Hack Remote PC using BrowserBackdoor –

JavaScript WebSocket Backdoor

BrowserBackdoor is an Electron application that uses a JavaScript WebSocket Backdoor to connect to the listener.

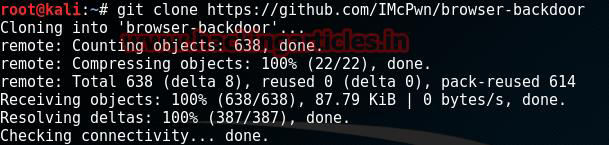
BrowserBackdoorServer is a WebSocket server that listens for incoming WebSocket connections and creates a command-line interface for sending commands to the remote system.

The JavaScript backdoor in BrowserBackdoor can be used on all browsers that support

WebSockets.

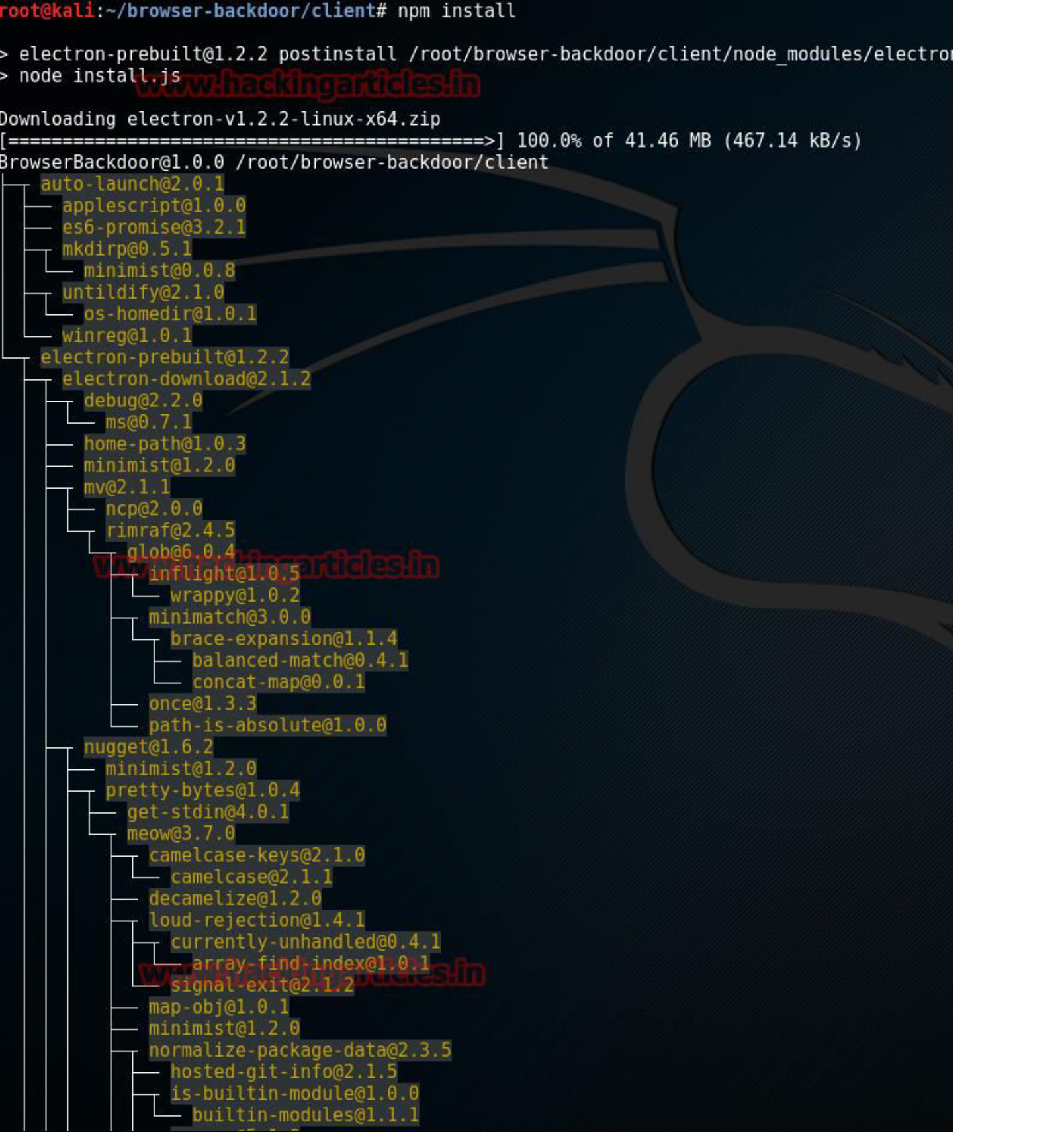
First clone BrowserBackdoorServer repository from github, to do so type:

**https://github.com/IMcPwn/browser-backdoor.git**

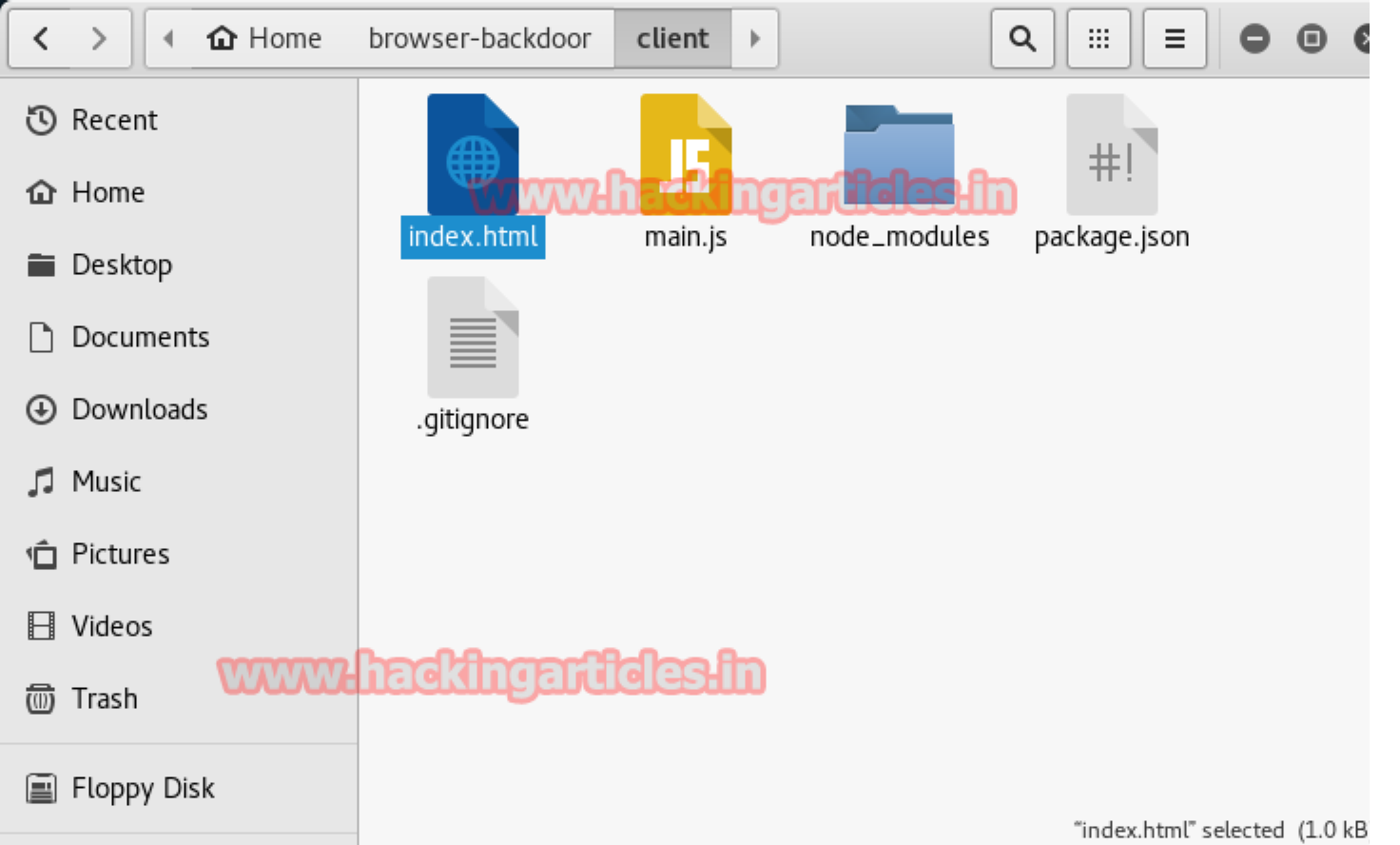


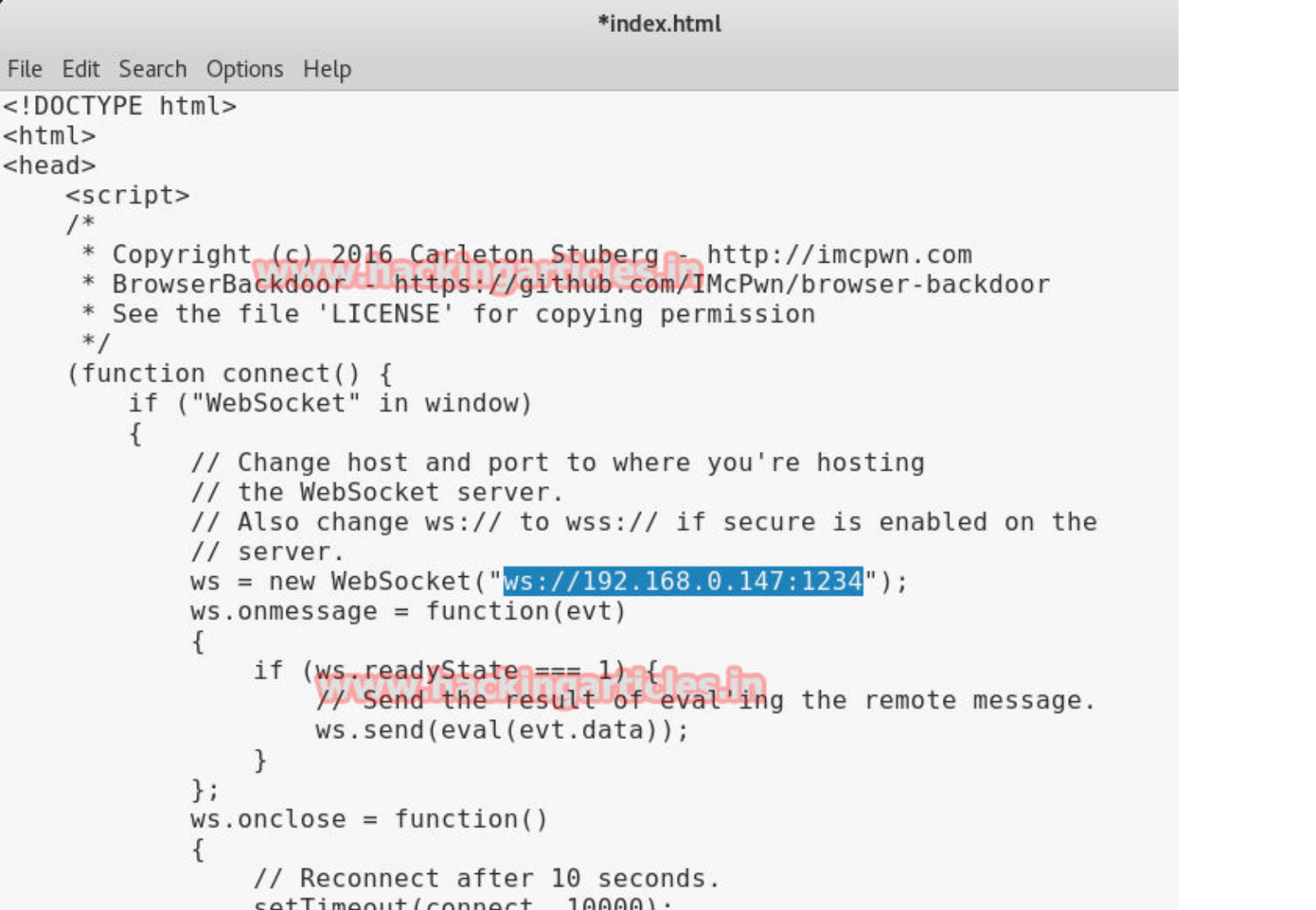
Follow the below steps one by one:

**cd client npm install**



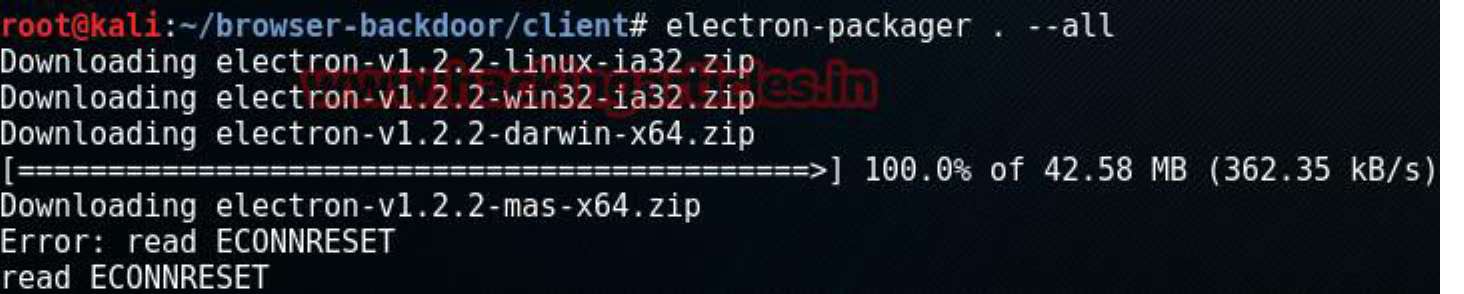
Now go to the client folder and open **index.html** file in leafpad and edit the following line now type your kali Linux ip screenshot is given below.

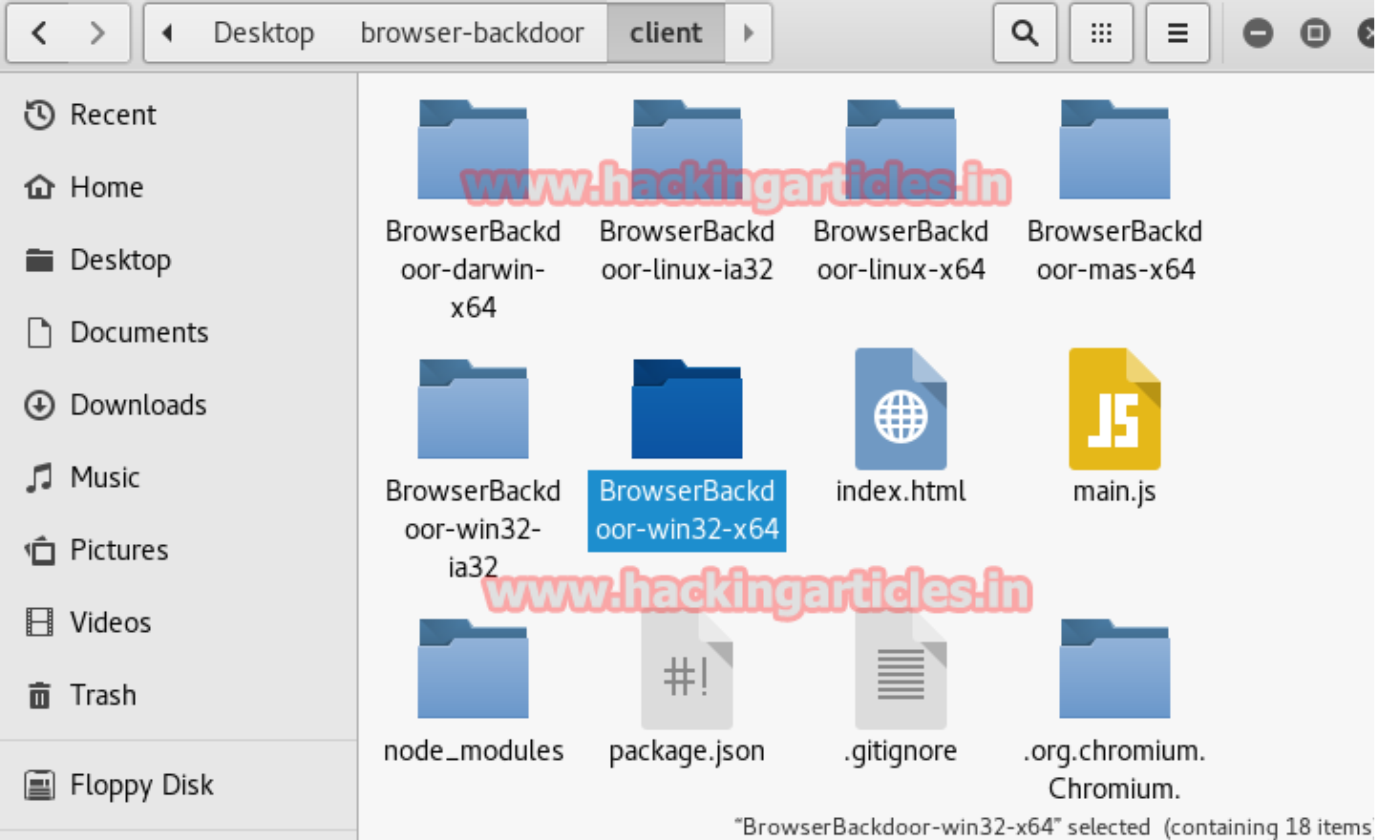




After finishing the above task it will create the Browser backdoor script folder for windows and

Linux users



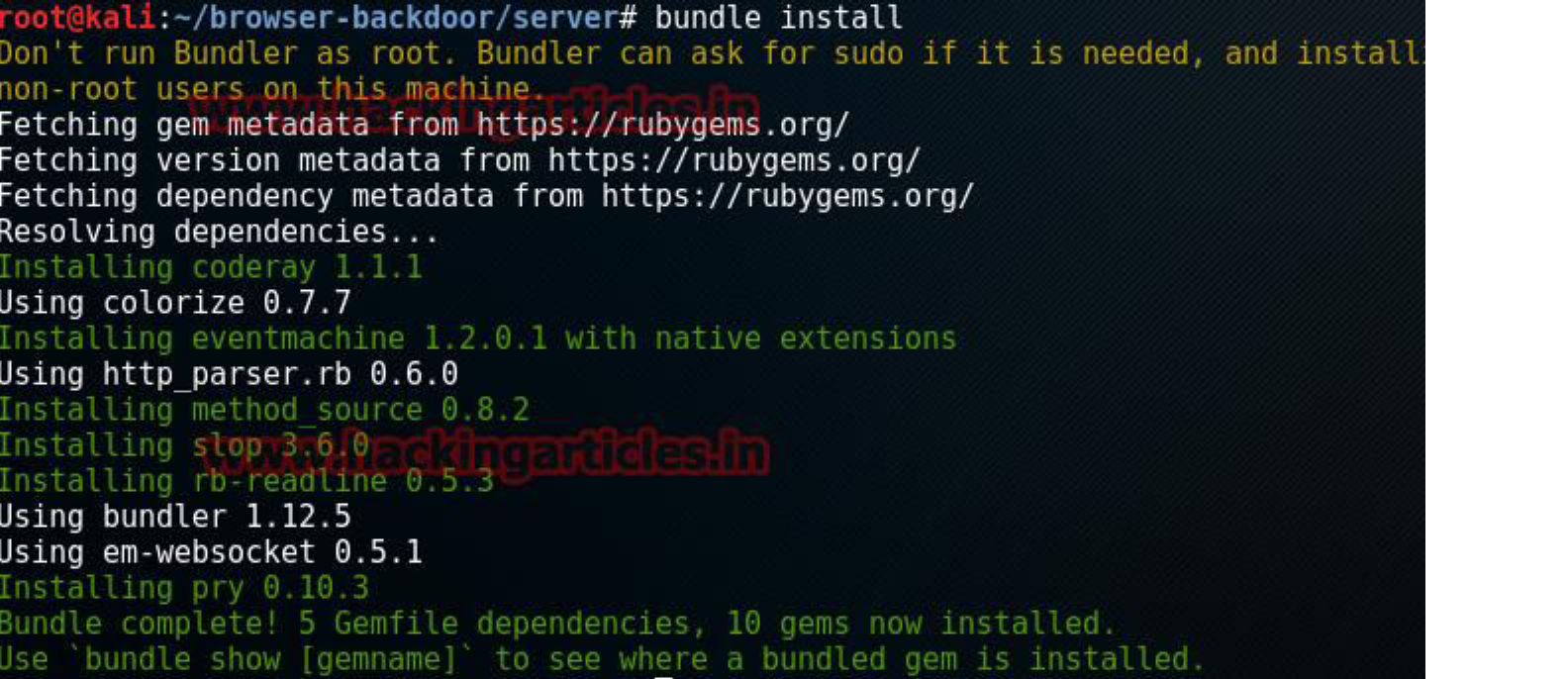


Now type the following command step by step

**npm install electron-packager -g electron-packager . –all**

Now go to the server folder in browser-backdoor directory and the following command

**Bundle install**



After that start browser backdoor by typing in terminal:

**ruby bbsconsole.rb**

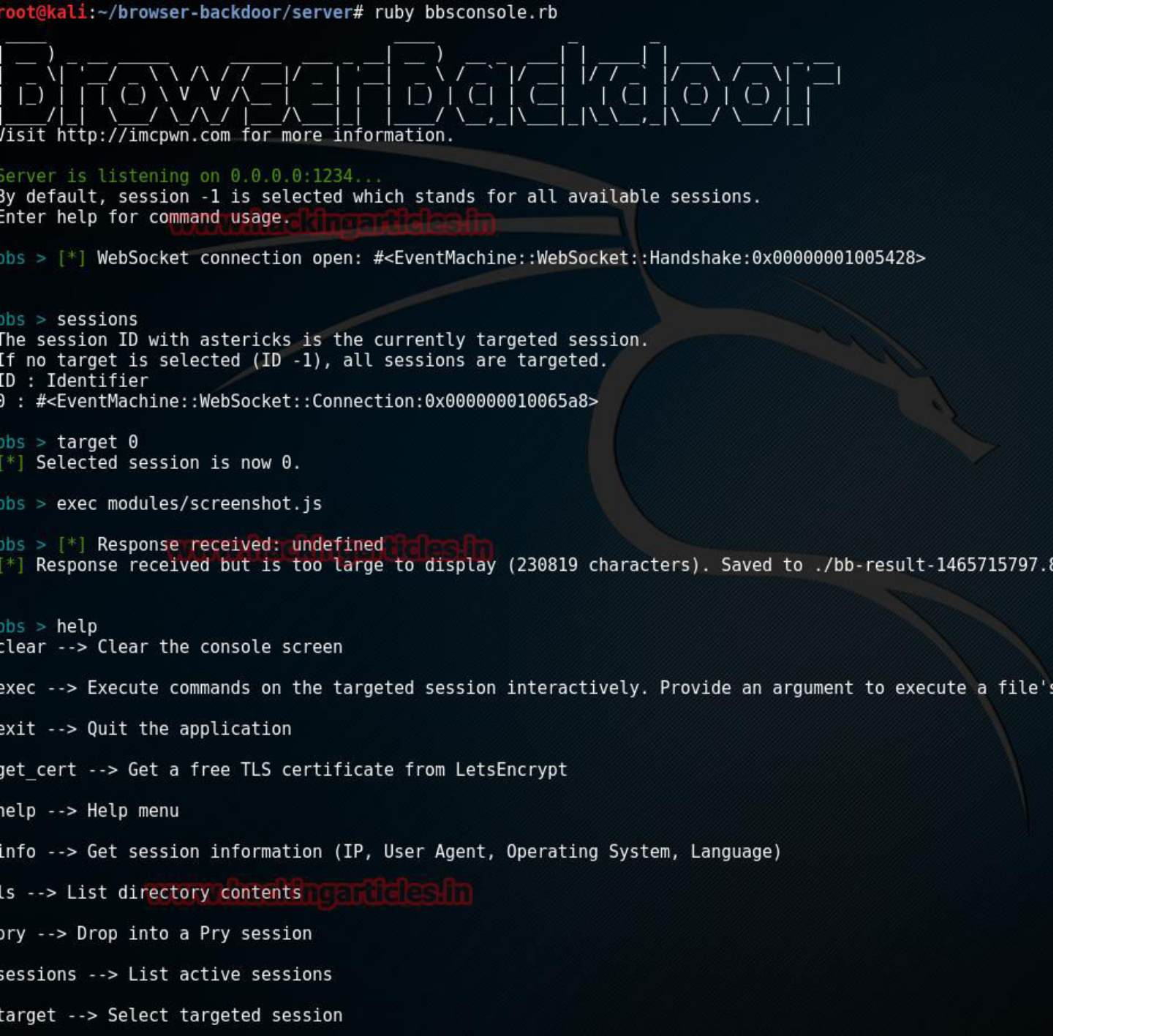
Now send the Brwoserbackdoor-win32-x64 to the victim using any social engineering method when the victim clink on BrowserBackdoor file you can get the victim session example are given below.

Now type the **session** command to check the active session it will show you the session with id no.

Type the target command with session id to interact with current session sees the following example

**Target 0**

Now if you want to more option type the **help** command you can get the list of all available command



**You might also like:**