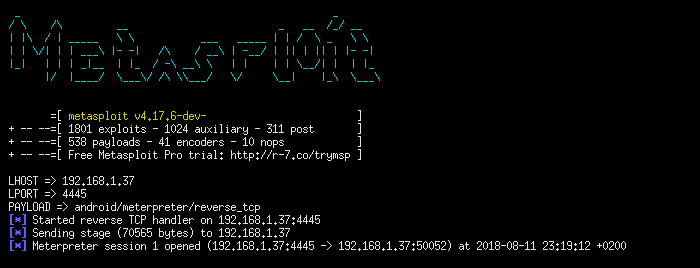
[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)

**You might be interested in**

**LAUNCH THE ATTACK**

At this stage we can say that you are almost done ! A new terminal will automatically start a session of Metasploit allowing you to conduct your attack with the encrypted Payload.

[[](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)click to enlarge](https://neoslab.com/2018/08/11/bypass-antivirus-detection-with-encrypted-payloads-using-venom/)