Embedded Backdoor with Image using



FakeImageExploiter

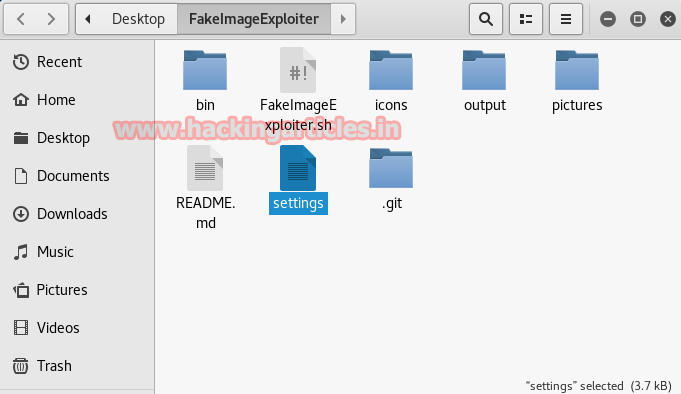
In this article we are introducing a newly launched hacking tool “**Fake Image Exploiter**”. It is design so that it becomes easier for attackers to perform phishing or social engineering attacks by generating a fake image with hidden malicious .bat/.exe file inside it.

**Let’s start!**

Open the terminal inside your kali Linux and type following command to download it from github.

**Git clone https://github.com/r00t-3xp10it/FakeImageExploiter.git**

Once it gets downloaded then opens the folder and selects the file “**settings**” for configuration before running the program as shown the given screenshot.



Now made some changes inside setting file as shown the screenshot:

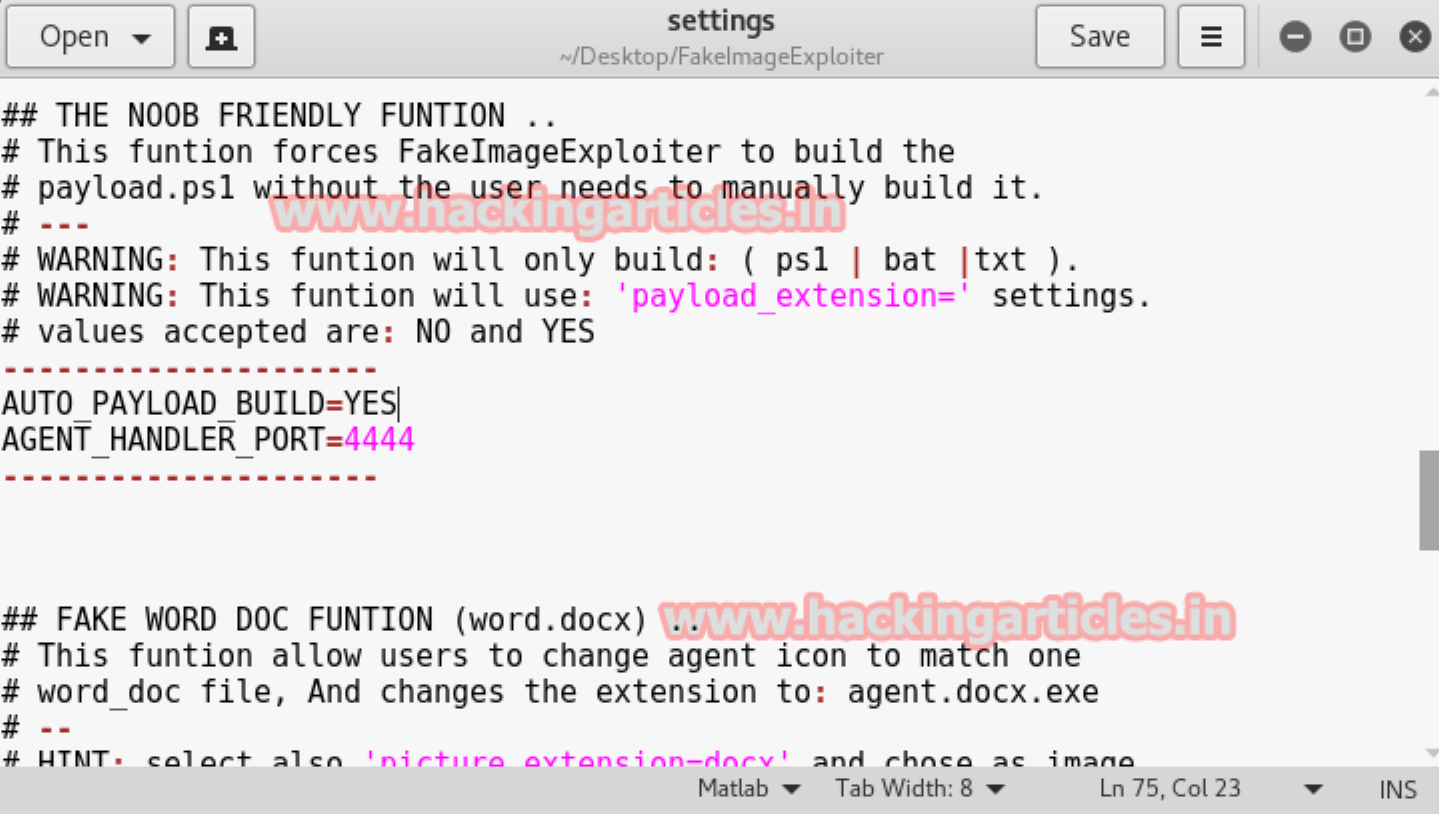
Here you have to declare the type of payload extension you will use to hide it inside the image. You can set any exetension among these four : ps1, bat, txt, exe. I had

set **PAYLOAD\_EXETNSION=bat** similarly set **BYPASS\_RH=NO** and scroll down for next configration.



In same way set these two values also as shown in screenshot then save the changes.

**AUTO\_PAYLOAD\_BUILD=YES AGENT\_HANLER\_PORT=4444**



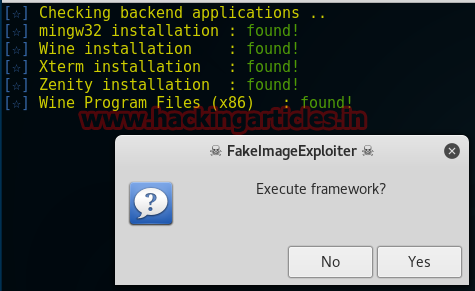
After making certain changes in setting file then open the terminal and run the program file:

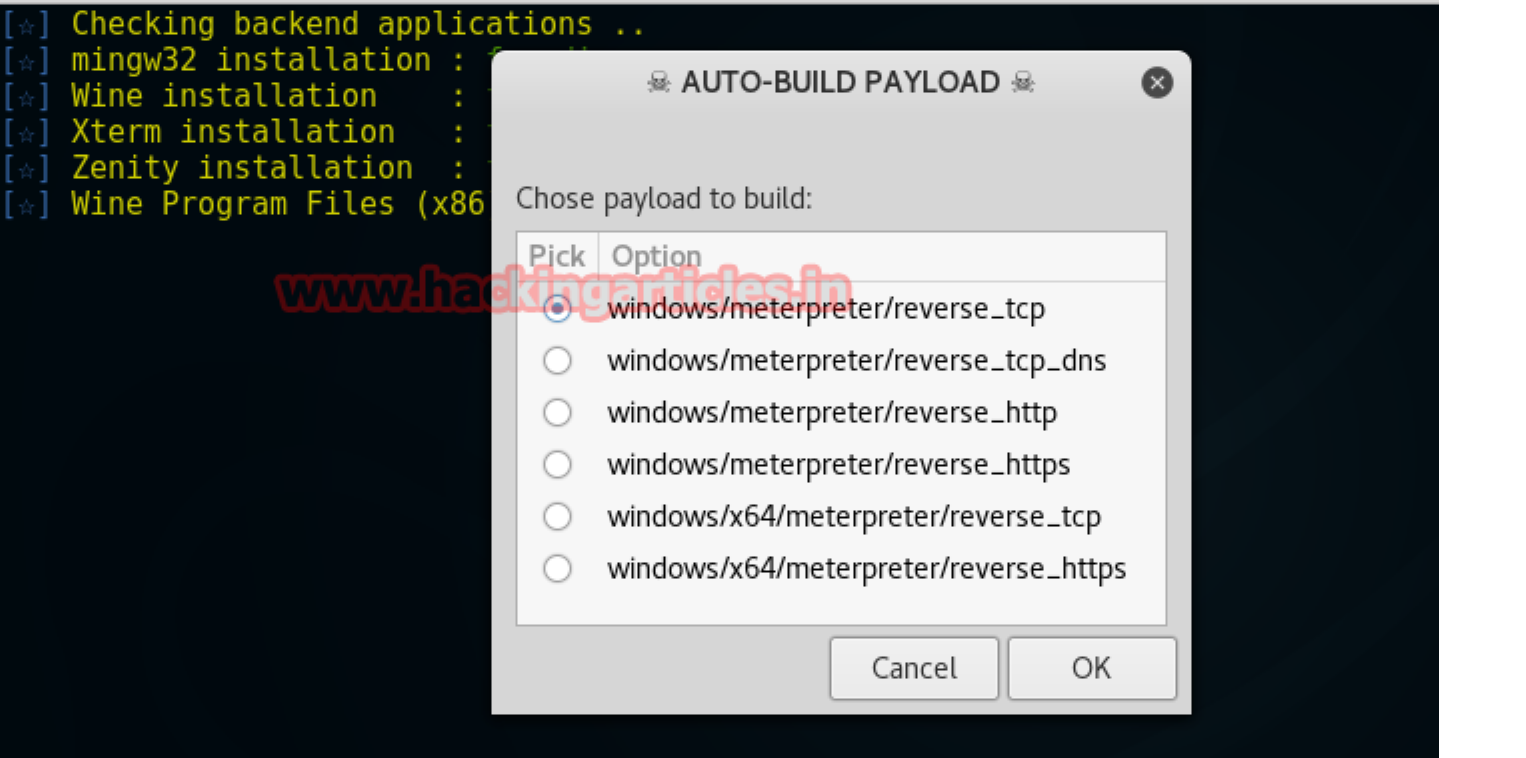
**Cd FakeImageExploiter**

**./ FakeImageExploiter.sh**



**Click** on **YES** to execute framework.

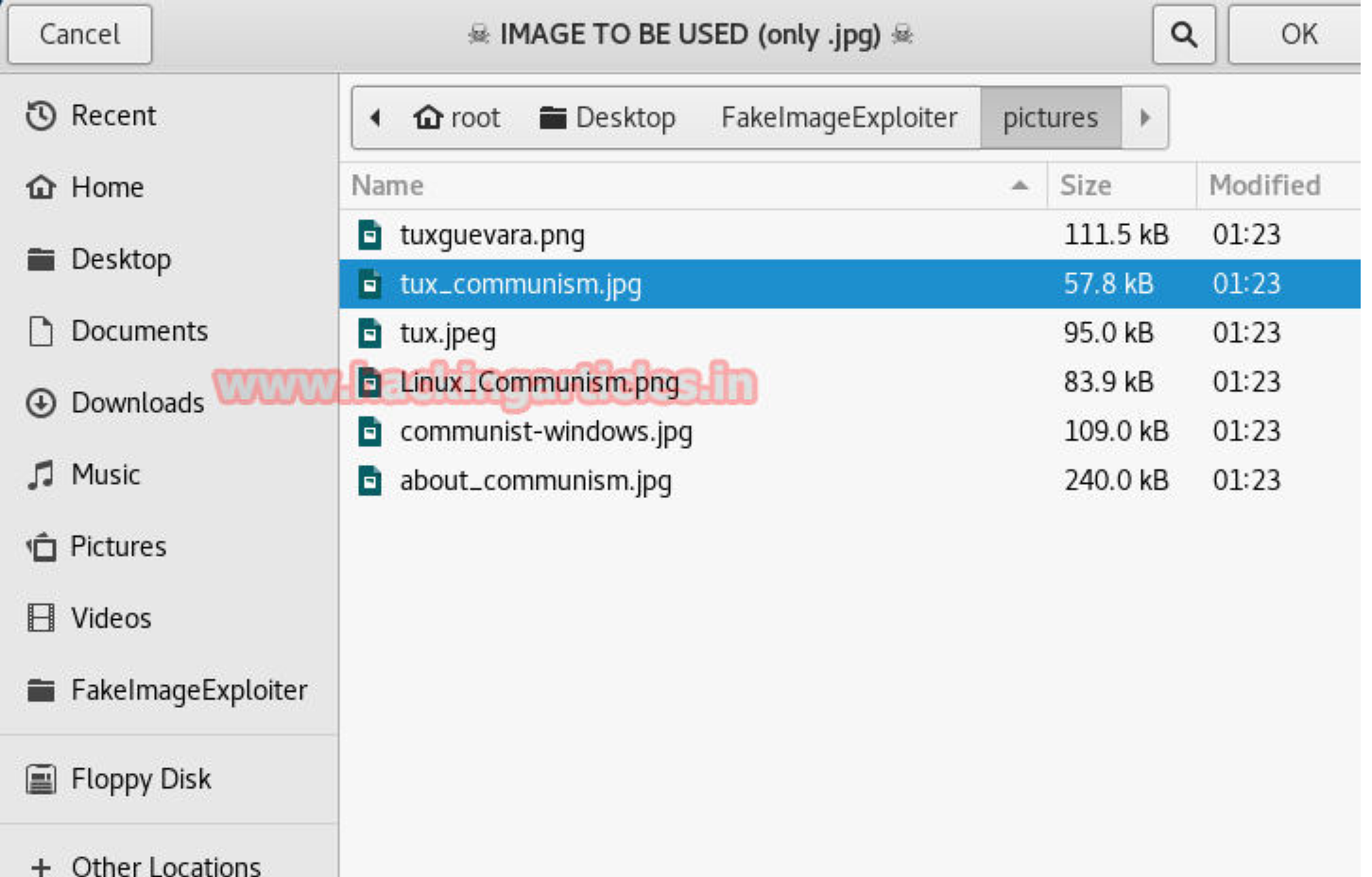




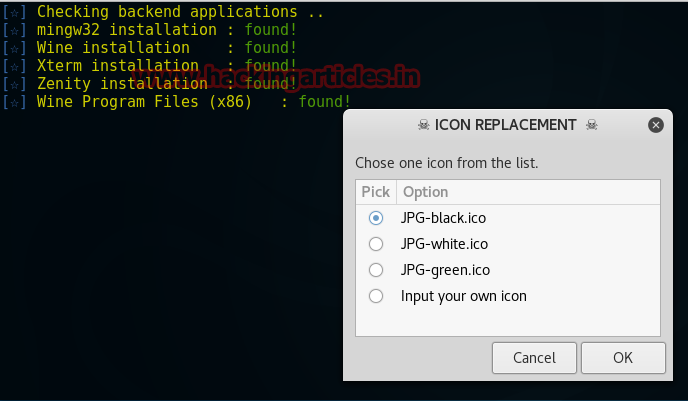
Select payload to build as I had choose **window/meterpreter/reverse\_tcp** for attack.

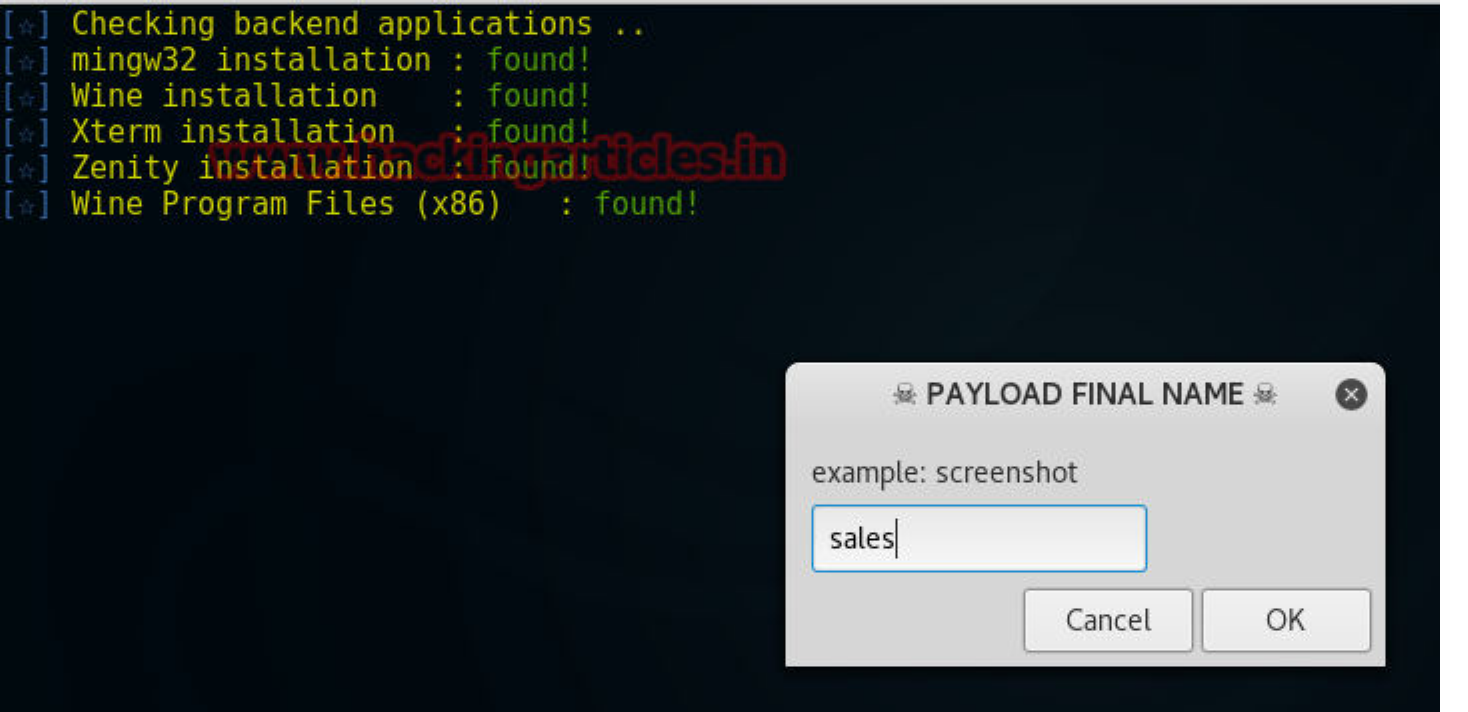
After then a pop up box will open which will allow choosing any **jpg image** so that it could hide

.bat file payload inside that image.



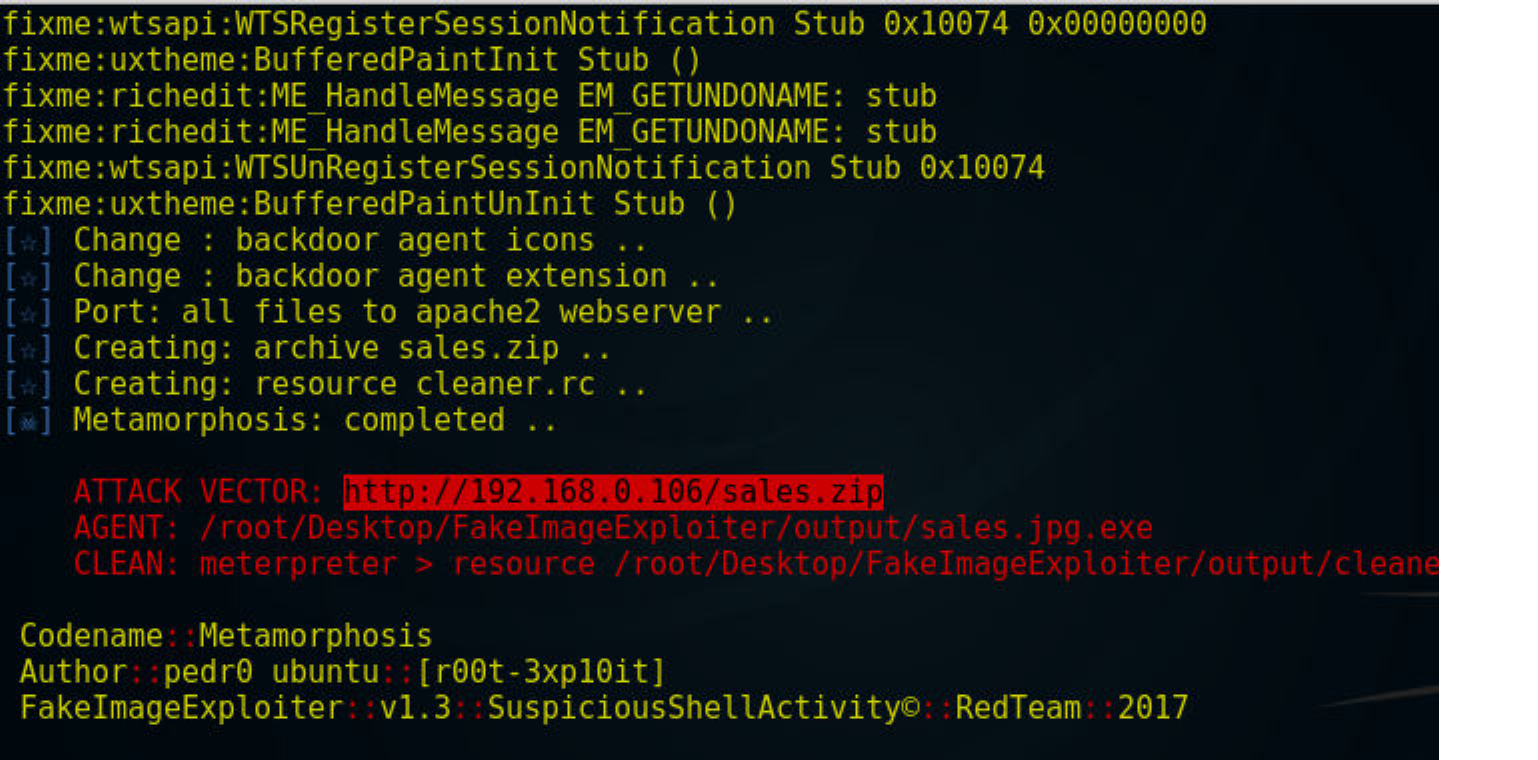
Now select icon for your malicious image.



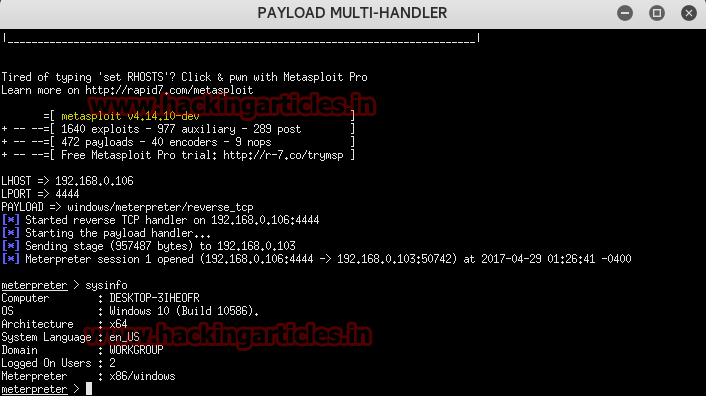


Give a name to your payload which will be display to victim as file name, from screenshot you can see I had given **sales**.

Now it generates a **link** as you can observe it from highlighted part of screenshot and then send this link to victim. Now victim will download the zip file and click on the **sales.jpg**.



When victim will click on sales.jpg, we will get meterpreter session at the background on metasploit framework.



**Author**: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information

Security Consultant Social Media Lover and Gadgets. Contact **here**